



Brussels, 13.9.2017  
SWD(2017) 500 final

PART 1/6

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF  
THE COUNCIL**

**on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013,  
and on Information and Communication Technology cybersecurity certification  
("Cybersecurity Act")**

{ COM(2017) 477 final }

{ SWD(2017) 501 final }

{ SWD(2017) 502 final }

## Table of Contents

<i>GLOSSARY</i> .....	5
1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT.....	11
2. PROBLEM DEFINITION .....	17
<b>2.1. Overview of the findings of the evaluation of ENISA and the relevant public consultations</b> .....	17
<b>2.2. What is the size of the problems?</b> .....	20
<b>2.3. What are the problem drivers?</b> .....	23
<b>2.4. What are the problems for action?</b> .....	25
2.4.1. Problem 1: Fragmentation of policies and approaches to cybersecurity across Member States .....	28
2.4.2. Problem 2: Dispersed resources and fragmentation of approaches to cybersecurity across EU institutions, agencies and bodies.....	35
2.4.3. Problem 3. Insufficient awareness and information of citizens and companies. ....	38
<b>2.5. Who is affected by the problem and to what extent?</b> .....	42
<b>2.6. How will the problem evolve?</b> .....	45
3. WHY SHOULD THE EU ACT? .....	46
<b>3.1. Legal basis</b> .....	46
<b>3.2. Subsidiarity</b> .....	46
4. OBJECTIVES: WHAT SHOULD BE ACHIEVED?.....	47
<b>4.1. General objectives</b> .....	47
<b>4.2. Specific objectives</b> .....	47
5. WHAT ARE THE AVAILABLE POLICY OPTIONS? .....	48
<b>5.1. What is the baseline from which options are assessed?</b> .....	48
<b>5.2. Policy options related to ENISA</b> .....	49
<b>5.3. Options related to certification</b> .....	54
<b>5.4. Options discarded at an early stage</b> .....	60
6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?.....	62
<b>6.1. ENISA</b> .....	62
<b>6.2. Certification</b> .....	70

7.	HOW DO THE OPTIONS COMPARE? .....	82
8.	PREFERRED OPTION .....	88
9.	HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED? .....	96

### **Table of Figures**

Figure 1	Priority areas for EU action in cybersecurity .....	14
Figure 2	Selection of significant cyber-attacks in 2016. ....	21
Figure 3	Problems to tackle .....	25
Figure 4	Problem Tree .....	26
Figure 5	Some issues on awareness and knowledge of cybersecurity issues in Europe ..	39
Figure 6	Overview of a how a European cybersecurity certification scheme is adopted. ....	57

### **Table of Tables**

Table 1	Summary of results of the evaluation according to the criteria.....	16
Table 2	Scope of NIS Directive in relation to key areas .....	27
Table 3	Most urgent gaps and needs, as emerging from the stakeholder consultations... ..	30
Table 4	Mission of relevant EU agencies and bodies in the cybersecurity field.....	36
Table 5	Overall impact of the various policy options for ENISA.....	85
Table 6	Overall impact of the various policy options for certification. ....	86
Table 7	Overview of main changes in the tasks between current ENISA and preferred option.....	88
Table 8	List of indicators to monitor progress towards general objectives.....	97

## **List of Annexes**

**Annex 1 Procedural Information**, including organisation and timing of the initiative, exceptions to the Better Regulation Guidelines, the replies to the ISG comments made and the list of evidence provided.

**Annex 2 Stakeholder Consultations**, including the consultation strategy (which stakeholders, which type of mechanism) and the individual consultation results.

**Annex 3 EU Agencies Budget and Staff**, providing information on the total EU financial contribution to the 32 decentralised EU agencies, as well as their authorised establishment plans (i.e. staff) in 2017.

**Annex 4 Preliminary Mapping of the 16 EU-level Entities that Provide Cybersecurity Content.**

**Annex 5 Final Study on the Evaluation of ENISA**, as delivered 20 July, 2017 which involves an evaluation over the 2013-2016 period, assessing the Agency's performance, governance and organisational structure, and positioning with respect to other EU and national bodies. It assesses ENISA's strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It also provides options to modify the mandate of the Agency to better respond to new, emerging needs and assesses their financial implications.

**Annex 6 Economic Analysis of Policy Options for ENISA**, providing an estimation of the costs related to each of the four options for the future of ENISA derived from the results of the evaluation of ENISA.

**Annex 7 ICT Security Certification Study** as final version of the commissioned study providing the essential evidence base for the Impact Assessment, as delivered 25 July, 2017.

**Annex 8 JRC Study on Certification**, which investigates and proposes recommendations for the establishment of a European ICT security certification framework and assesses the feasibility of a European cybersecurity labelling framework.

**Annex 9 Sectoral Mapping of EU and International initiatives on Cybersecurity**, as recently revised which maps ongoing initiatives in the field of cybersecurity across key sectors covered by Chapter III of the NIS Directive: energy, transport, banking and finance, health, drinking water.

**Annex 10 Who is Affected and How**, describing the practical implications of the preferred option identified in the Impact Assessment for stakeholder groups likely to be directly or indirectly affected by the initiative.

**Annex 11 ICT Security Certification Landscape**, which lists the International and national certification schemes and other initiatives.

**Annex 12 Case Studies** as a new annex on certification schemes in the areas of smart meters, and cloud computing.

## ***GLOSSARY***

The below table explains the key terms or acronyms used in this document.

<b><i>Term or acronym</i></b>	<b><i>Meaning or definition</i></b>
2016 Council Conclusions	Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry – 15 November, 2016.
2016 Cybersecurity Communication	Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.
Accreditation	Accreditation means an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity. (see also EC Reg. No. 765/2008)
ACER	Agency for the Cooperation of Energy Regulators.
ANSSI	Agence nationale de la sécurité des systèmes d'information; this is the National Cybersecurity Agency of France.
ARGUS	ARGUS is the Commission's general alert system in place since 2005. It is a process supported by an information technology (IT) tool and a dedicated network of 24/7 duty officers in each relevant Directorate-General
Blueprint	Framework (under preparation) for EU level approach on responding to large-scale cross-border cybersecurity incidents or cybersecurity crises.
BSI	Bundesamt für Sicherheit in der Informationstechnik; the German Federal Office for Information Security.
BSPA	The Dutch Baseline Security Product Assessment.
CAB	Conformity Assessment Bodies (please see below the definition).
C-ITS	Cooperative Intelligent Transport Systems.
CEF	Connecting Europe Facility.
Certification	The formal evaluation of products, services and processes by an independent and accredited body against a defined standard and the issuing of a certificate indicating conformance.
CERT(s)	Computer Emergency Response Team(s).
CERT-EU	This is a Computer Emergency Response Team CERT-EU for the EU institutions, agencies and bodies.

<b>Term or acronym</b>	<b>Meaning or definition</b>
CII(s)	Critical Information Infrastructure(s).
Common Approach on decentralised agencies	Joint Statement of the European Parliament, the Council of the European Union and the European Commission on decentralised agencies – Common Approach – 2012.
Common Criteria (CC)	The Common Criteria for Information Technology Security Evaluation (commonly known as CC) is an international standard (ISO/IEC 15408) for computer security evaluation. It is based on third party evaluation and envisages 7 evaluation assurance levels. The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that CC certificates are recognized by all the signatories of the CCRA.
Communication on the DSM Strategy Mid-term Review	Commission Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy – COM (2017) 228.
Conformity assessment	The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.
Conformity assessment bodies	A body that performs conformity assessment activities including calibration, testing, certification and inspection.
CPA	Commercial Product Assurance.
cPPP	Contractual Public-Private Partnership on cybersecurity, signed by the European Commission and the European Cyber Security Organisation (ECSO) on 5 July 2016.
Critical infrastructure	‘Critical infrastructure’ means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (as defined by Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection).
CSIRT	Computer Security Incident Response Team.
CSPN	Certification Sécuritaire de Premier Niveau.
Cybersecurity	Cybersecurity comprises all activities necessary to protect network and information systems, their users and other impacted persons from cyber risks and threats.
Cyber Europe	ENISA manages the programme of pan-European exercises named Cyber Europe. This is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States.

<b>Term or acronym</b>	<b>Meaning or definition</b>
DSM Strategy	Commission Communication – A Digital Single Market Strategy for Europe – COM/2015/0192.
EAL	Evaluation Assurance Level.
EASA	European Aviation Safety Agency.
EC3	European Cybercrime Centre at Europol.
ECCB	European Cyber-certification Group proposed by Option 3 regarding certification.
ECSM	European Cyber Security Month.
ECSO	European Cybersecurity Organisation. It is an umbrella organisation whose members include a wide variety of stakeholders such as large companies, SMEs and start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State’s local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.
EDA	European Defence Agency.
EEA	European Economic Area.
EECC	Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM/2016/0590 final - 2016/0288 (COD).
EFTA	European Free Trade Association.
eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
ENISA	European Union Agency for Network and Information Security.
ENISA Regulation	Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.
EU Cybersecurity Strategy	Joint Communication of the European Commission and the European External Action Service: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN(2013).

<b>Term or acronym</b>	<b>Meaning or definition</b>
European Agenda on Security	Commission Communication – The European Agenda on Security COM(2015) 185.
Evaluation / Evaluation report	<p>Evaluation is an assessment of the effectiveness, efficiency, coherence, relevance and EU added-value of one single EU intervention. The Roadmap informs about evaluation work and timing.</p> <p>An evaluation report (SWD) is prepared by the lead service and presents the findings and conclusions about the evaluation. The quality of major evaluation reports is checked by the Regulatory Scrutiny Board against the requirements of the relevant guidelines prior to publication and/or transmission to the Legislator as part of a formal report from the Commission.</p>
Framework Directive for Electronic Communications	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC and Regulation 544/2009.
H2020	Horizon 2020.
IACS	Industrial automation control systems.
ICT(s)	Information and communications technologies.
ICT Security Certification	The various documents submitted in and with the Impact Assessment reflect different actors as well as different publication dates. Therefore, several terms are used which are largely inter-changeable. In this case, the terms ‘cybersecurity certification’ and ‘security certification’ have also been used frequently.
Impact	In an impact assessment process, the term impact describes all the changes which are expected to happen due to the implementation and application of a given policy option/intervention. Such impacts may occur over different timescales, affect different actors and be relevant at different scales (local, regional, national and EU). In an evaluation context, impact refers to the changes associated with a particular intervention which occur over the longer term.
Impact Assessment / Impact Assessment report	<p>Impact Assessment is an integrated process to assess and to compare the merits of a range of policy options designed to address a well-defined problem. It is an aid to political decision making not a substitute for it. The Roadmap informs whether an impact assessment is planned or justifies why no impact assessment is carried out.</p> <p>An impact assessment report is a Staff Working Document (SWD) prepared by the lead service which presents the findings of the impact assessment process. It supports decision making inside of the Commission and is transmitted to the Legislator following adoption by the College of the relevant initiative. The quality of each IA report is checked by the Regulatory Scrutiny Board against the requirements of the relevant guidelines.</p>



<b>Term or acronym</b>	<b>Meaning or definition</b>
Implementation	Implementation describes the process of making sure that the provisions of EU legislation can fully enter into application. For EU Directives, this is done via transposition of its requirements into national law, for other EU interventions such as Regulations or Decisions other measures may be necessary (e.g. in the case of Regulations, aligning other legislation that is not directly touched upon but affected indirectly by the Regulation with the definitions and requirement of the Regulation). Whilst EU legislation must be transposed correctly it must also be applied appropriately to deliver the desired policy objectives.
Incident	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.
Initiative	An initiative is a policy instrument prepared at EU level to address a specific problem or societal need. An impact assessment will assess options to inform the policy content of the initiative.
Intervention	Intervention is used as umbrella terms to describe a wide range of EU activities including: expenditure and non-expenditure measures, legislation, action plans, networks and agencies.
IPCR	Integrated Political Crisis Response
ISACs	Information Sharing and Analysis Centres.
JRC	Joint Research Centre.
MS(s)	Member State(s).
Network and information systems	Network and information systems (as defined by article 1 of Directive (EU) 2016/1148 – the "NIS Directive") mean: "(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance"
NIS	Network and information security.
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

<b>Term or acronym</b>	<b>Meaning or definition</b>
PSD2 (Payment Service Directive 2)	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
PSG	Permanent Stakeholder Group of ENISA.
R&D	Research and Development.
R&I	Research and Innovation.
Ransomware	A ransomware is a type of malicious software that infects the computer systems of users and manipulates the infected system in a way that the victim cannot (partially or fully) use it and the data stored on it. The victim usually receives a request to pay a ransom to regain full access to system and files.
Security	All aspects related to defining, achieving, and maintaining data confidentiality, integrity, availability, accountability, authenticity, and reliability. A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way.
SME(s)	SME(s) is the abbreviation for micro, small and medium-sized enterprises (SMEs). SMEs are defined in Commission Recommendation 2003/361 as enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.
SOG-IS	Senior Officials Group – Information Systems Security.
SOG-IS MRA	Senior Officials Group – Information Systems Security Mutual Recognition Agreement of Information Technology Security Certificates.
Stakeholder	Stakeholder is any individual or entity impacted, addressed or otherwise concerned by an EU intervention.
Standardisation	A voluntary, multi-stakeholder process aiming to develop these technical specifications that respond to legal, business, or societal requirements. The parties involved in standardisation usually include enterprises, users, standards organizations and governments.
Threat	Any circumstance or event with the potential to adversely impact an asset, system or part thereof through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
TFEU	Treaty on the Functioning of the European Union.
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable compromising the security of the computer system, network, application, or protocol involved.

## 1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

Since 2013, when the first EU Cybersecurity Strategy<sup>1</sup> was adopted and the Regulation (EU) No 526/2013 set out the current mandate and tasks for European Union Agency for Network and Information Security (ENISA), the challenges related to cybersecurity<sup>2</sup> have significantly evolved alongside with technology and market developments.

Since then, cybersecurity and cybercrime have been included in the Commission political priorities on the **Digital Single Market Strategy**<sup>3</sup> (DSM) and in the **European Agenda on Security**<sup>4</sup>. The EU agencies, in particular **ENISA** and the **European Cybercrime Center** (EC3) at Europol, have been in the frontline in terms of supporting the EU response to cybethreats, for example by providing information on the threat landscape, supporting Member States in building their capabilities and providing operational and analytical support to Member States' investigations.

Following up from the 2013 strategy, two cornerstones for European cybersecurity were adopted in 2016: the **Directive on security of network and information systems**<sup>5</sup>, (the 'NIS Directive') and the **contractual public-private partnership on cybersecurity**<sup>6</sup> between the EU and the European Cybersecurity Organisation (ECSO)<sup>7</sup>.

These developments are helping to further build-up the EU's cybersecurity resilience.

### **Box 1 – The Directive on Security of Network and Information Systems (NIS Directive)**

Adopted in 2016, the NIS Directive aims at ensuring a high common level of cybersecurity in the EU. The Directive builds on three main pillars aiming to ensure:

1. Member States (MS) **preparedness** by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
2. **Cooperation** among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks.

<sup>1</sup>Joint Communication of the European Commission and the European External Action Service: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013).

<sup>2</sup> Cybersecurity comprises all activities necessary to protect network and information systems, their users and other impacted persons from cyber risks and threats.

<sup>3</sup> Commission Communication - A Digital Single Market Strategy for Europe - COM/2015/0192

<sup>4</sup> Commission Communication - The European Agenda on Security COM(2015) 185

<sup>5</sup> Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

<sup>6</sup> Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation - C(2016) 4400.

<sup>7</sup> ECSO is an umbrella organisation whose members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as MS's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries

3. A **culture of security** across sectors which are vital for our economy and society and moreover rely heavily on ICTs. Businesses that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. These sectors include **energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure**. Also key **digital service providers** (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive. Similar requirements already apply to telecom operators and internet service providers through the EU telecoms regulatory framework.

ENISA is expected to play an important role in the implementation of the NIS Directive. In particular, the Agency provides the secretariat to the CSIRT network, which is the cornerstone of operational cooperation, and it is also called to assist the Cooperation Group in the execution of its tasks. In addition, the Directive requires ENISA to assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practices.

### **Box 2 – The contractual public-private partnership on cybersecurity (cPPP)**

The cPPP was one of the key initiatives announced in the 2015 Digital Single Market Strategy.

The partnership was signed on 5 July 2016 by the Commission and the European Cyber Security Organization (ECSO).

The goal of this partnership is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions.

The initiative leverages EU, national, regional and private efforts and resources - including research and innovation funds - to increase investments in cybersecurity. The partnership is supported by EU funds coming from the Horizon 2020 Research and Innovation Framework Programme (H2020) with a total investment of up to €450 million until 2020.

Nevertheless, cyberattacks are increasing at an alarming pace. The latest example of a ransomware<sup>8</sup> cyber-attack in May 2017 shows the potentially massive impact of a cyber-attack across sectors and countries: more than 150 countries and over 230,000 systems were affected, including those related to essential services such as hospitals, despite the damage being contained this time in comparison to the potential (deeper) consequences it may have had<sup>9</sup>. This example is just the last of a series: more than 4,000 ransomware attacks have occurred every day since the beginning of 2016, a 300% increase over 2015<sup>10</sup>.

---

<sup>8</sup> A ransomware is a type of malicious software that infects the computer systems of users and manipulates the infected system in a way that the victim cannot (partially or fully) use it and the data stored on it. The victim usually receives a request to pay a ransom to regain full access to system and files.

<sup>9</sup> WannaCry Ransomware Outburst, Infonotes, ENISA, 2017 <https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst>.

<sup>10</sup> How to protect your networks from ransomware, CCIPS, 2016 <https://www.justice.gov/criminal-ccips/file/872771/download>.

The number and size of cyberattacks can affect public trust in the capacity of modern societies to ensure security and privacy, therefore undermining the very foundations of the digital economy. Moreover, the digital society is shifting from specific connected devices (computers, smartphones or wearables) to omnipresent connectivity (household items, industrial goods, etc.). By 2020 it is estimated that billions of devices, including consumer ones (televisions, refrigerators, washing machines etc.), will be connected to the internet in the EU alone.<sup>11</sup> A connected economy and society is more vulnerable to cyber threats and attacks and requires stronger defences.

In order to gain and preserve trust and security, ICT products and services need to incorporate security features directly in the early stages of their technical design and development. Customers and users need to be able to ascertain the level of security assurance of the products and services they procure or purchase. By providing specific procedures for the evaluation of security properties, formal processes such as certification play an important role in increasing trust and security in products and services. This is particularly relevant for new systems that make extensive use of digital technologies and which require a high level of security, such as connected and automated cars, electronic health, industrial automation control systems (IACS)<sup>12</sup> or smart grids.

Against this background, in the **2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry**<sup>13</sup>, the Commission encouraged Member States to make the utmost use of the voluntary cooperation schemes under the NIS Directive. The Commission announced a number of measures to further step-up cooperation mechanisms and information and knowledge sharing to increase the EU's resilience and preparedness, also taking into account large scale incidents and a possible pan-European cybersecurity crisis. In this context, the Commission announced that it would advance the **evaluation** and **review** of ENISA as an opportunity for a possible enhancement of the Agency's capabilities and capacities to support Member States in a sustainable manner in achieving cybersecurity resilience.

### **Box 3 – The European Union Agency for Network and Information Security (ENISA)**

ENISA was set up in 2004<sup>14</sup> to contribute to the overall goal of ensuring a high level of network and information security within the EU. In 2013, the Regulation (EU) No 526/2013 established the new mandate of the Agency for a period of seven years, until 2020. The Commission is required to conduct an evaluation of the Agency by 20 June, 2018 and address the possible need to modify its mandate and the financial implications of any such modification.

ENISA supports the European Institutions, the Member States and the business community in

<sup>11</sup> IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, study for the European Commission.

<sup>12</sup> DG JRC has published a report that proposes an initial set of common European requirements and broad guidelines related to cybersecurity certification of IACS components. Available at: <https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf>

<sup>13</sup> Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.

<sup>14</sup> Regulation (EC) n° 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77, 13.3.2004, p. 1.

**addressing, responding and especially preventing network and information security problems.** It does so through a series of activities across five areas identified in its strategy<sup>15</sup>:

- **Expertise:** provision of information and expertise on key network and information security issues.
- **Policy:** support to policy making and implementation in the Union.
- **Capacity:** support to capacity building across the Union (e.g. through trainings, recommendations, awareness raising).
- **Community:** foster the network and information security community (e.g. support to the Computer Emergency Response Teams (CERTs), coordination of pan-European cyber exercises).
- **Enabling** (e.g. engagement with the stakeholders and international relations).

In the course of the negotiations of the NIS Directive, the EU co-legislators decided to attribute important roles to ENISA in the implementation of the law<sup>16</sup>. As an example of the spirit of the law, recital 38 strongly links ENISA to the Cooperation Group, stating that "the respective tasks of the Cooperation Group and of ENISA are interdependent and complementary".

ENISA has its offices in Greece, the administrative seat in Heraklion (Crete) and the core operations in Athens.

In the same Communication, the Commission noted that multiple national initiatives are emerging to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Even if important, these initiatives bear the risk of creating single market fragmentation and interoperability issues. Accordingly, the Commission announced that it would work, among others, on a **possible European ICT security certification framework proposal**, to be presented by end-2017, and to assess the feasibility and impact of a European lightweight cybersecurity labelling framework.

This vision was further confirmed in the 2016 **Council Conclusions**, which acknowledged that "cyber threats and vulnerabilities continue to evolve and intensify which will require continued and closer cooperation, especially in handling large-scale cross-border cybersecurity incidents". The conclusions reaffirmed that "the ENISA Regulation is one of the core elements of an EU cyber resilience framework"<sup>17</sup>. At the same time, the Council called on the Commission "to explore the opportunity to create a cybersecurity certification scheme, while reflecting the existing effective security schemes, if relevant, with a view to proposing measures, including legislative ones".

In its Communication on the **DSM Strategy Mid-term Review of May 2017**, the Commission further specified that by September 2017 it would review the 2013 EU Cybersecurity Strategy to address the risks faced today, help improve the security in the Union and Member States and increase the confidence and trust of businesses and people in the digital economy and society. Moreover, it would review the mandate of ENISA in order to define its role in the changed cybersecurity ecosystem and develop measures on

<sup>15</sup> <https://www.enisa.europa.eu/publications/corporate/enisa-strategy>

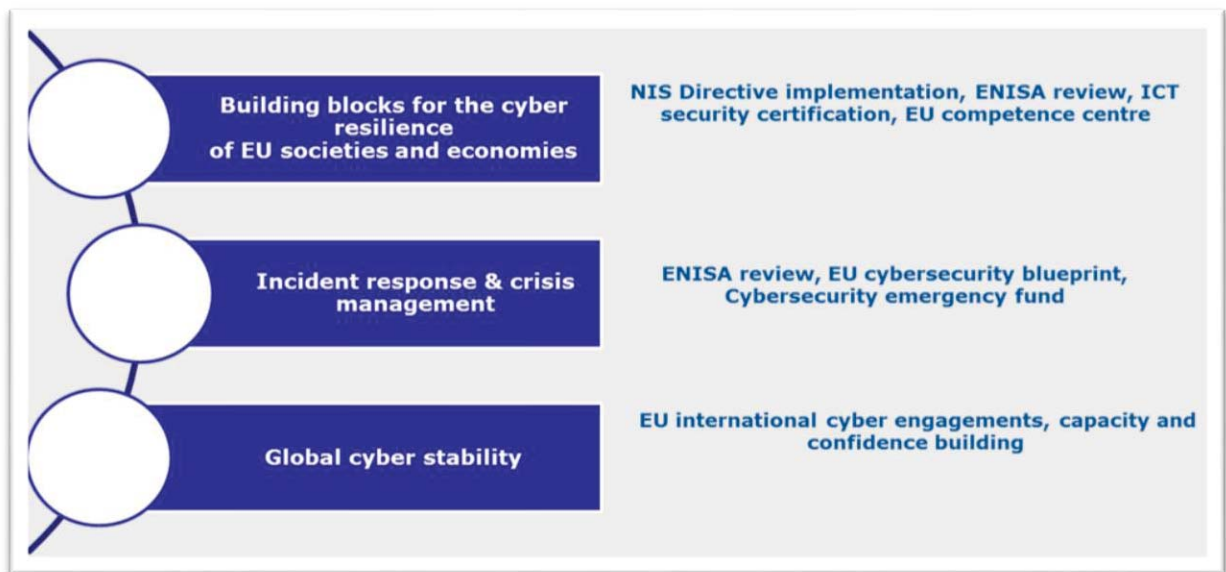
<sup>16</sup> See in particular articles 7, 9, 11, 12, 19 as well as recitals 36, 68 and 69 of Directive (EU) 2016/1148.

<sup>17</sup> Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

cybersecurity standards and certification to make ICT-based systems, including connected objects more cyber-secure.<sup>18</sup> This approach has been endorsed by the **European Council** in June 2017, which welcomed the Commission's intention to review the Cybersecurity Strategy in September and to propose further targeted actions<sup>19</sup>.

On this basis, the Commission is discussing a set of measures in three interrelated areas (see figure 1) as part of the Strategy's review that will be presented in the upcoming September Communication<sup>20</sup>, which sets out the vision for the EU to adopt a proactive approach to protect European prosperity, society and values through effective cybersecurity. The Communication includes actions directed to increase EU resilience, step-up response to cyber attacks, stimulate a single market for cybersecurity and cooperate globally on cybersecurity and defence.

**Figure 1 Priority areas for EU action in cybersecurity**



The initiative under assessment in this report refers specifically to the review of ENISA and the policy on ICT security certification, which are combined as they address complementary aspects forming part of the overall effort to increase harmonisation of cybersecurity policy and ensure the proper functioning of the single market. In addition, the combined analysis of policies and organisational solutions to implement these with a view of developing a single legislative proposal is a common practice at EU level. One relevant example is provided by the Regulation establishing the European Aviation Safety Agency (EASA) which at the same time covers the common rules in the field of civil aviation<sup>21</sup>. In the case of the policy on ICT security certification, ENISA has been

<sup>18</sup> Commission Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy - COM(2017) 228.

<sup>19</sup> European Council meeting (22 and 23 June 2017) – Conclusions EUCO 8/17.

<sup>20</sup> JOIN(2017) 450

<sup>21</sup> Recital 12 of Regulation (EC) No 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency: "There is a need for better arrangements in all the fields covered by this Regulation so that certain tasks currently performed at Community or national level should be carried out by a single specialised expert body. There is, therefore, a need within the

identified as the main organisation to support its implementation by virtue of ENISA being the only EU-level body with extensive experience and knowledge base in the field of security certification such as its Cloud Certification Schemes Metaframework (CCSM)<sup>22</sup> and standardisation (more details are provided in section 5.3). It can moreover present an organizational structure which ensures relevant, consistent and structured Member State input while maintaining an independent EU-level verification capacity. Bringing cybersecurity resilience and cybersecurity certification under one roof and under one Regulation would further favour efficiency gains and avoid the setting up of completely new organisational structures.

The proposed actions addressed in the present impact assessment would be part of the EU's wider resilience building efforts to be endorsed in the 2017 September Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'<sup>23</sup>, and therefore also effect the work of ENISA. More specifically, in addition to addressing the end of the Agency's current mandate and the review of its tasks and functions, the proposed Regulation would also address the role of such an Agency in the wider cybersecurity ecosystem in the EU. Building on the responsibilities conferred to ENISA by the NIS Directive, this would include its role in handling incidents for which Member States may ask ENISA for assistance and in large scale cross-border incidents referred to in the EU cybersecurity blueprint<sup>24</sup>, an initiative that is part of the September 2017 Communication<sup>25</sup>, which describes how national and Union actors should interact (cooperate and exchange information) in response to large scale cross-border cybersecurity incidents and crises within existing crisis management mechanisms such as the IPCR and ARGUS. The crisis management ecosystem as regards cybersecurity at Union level involves many actors including ENISA, CSIRTs Network, the European Cybercrime Centre (EC3) at Europol, and CERT-EU. As regards ENISA, blueprint it identifies its role and responsibilities within established crisis management procedures as well as the role it plays in the CSIRTs Network during crises.

The new Regulation would also build such a capacity that would allow ENISA to also have a role in providing assistance upon creation of an EU emergency fund<sup>26</sup> subject to the relevant legal instrument's requirements. ENISA's role would also be further enhanced and supported by the eventual creation of the European Cybersecurity Research

---

Community's existing institutional structure and balance of powers to establish a European Aviation Safety Agency (hereinafter referred to as the Agency) which is independent in relation to technical matters and has legal, administrative and financial autonomy. To that end, it is necessary and appropriate that it should be a Community body having legal personality and exercising the implementing powers which are conferred on it by this Regulation".

<sup>22</sup> See under: <https://resilience.enisa.europa.eu/cloud-computing-certification>

<sup>23</sup> JOIN(2017) 450

<sup>24</sup> In the COMM/2016/0410, the Commission announced that it would submit for consideration a cooperation blueprint to handle large-scale cyber incidents.

<sup>25</sup> JOIN(2017) 450

<sup>26</sup> The EU Cybersecurity Emergency Fund is an initiative developed in the context of the review of the Cybersecurity Strategy on the example of existing crisis mechanisms in other EU policy areas. It will provide the possibility for Member States to seek help at the EU level in case of major incident. It could be used to support, directly or indirectly, citizens, companies or public administrations hit by cyberattacks, provided that a basic level of cybersecurity protection had been in place before the incident occurred.



and Competence Centre<sup>27</sup>, bringing together a network of European centres from which ENISA could draw further competences and expertise for its functions.

## 2. PROBLEM DEFINITION

### 2.1. Overview of the findings of the evaluation of ENISA and the relevant public consultations

The present impact assessment is supported, among other sources of evidence, by the results of the ex-post evaluation of ENISA (2013-2016 period) and two public consultations related to the evaluation and review of ENISA's mandate and the contractual public-private partnership (cPPP) on cybersecurity, where a section was devoted to the topic of ICT security certification. In this paragraph a brief overview of their results is presented, while a detailed summary can be found in Annex 2, together with the results of the targeted consultation activities. References to specific results are also included throughout the document.

#### *The evaluation of ENISA*

The Commission, according to the evaluation roadmap<sup>28</sup>, assessed the **relevance, impact, effectiveness, efficiency, coherence and EU added value** of the Agency with regard to its performance, governance, internal organisational structure and working practices in the period 2013-2016. Inter alia, the results of stakeholder consultations for this evaluation suggest that ENISA's resources and mandate need to be adapted so that it can adequately support Member States to respond to the challenges of the future.

The main findings can be summarised as follows (for more see the Staff Working Document on the subject, accompanying the impact assessment).

**Table 1 Summary of results of the evaluation according to the criteria**

Evaluation criterion	Overall assessment
<b>Relevance</b>	Achieved to a large extent
<b>Effectiveness</b>	Partially achieved
<b>Efficiency</b>	Achieved to a large extent
<b>Coherence</b>	Partially achieved
<b>EU-added value</b>	Partially achieved

**Relevance:** In a context of technological developments and evolving threats and of significant need for increased network and information security (NIS) in the EU,

<sup>27</sup> The European Cybersecurity Research and Competence Centre is an initiative developed in the context of the review of the Cybersecurity Strategy. Building on the work of Member States and the Public-Private Partnership, the Centre would be the central hub of a EU network of competence centres in Member States. This network and its Centre would stimulate development and deployment of technology in cybersecurity, implementing advanced cybersecurity research and adding a central capability that provides all of Europe with latest technologies and competences. The Centre will coordinate efforts in the area of research, training and marketing, addressing civilian, industrial, government and military needs promoting innovation and industrial competitiveness.

<sup>28</sup> [http://ec.europa.eu/smart-regulation/roadmaps/docs/2017\\_cnect\\_002\\_evaluation\\_enisa\\_en.pdf](http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf)

ENISA's objectives proved to be relevant. In fact, Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. NIS continues to be a key political priority of the EU to which ENISA is expected to respond; however, ENISA's design as EU agency with a fixed-term mandate: (i) does not allow for long-term planning and sustainable support to Member States and EU Institutions; (ii) may lead to a legal vacuum as the provisions of the NIS Directive entrusting ENISA with tasks are of a permanent nature<sup>29</sup>; (iii) lacks coherence with a vision linking ENISA to an enhanced EU cybersecurity ecosystem.

**Effectiveness:** ENISA overall met its objectives and implemented its tasks. It made a contribution to increased NIS in Europe through its main activities (capacity building, provision of expertise, community building, support to policy). It showed potential for improvement in relation to each. The evaluation concluded that ENISA has effectively created strong and trustful relationships with some of its stakeholders, notably with the Member States and the CSIRT community, “acting as a neutral, independent broker at EU level and as a bridge between the strategic and operational worlds”<sup>30</sup>. Interventions in the area of capacity building were perceived as effective in particular for less resourced Member States. Stimulating broad cooperation has been one of the highlights, with stakeholders widely agreeing on the positive role ENISA plays in bringing people together. However, ENISA faced difficulties to make a big impact in the vast field of NIS. This was also due to the fact it had fairly limited human and financial resources to meet a very broad mandate. The evaluation also concluded that ENISA partially met the objective of providing expertise, linked to the problems in recruiting experts (see also below in the efficiency section).

**Efficiency:** Despite its small budget the Agency has been able to contribute to targeted objectives, showing overall efficiency in the use of its resources. The evaluation concluded that processes generally were efficient and a clear delineation of responsibilities within the organisation led to a good execution of the work. One of the main challenges to the Agency's efficiency relates to ENISA's difficulties in recruiting and retaining highly qualified experts. The findings show that this can be explained by a combination of factors, including the general difficulties across the public sector to compete with the private sector when trying to hire highly specialised experts, the type of contracts (fixed term) that the Agency could mostly offer and the somewhat low level of attractiveness related to ENISA's location, for example linked to difficulties encountered by spouses to find work. A location split between Athens and Heraklion required additional efforts of coordination and generating additional costs but the move to Athens in 2013 of the core operations department increased the agency's operational efficiency.

**Coherence:** ENISA's activities have been generally coherent with the policies and activities of its stakeholders, at national and EU level, but there is a need for a more coordinated approach to cybersecurity at EU level. The potential for cooperation between ENISA and other EU bodies has not been fully utilised. The evolution in the EU legal and policy landscape make the current mandate less coherent today.

---

<sup>29</sup> Reference to articles 7, 9, 11, 12, 19 of the Directive on Security of Network and Information Systems (NIS Directive).

<sup>30</sup> Study, Annex 5, p. 40

**EU-added value:** ENISA’s added value lie primarily in the Agency’s ability to enhance cooperation, mainly between Member States but also with related NIS communities. Indeed, “ENISA is providing significant added value to the cybersecurity activities implemented in the Member States”<sup>31</sup> There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. The added value provided by the agency varied according to the diverging needs and resources of its stakeholders (e.g. big versus small Member States; Member States versus industry) and the need for the agency to prioritize its activities according to the work programme. The evaluation concluded that a potential discontinuation of ENISA would be a lost opportunity for all Member States. It will not be possible to ensure the same degree of community building and cooperation across the Member States in the field of cybersecurity without a decentralised EU agency the picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA.

*Results of the public consultations on the contractual public-private partnership on cybersecurity (cPPP) and the ENISA evaluation and review.*

The results from the 2016 consultation on cybersecurity cPPP<sup>32</sup> on the section on certification show that:

- 50,4% (e.g. 121 out of 240) of respondents do not know whether national certification schemes are mutually recognised across EU Member States. 25.8% (62 out of 240) replied 'No', while 23.8% (57 out of 240) replied 'Yes'.
- 37,9% of respondents (91 out of 240) think that existing certification schemes do not support the needs of Europe's industry. On the other hand, 17, 5% (42 out of 240) – mainly global companies operating on the European market - expressed the opposite view.
- 49.6% (119 out of 240) of respondents says that it is not easy to demonstrate equivalence between standards, certification schemes, and labels. 37.9% (91 out of 240) replied 'I do not know', while only 12,5% (30 out of 240) replied 'Yes'.

In addition, in the context of the 2017 public consultation on the evaluation and review of ENISA, 67.5 % of respondents to the specific question (54 out of 80, of which 11 national authorities) expressed the view that ENISA could play a role in establishing a harmonized framework for security certification of ICT products and services. In terms of stakeholder coverage, the consultation provided a good and representative level of qualified input, covering relevant stakeholders ranging from operators of critical infrastructures, service providers, ICT vendors, associations from the ICT, banking or telecommunications sectors, to Member States and their cybersecurity and certification agencies. Their responses showed that stakeholders count on ENISA to continue its work and strengthen its role in the future. Some of the most supportive comments speak of it ‘becoming a central information hub’, ‘a more visible agency in the service of all Member States’, express the wish to ‘confirm and reinforce’ ENISA. Other comments highlight the need for ENISA to adapt to changing circumstances, also strengthening its

---

<sup>31</sup> Study, Annex 5, p. 92

<sup>32</sup> 240 stakeholders from national public administrations, large businesses, SMEs, microbusinesses and research bodies responded to the section on certification.

resources, or by offering ‘real-time cybersecurity warnings’ or commending the organisation of the cyber-exercises and acting as ‘energizer for the industry’ and ‘enabler of a security designed in Europe label’. With specific regard to ENISA past performances and future, the main trends emerging from the 2017 consultation are the following<sup>33</sup>:

- The overall performance of ENISA during the period 2013 to 2016 was positively assessed by a majority of respondents (74%). A majority of respondents furthermore considered ENISA to be achieving its different objectives (at least 63% for each of the objectives). ENISA’s services and products are regularly (monthly or more often) used by almost half of the respondents (46%) and are appreciated for the fact that they stem from an EU-level body (83%) and for their quality (62%).
- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU, in particular the top five (in a list of 16) were: cooperation across Member States; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation across Member States in matters related to cyber security; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks.
- A large majority (88%) of respondents considered the current instruments and mechanisms available at EU level to be insufficient or only partially adequate to address these. A large majority of respondents (98%) saw a need for an EU body to respond to these needs and among them ENISA was considered to be the right organisation to do so by 99%.

## **2.2. What is the size of the problems?**

Europeans increasingly value and rely on digital technologies. According to a recent Eurobarometer survey<sup>34</sup>, the majority of citizens think digital technologies have a positive impact on the economy (75%), on their quality of life (67%) and on society (64%).

Critical economic sectors such as transport, energy, health or finance have become increasingly dependent on network and information systems to run their core businesses. The Internet of Things (IoT), interconnecting objects between them and with people

---

<sup>33</sup> 90 stakeholders from 19 MSs replied to the consultation (88 responses and 2 position papers), including national authorities from 15 MSs, including France, Italy, Ireland and Greece, and 8 umbrella organisations representing a significant number of European organisations, for example the European Banking Federation, Digital Europe (representing the digital technology industry in Europe), European Telecommunications Network Operators’ Association (ETNO). The ENISA public consultation was complemented by several other sources, including; (i) in-depth interviews, with approximately 50 key players in the cybersecurity community; (ii) survey to the CSIRT Network; (iii) survey to the ENISA Management Board, Executive Board, Permanent Stakeholder Group.

<sup>34</sup> Attitudes towards the impact of digitisation and automation on daily life, Eurobarometer, 2017.

through communication networks<sup>35</sup>, is already a reality and it is expected to boom in the near future: a few billions of IoT connections are forecasted in the EU in 2020<sup>36</sup>.

While the growing digital connectivity brings enormous opportunities, it also exposes the economy and society to cyber threats.

Cyber-attacks are constantly on the rise. In some Member States, it has been estimated that half of all the crimes are cybercrimes<sup>37</sup>. Some of these attacks have aimed at high-profile targets, including power grids, important webmail services, central banks, telecommunications companies and electoral commissions. This is reflected also in citizens' own perception of risk: 86% of respondents to the latest Eurobarometer on the subject believe that the risk of becoming a victim of cybercrime is increasing<sup>38</sup>.

A 2016 study by PwC revealed that the number of security incidents across all industries rose by 38% in 2015, which is the biggest increase in the past 12 years, while at least 80% of European companies have experienced at least one cybersecurity incident.<sup>39</sup> In Q3 2016 alone, 18 million new malware samples were captured, i.e. an average of 200,000 per day.

Moreover, a large share of cybersecurity incidents are due to technical failures without malicious intent – deriving from products which are weak on security, to the lack of software updates or appropriate procedures – or are due to some type of human error.

Cyber incidents cause major economic damage to European businesses, undermine the trust of citizens and enterprises in the digital society and affect citizens' fundamental rights. A 2014 study<sup>40</sup> estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013; with Germany being the most affected Member States (1.6 % of GDP). A recent report, in the aftermath of the "wannacry" attack, estimated that a serious cyber-attack could cost the global economy more than \$120bn (£92bn) – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy<sup>41</sup>.

The most affected sectors are financial services, energy, technology, services, industry and defence<sup>42</sup> and, as shown in figure 2, several big attacks to critical sectors were reported in 2016.

---

<sup>35</sup> Many IoT devices are either already available or are being developed for deployment in the near future, including: sensors to better understand patterns of daily life and monitor health; monitors and controls for home functions, from locks to heating and water systems; devices and appliances that anticipate a consumer's needs and can take action to address them (e.g., devices that monitor inventory and automatically re-order products for a consumer).

<sup>36</sup> Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, IDC and TXT, study carried out for the European Commission, 2014.

<sup>37</sup> PwC, Global State of Information Security Survey, 2016.

<sup>38</sup> Special Eurobarometer 464, 2017.

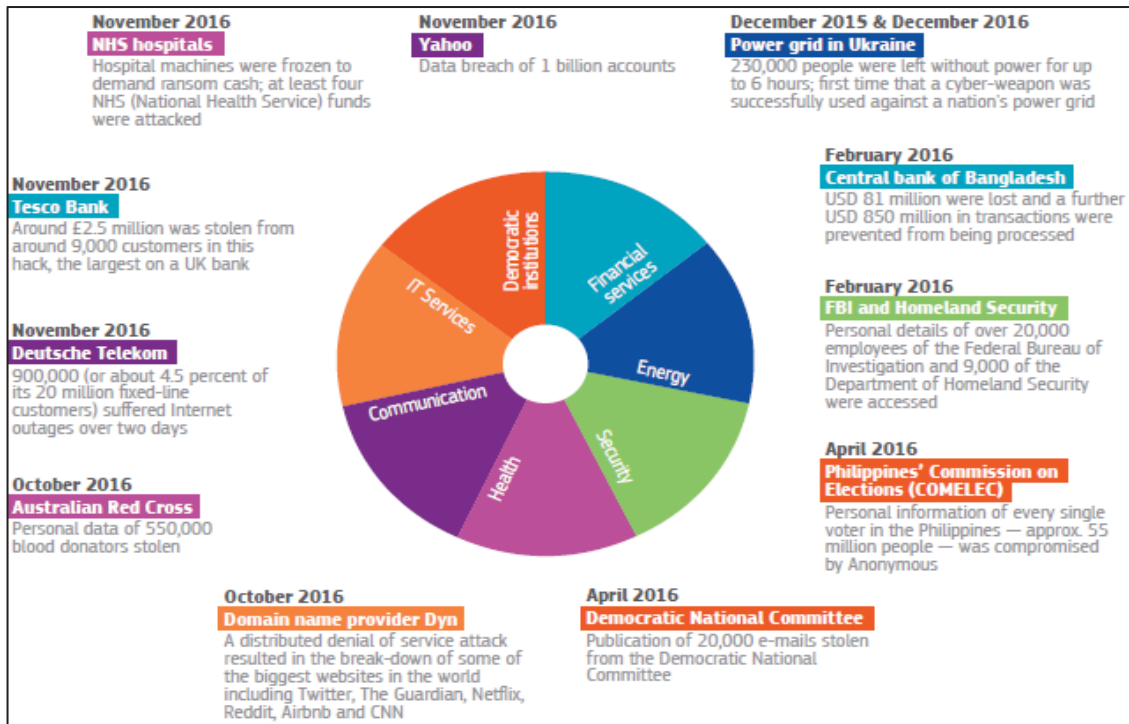
<sup>39</sup> PwC, Global State of Information Security Survey, 2016 and <http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/>

<sup>40</sup> McAfee & Center for Strategic and International Studies, 'Net Losses: Estimating the Global Cost of Cybercrime', 2014

<sup>41</sup> Counting the cost – Cyber exposure decoded, Lloyd's and Cyence, 2017.

<sup>42</sup> 2015 Cost of Cyber Crime Study: Global, Ponemon Institute October 2015.

Figure 2 Selection of significant cyber-attacks in 2016.



Source: European Political Strategy Centre, 2017

The IoT has brought new risks. This applies in particular to consumer IoT, as it can involve "non-technical" or "uninterested" consumers, who connect an increasingly wide variety of devices to their home networks. They risk losing track of which devices are connected to the Internet over time, therefore making the efforts of securing them even more challenging<sup>43</sup>. Connectable home devices, such as TVs, home thermostats or home alarms, create multiple connection points for hackers to gain entry into IoT ecosystems, access customer information, or even penetrate manufacturers' back-end systems<sup>44</sup>.

Cyber threats evolve so rapidly that strategies and tools to prevent and respond to them easily become outdated. For example, in the public consultation on ENISA review, 83% of respondents considered that the current instruments and mechanisms at European level (such as the regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) are either "partially" or only "marginally adequate" and 5% found them "not at all adequate" to promote and ensure cybersecurity.

In this context, ICT security certification is a valuable tool whose use is inadequate in the EU. All participants to a recent ENISA survey (see Annex 2) agreed on the need to leverage on certification to mitigate cybersecurity risks. In addition, 40 out of 46

<sup>43</sup> Internet of Things (IoT) Security and Privacy Recommendations, Broadband Internet Technical Advisory Group Report, 2016. Risks of IoT are linked, among the others, to: lack of IoT supply chain experience with security and privacy; lack of incentives to develop and deploy updates after the initial sale; difficulty of secure over-the-network software updates; devices with constrained or limited hardware resources (precluding certain basic or "common-sense" security measures); devices with constrained or limited user-interfaces (which if present, may have only minimal functionality), and devices with malware inserted during the manufacturing process. Internet of Things (IoT) Security and Privacy Recommendations

<sup>44</sup> Cyber risk in an Internet of Things world, Flashpoint Report, Deloitte, 2015.

respondents<sup>45</sup> to a survey aimed at SMEs think that ICT security certification is a valuable tool to reduce cyber vulnerabilities of ICT products or services (see Annex 2).

### 2.3. What are the problem drivers?

The analysis of the evidence supporting the impact assessment identified the following main drivers contributing to the problem:

- Incomplete regulatory framework, in particular as regards a coherent approach to cybersecurity policies at the EU-level. Several pieces of legislation contain provisions on cybersecurity requirements, primarily; the NIS Directive, the General Data Protection Regulation (GDPR), the current Telecoms Framework (and the related proposal for a European Electronic Communications Code), the Payment Service Directive 2 (PSD2) but also market regulation (e.g. Radio Equipment Directive). These legislative acts do not provide for an EU-wide coordinated approach on the implementation of the requirements and the guidance on the implementation is entrusted to different agencies or bodies, risking a silo-ed and in many cases sectoral approach<sup>46</sup>. This leads to fragmentation of policies and approaches across Member States and EU institutions and agencies in an area where a harmonised approach is fundamental to increase resilience and ensure the functioning of the internal market.
- Immature cooperation mechanisms. Cooperation across Member States, between public and private actors and between the national and the EU level is taking shape, although at slow pace. In particular, the NIS Directive provides for mechanisms that can stimulate cross-border cooperation at least on a voluntary basis. However, these measures are only starting to take place. Furthermore, the shift in culture towards cooperation in an area close to national security takes time to progress especially at EU level, where cooperation takes place mostly on an ad-hoc basis or according to bilateral agreements between different actors. The low degree of development of cooperation mechanisms has a direct impact on the fragmentation of the policies and the approaches to cybersecurity across Member States and across the EU institutions, agencies and bodies.
- Lack of EU-wide reliable data and analyses. There is little information and independent analyses on key cybersecurity issues (such as the economics of cybersecurity, reliable trends of expected new challenges, the best solutions to face threats or criminal statistics related to cybercrime<sup>47</sup>) covering the whole EU. This applies in particular to the cybersecurity incidents. The incident reporting requirements of the GDPR, the NIS Directive and as well as other similar requirements stemming from other pieces of legislation<sup>48</sup>, should somehow

---

<sup>45</sup> 4 replied "no", 2 replied "don't know"

<sup>46</sup> For example in the PSD2 it is the European Banking Authority, in the GDPR the Data Protection Board in the Telecoms Framework it is ENISA, in energy sector ACER, in aviation EASA etc.

<sup>47</sup> Article 14 of the Directive on attacks against information systems (2013/40/EU) requires the collection of statistics on the offences described in the Directive, and their transmission to the Commission. In 2015, the Commission published the results of an exploratory data collection on criminal statistics on cyber-attacks (based on the offences covered in the Directive on attacks against information systems): <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=21219&no=6>

<sup>48</sup> For example, the PSD2, the Regulation on electronic identification and trust services for electronic transactions in the internal market - eIDAS, the recent proposal from a European Electronic Communications Code.

improve the situation, but primarily at the national level as notifications are to be addressed to the national authorities. This is insufficient for the EU needs and it leads to fragmentation of policies and approaches across the Member States and EU institutions, and to insufficient awareness and information of citizens and companies. In particular, companies that are present in more than one Member State, EU-level regulators or even national regulators in sectors with significant cross-border dependencies, need to be aware of the situation in the entire EU if they want to make reliable risk-based decisions or take appropriate measures. The lack of EU-wide reliable data also impacts the cybersecurity industry's ability to design products that would meet the requirements of companies and citizens across the whole EU.

- Limited efficiency and suitability of current certification mechanisms: The main mutual recognition instrument in Europe - the SOG-IS MRA - has a number of shortcomings. It only includes twelve Member States plus Norway and has developed only a few protection profiles regarding certain digital products (such as digital signatures, digital tachograph and smart cards). Furthermore, SOG-IS MRA is based on the methodology of Common Criteria (CC), which is criticised for the long duration of process and high costs, among others<sup>49</sup>. CC envisages seven Evaluation Assurance Levels (EAL), with one being the lowest-level evaluation and seven being the highest-level one<sup>50</sup>. It has been estimated that a CC certificate for the lowest level of assurance can be obtained in about six months at a cost of around EUR 20,000. A higher assurance level certificate (e.g. EAL 4) for an ICT product can take one to two years, and, often, by the time the process is completed a new version of that product is already delivered<sup>51</sup>. According to the smart metering industry, CC certification is the most expensive (not less than EUR 500,000) among the various certifications they have to provide. Governments and industry have taken actions to develop more agile certification schemes. However, the use of these schemes is occurring in an uncoordinated way. As a result, manufacturers of products such as smart meters would typically need to apply for different certification schemes or comply with different security requirements across the EU. The duration of each certification process for these products can take from six months to one year. These initiatives acknowledge the importance of ICT security certification and are in line with the objective of mainstreaming cybersecurity in the EU policy making. However, they can also lead to dispersed resources and diverging approaches to cybersecurity if the initiatives across different policy domains are not, as it currently is the case, sufficiently coordinated.
- Insufficient and uneven resources allocated at national and EU level, is a driver for all three problems outlined in figure 3. Only in recent years has cybersecurity acquired a status of important policy where both governments and companies have decided to invest and yet, as presented above, it is still very difficult to estimate the return on such investments, sometimes making the choice to allocate resources difficult. The differences in the resources available across organisations, Member States and EU institutions impact directly the level of capabilities and preparedness of Member States, the EU capacity to complement

---

<sup>49</sup> For a description of criticism to CC, see pp 24-26 of the JRC study (Annex 8).

<sup>50</sup> An EAL defines how thoroughly the product is tested.

<sup>51</sup> <http://www.eurecom.fr/en/publication/4438/download/rs-publi-4438.pdf>



the action of Member States and the information made available to citizens and businesses. Furthermore, in the context of the budgeting policies of each organisation, limited resources also hamper the possibility to invest as needed in the cooperation and coordination mechanisms, leading to an overall insufficient cooperation and coordination across Member States and EU institutions.

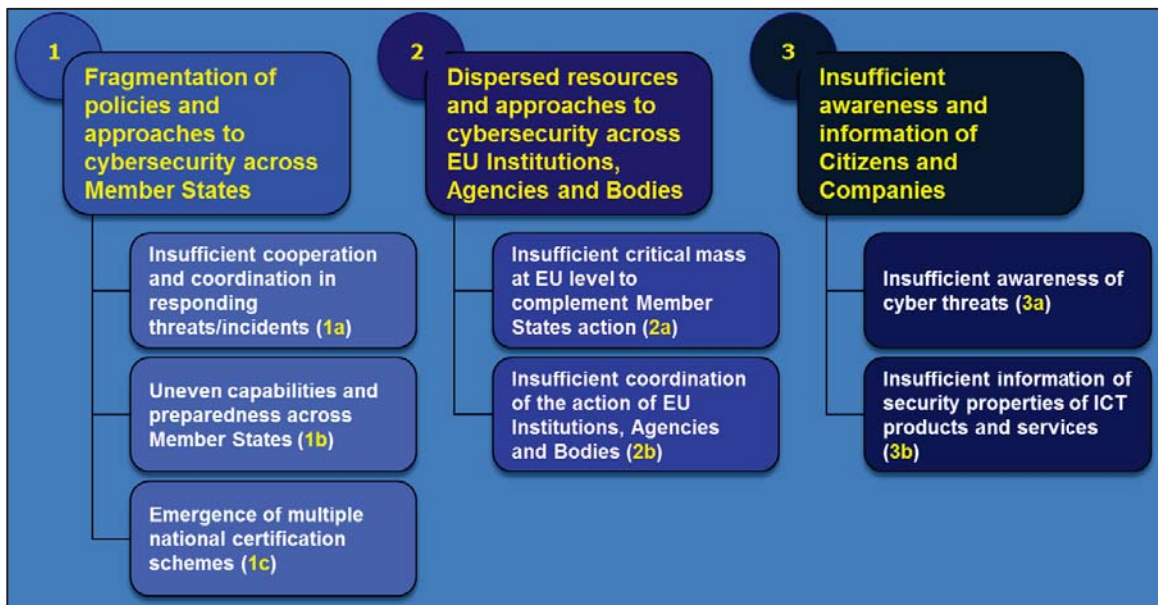
- Insufficient education and awareness programmes. The lack of adequate education and awareness programmes, together with the lack of sufficient data and analyses, leads to the insufficient awareness of cyber threats. There is not such a culture of embedding basic measures of cybersecurity among the key learnings for the citizens of the digital society and the pace at which people become aware of cyber threats and possible remedies is much slower than the one at which they embrace technological innovations.

#### **2.4. What are the problems for action?**

Within the broader course of action defined by the review of the EU cybersecurity strategy, and within the limits of the available instruments, the present initiative aims to **contribute to tackling** the following **interrelated problems**:

- **Fragmentation** of policies and approaches to cybersecurity across the **Member States**. This problem, highlighted by stakeholders (see Annex 2 presenting results of stakeholders' consultation), covers several aspects that are under remit of ENISA (support to cooperation among Member States, EU level capabilities to support Member States, coordination between the EU bodies, support in implementation of legislation) and specifically the policy on certification (emergence of multiple national certification schemes and initiatives that are not recognised across EU in a coherent manner).
- **Dispersed resources and approaches** to cybersecurity of the **EU institutions, agencies and bodies**.
- Insufficient **awareness** among citizens and companies of **cyber threats and insufficient information concerning the security properties of ICT products and services** they purchase.

Figure 3 Problems to tackle

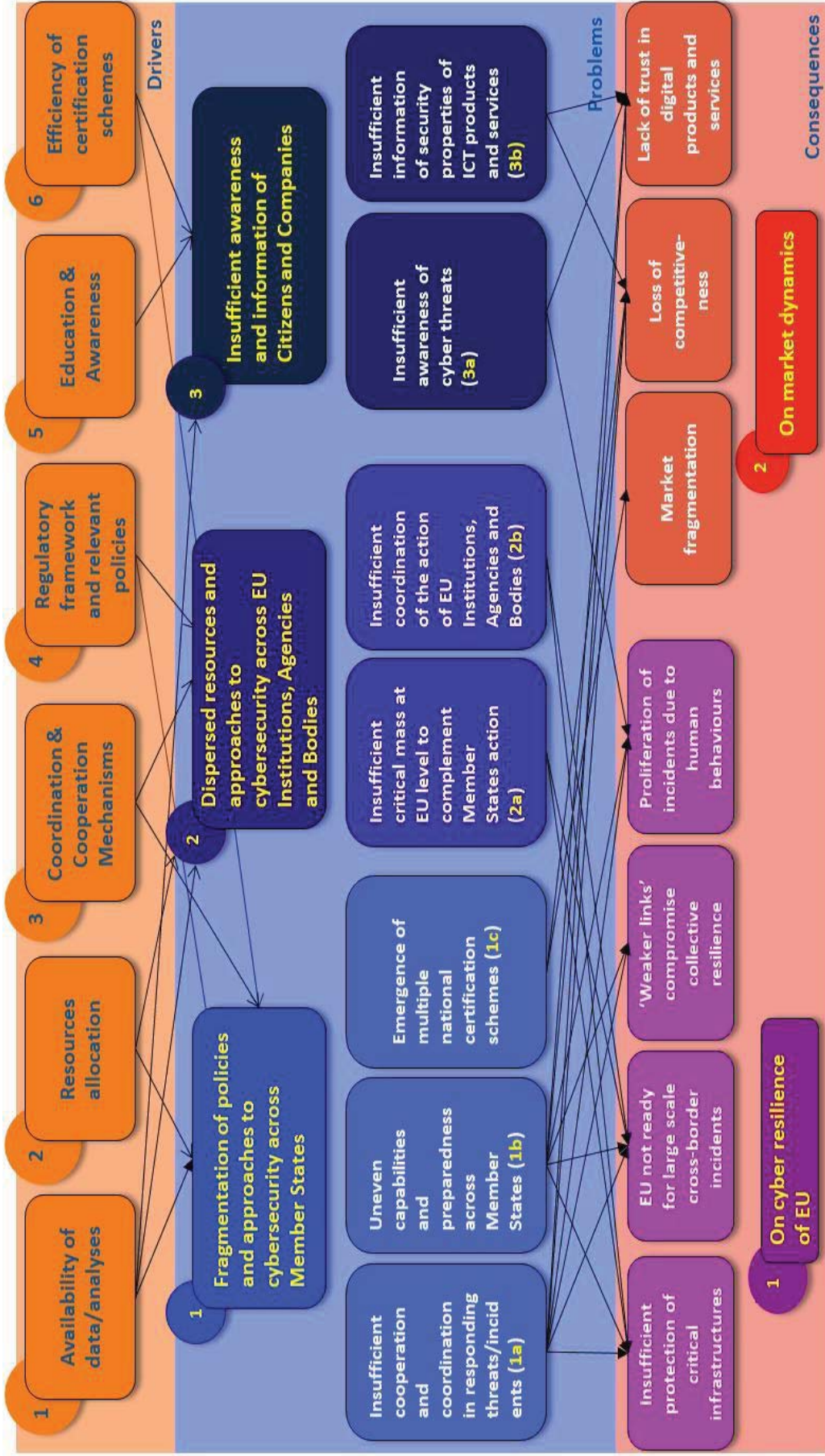


The three problems in turn lead to a series of consequences related to cyber resilience and market dynamics (see also figure 4):

- **Cyber resilience:** The fragmentation of policies and approaches at both national and EU level, together with a continuing lack of awareness of cybersecurity issues among individuals and organisations lead to the insufficient protection of critical infrastructures, the potential proliferation of incidents due to human behaviour, the exposure of the whole system to the effects of incidents due to "weaker links" in other words less equipped parts, and to a lack of preparedness of the EU to face large scale cross-border incidents.
- **Market dynamics:** The emergence of multiple national certification schemes which are not recognised throughout the EU may lead to single market fragmentation and - due to the fact that ICT vendors might need to undergo several certification processes to be able to sell in several Member States - a loss of competitiveness for the businesses, in particular for SMEs. The lack of information on security properties of ICT products and services in a context of growing cyber threats undermines the trust of users (both citizens and businesses) in digital products and services.

The impact of each sub-problem on the cyber resilience and the market dynamics are explained more in detail in the following sections.

Figure 4 Problem Tree



#### 2.4.1. Problem 1: Fragmentation of policies and approaches to cybersecurity across Member States

*Problem 1.a: Insufficient cooperation and coordination in responding to cyber threats and incidents.*

Cybersecurity is a truly global issue, which is cross-border by nature and is becoming increasingly cross-sector due to the interdependencies between networks and information systems. The impact of incidents that affect one organisation can easily spread to others and the same logic applies to countries.

**When it comes to attacks**, as shown in several cases including the most recent ransomware campaign, **the perpetrators often tend to collaborate** internationally by sharing information, building their intelligence collectively and rapidly responding to possible counter-measures from the victims.

Despite some progress made in the past years, **the Commission cannot see the same level of cooperation and coordination on the side of public authorities and businesses** in the EU.

Since its establishment in 2004, ENISA has aimed to foster cooperation between Member States and the NIS stakeholders, including through the support of public-private cooperation. This included the technical work to provide an EU-wide picture of the threat landscape<sup>52</sup>, the setting-up of expert groups and the organisation of pan-European cyber incident and crisis management exercises for public and private sectors exercises (in particular "Cyber Europe"<sup>53</sup>).

The 2016 NIS Directive is a key step in building trust between Member States to stimulate information sharing, mutual learning and shared approaches to risk management. However, the scope of the NIS Directive is not all-encompassing (see table 2) and does not cover some of the key areas this initiative is addressing. To do this would require specific measures that complement the NIS Directive (see description of the preferred option in section 8).

**Table 2 Scope of NIS Directive in relation to key areas**

Areas	NIS- Directive scope
<b>Cooperation</b>	It created a framework for cooperation where there was none before (Cooperation Group <sup>54</sup> and CSIRT <sup>55</sup> Network <sup>56</sup> ). Cooperation is voluntary only

<sup>52</sup>Since 2012, ENISA has developed the ENISA Threat Landscape (ETL), as a series of deliverables with the yearly threat landscape report being the major publication.

<sup>53</sup>ENISA developed a cyber-exercise capability that is able to train the EU cyber response teams to deal with crisis scenarios. Cyber Europe is the main cyber exercises of the European Union, engaging more than one thousand participants from the public and the private sector, taking place every 2 years since 2010.

<sup>54</sup> The Cooperation Group is composed of representatives of all MSs, the Commission and ENISA and aims to foster strategic cooperation.

<sup>55</sup>CSIRT stands for Computer Security Incident Response Team. Tasks of a national CSIRTs (as per Annex I of NIS Directive) include: monitoring incidents at a national level; (ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and

	and no specific target was set for both the strategic and operational levels (level of ambition depends on work plans adopted by Member States)
<b>Security Requirements and Reporting Obligations</b>	For the first time, the NIS Directive introduced obligations on operators of essential services (OES) and digital service providers (DSPs) to take security measures and notify significant incidents. The security requirements placed on digital service providers (DSPs) are determined at EU level; for the operators of essential services (OES) each Member State may set its own requirements. The incident reporting obligations foresee that notifications are to be addressed to the national authorities.
<b>Sectors</b>	Not all sectors are covered (e.g. public administration) and for the sectors that are covered (energy, transport, water, healthcare, financial market infrastructure, banking) there is no specific mechanism to ensure consistency of policy approaches in areas with different level of cyber maturity (e.g. healthcare much less developed than finance and banking).
<b>Large scale cross-border incidents and Crisis management</b>	Not addressed
<b>ICT security certification</b>	Not addressed and there is no provision that stimulates increased security of ICT products and services (e.g. for digital devices and services or connected objects).
<b>EU level action</b>	No mechanism is foreseen to ensure better coordination of EU institutions, agencies and bodies and increase EU operational capabilities.

Better and more technical support at the EU level is also needed to help bridge the existing gaps, for example regarding the availability of reliable data and analyses on threats and incidents and of EU-wide good practices, in particular in critical sectors.

The lack of an adequate EU-wide technical support and the differences in the approaches to cybersecurity standards make it difficult to establish common baselines and security requirements, for instance, to reduce cost burdens on businesses which operate cross-border.

It is furthermore becoming clear that a variety of requirements for security certification are emerging at both the national and regional level. For example at a national level, although VPN<sup>57</sup> products are usually certified against international “collaborative”

---

incidents; (iii) responding to incidents; (iv) providing dynamic risk and incident analysis and situational awareness.

<sup>56</sup> The CSIRT Network, brings together CSIRTs from all MSs and CERT-EU (the Computer Emergency Response Team for the EU institutions, bodies and agencies) with the aim to foster operational cooperation. ENISA provides the secretariat to the CSIRT Network.

<sup>57</sup> Virtual Private Network

protection profiles (cPP)<sup>58</sup>, vendors wanting to access the French market are typically requested to obtain an additional CSPN certification (see box 4). This process takes from six to nine months and it costs around EUR 80,000. Security products such as Hardware Security Module (HSMs) and/or the cryptographic modules they employ are typically certified to internationally recognized standards such FIPS. However, SOG-IS members request an additional CC certificate with a related vulnerability analysis. At a regional level, an Italian local public authority<sup>59</sup> had for example issued requirements in a public procurement procedure for security certification of a video surveillance system according to Common Criteria<sup>60</sup> (CC) at a low assurance level (EAL 1). It has been estimated that such a certification process takes 6 months and costs around EUR 20,000 (see Annex 7). In the absence of common ICT security requirements, authorities may decide both at which level such products should be tested and indeed whether such products should be tested at all, again leading to a situation of fragmentation and uncertainty within the EU.

Furthermore, existing mechanisms for cooperation on operational matters, in particular on detection and response to cybersecurity incidents are still limited and often restricted to close circles of CSIRTs. Despite good results in ‘simulation mode’, especially in the context of Cyber Europe exercises, and the initial work of the CSIRT Network, the EU is lacking a coordinated approach in case of cross-border incidents and it is today not prepared to handle a potential cybersecurity crisis, such as simultaneous attacks on critical information systems in several Member States.

The type of gaps and developments described above were confirmed by the results of the recent stakeholder consultations (see table 3 below and for more details Annex 2), in particular the public consultation. Here – notwithstanding the adoption of the NIS Directive – cooperation at different levels, including public-private cooperation, and the capacity to prevent and handle large scale cyber-attacks are still perceived as the most urgent gaps in the EU.

---

<sup>58</sup> cPP is a Protection Profile developed by international technical communities

<sup>59</sup> Provincia di Trento

<sup>60</sup> The Common Criteria for Information Technology Security Evaluation (commonly known as CC) is an international standard (ISO/IEC 15408) for computer security evaluation. It is based on third party evaluation and envisages 7 Evaluation Assurance Levels (EAL). The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that CC certificates are recognized by all the signatories of the CCRA. Within the current version of CCRA only evaluations up to EAL 2 are mutually recognized.

**Table 3 Most urgent gaps and needs, as emerging from the stakeholder consultations**

<b>Most urgent gaps and needs in the cyber security field in the EU</b>
Cooperation across Member States in matters related to cybersecurity
Capacity to prevent, detect and resolve large scale cyber-attacks
Cooperation and information sharing between different stakeholders, including public-private cooperation
Protection of critical infrastructure from cyber-attacks
Research, knowledge and evidence to support policy action

In addition, there are still gaps in the cooperation and information-sharing mechanisms both within the private sector, as well as between public and private actors. For example, the role of industrial players in collecting, analysing and disseminating information on cyber threats is essential, but the emergence of proper Information Sharing and Analysis Centres (ISACs) as a two-way information sharing resource between the private and public sector to support the protection of critical infrastructures is only a recent phenomenon in the EU. Closing the cooperation gap along these lines should be further stimulated both within sectors and across different sectors.

*Problem 1.b: Uneven capabilities and preparedness across Member States*

The persistence of gaps between Member States in terms of their cybersecurity capabilities and thus their preparedness in facing cybersecurity challenges is a longstanding issue that requires continuous attention. Today, considerable discrepancies can still be observed between Member States' cybersecurity policies, legal frameworks and operational capabilities<sup>61</sup>. As a consequence, the effectiveness of the measures taken at national level by one or a few Member States can be affected by the lower level of protection in another Member State, potentially resulting in a 'contagion' effect in case of serious disruptions affecting the 'weakest links' in the EU community.

The implementation of the NIS Directive will introduce some common requirements for the minimum capabilities in each Member State; namely a national strategy, a CSIRT and a NIS competent national authority. However, it is clear that Member States cannot count on the same level of resources, experience and risk management culture, which impacts directly on their level of preparedness<sup>62</sup>. For example, while most Member States have established operational entities, such as CSIRTs, the mission and the experience of those entities vary greatly. Also, only about half of the Member States are currently

<sup>61</sup> Global Cybersecurity Index & Cyberwellness Profiles, ABI Research and ITU, 2017. In the Global Cybersecurity Index, the countries are assessed based on five criteria: legal measures, technical measures, organisational measures, capacity building, and cooperation. The EU MSs present quite diverging scores, ranking in the global list from the 5<sup>th</sup> to the 84<sup>th</sup> position.

<sup>62</sup> Cybersecurity in the European Digital Single Market, High Level Group of Scientific Advisors, Scientific Opinion No. 2/2017.

conducting national cybersecurity exercises. Similarly, in the area of security certification, a clear gap of capabilities (e.g. in terms of expertise and conformity assessment bodies) can be noticed across Member States, thus maintaining an uneven level of preparedness.

Another significant gap is the different approach to collaboration between governments and the private sector, including those operating critical infrastructures. While the role of the industry is key in responding to cybersecurity challenges, only a few Member States have mature frameworks for public-private partnerships<sup>63</sup> in place.

In this area, the conclusions of the ex-post evaluation of ENISA present both positive and negative aspects. An overall positive assessment of the Agency emerges when it comes to meeting its objective of supporting Member States' capacity building. This is mainly due to the trainings provided and to the support in developing national strategies, but also by ENISA acting as a 'broker' of national good practices<sup>64</sup>.

However, Member States have different needs and expectations when it comes to ENISA support especially on capacity building. While the most equipped ones rely little on the Agency, the less resourced or experienced Member States would need increased support, including for detection and response to cybersecurity incidents<sup>65</sup>.

#### *Problem 1.c: The emergence of multiple national and sectoral certification schemes*

The rise of cybercrime and security threats has resulted in national initiatives setting high-level cybersecurity and certification requirements for ICT components including those used in traditional infrastructure. While products and services - for which a mandatory certification is not required - can still circulate in the internal market, the emergence of these national initiatives bears the risk of creating market fragmentation and erecting barriers for interoperability. In the absence of mutual recognition mechanisms among these schemes, one possible consequence would be that an ICT vendor needs to undergo several certification processes to be able to sell the same products or service in several Member States.

For example, the technical study that supports this impact assessment shows that smart meter manufacturers comply with three different certification schemes in three European countries. These are CPA in the UK, CSPN in France (see box 4 for a description of the schemes), and a specific protection profile based on CC in Germany. The overall cost of these certifications is about EUR 1 million, which in particular penalises small and medium sized enterprises (SMEs). This is an additional barrier to market entry. For example, in Germany, only one of the biggest smart-metering companies is embarking on various certification processes to enter other markets, all the other companies are only present in the German market.

As the reliance on digital devices increases, requirements for ICT security are expected to proliferate and cover a wide range of products and services. In the worst case, an ICT

---

<sup>63</sup> EU cybersecurity dashboard, BSA, 2015.

<sup>64</sup> In particular with regard to training to CSIRTs, ENISA has delivered 114 courses during 2014-2017. In relation to national strategies, since 2013 ENISA has produced good practice guides on how to create and evaluate a strategy and it has run an experts group with the goal of information exchange on strategies lifecycle phases. It has furthermore directly supported 5 MSs in creating their strategy.

<sup>65</sup> For more information see the Staff Working Document on ENISA evaluation and the related study conducted by an external contractor.



product or service designed to fulfil cybersecurity requirements in one Member State would have difficulties to enter the market of other Member States where different requirements are in place.

**Box 4 – Existing and emerging certification initiatives in the EU<sup>66</sup>**

- The **Commercial Product Assurance (CPA)** developed in the UK is an example of national scheme which applies to commercial off-the-shelf products. According to CPA, a security product that is successfully assessed is awarded Foundation Grade certification, which means that the product has been proved to demonstrate good commercial security practice and is suitable for lower threat environments. CPA is open to all vendors, developers and suppliers of security products with a UK sales base. However, there is no Mutual Recognition Agreement for CPA, which means that products tested in the UK will not normally be accepted as certified products in other markets where a similar, but still different, security certification is required. Currently, 37 products have been certified under the CPA, 15 products are currently under evaluation.
- **Certification Sécuritaire de Premier Niveau (CSPN)**- an IT Security Certification Scheme established by the National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d’information – ANSSI) in 2008. Its main purpose is to offer a faster and cheaper alternative for IT Security Certification as compared to the CC approach. Yearly, ANSSI receives around 50 submissions for certification under CSPN. The cost of each CSPN certification is in the region of 25.000 – 35.000 euro while duration of process is approximately of 3 months<sup>67</sup>. Similarly to the CPA, there is no MRA for CSPN, which means that products tested in the France will not normally be accepted in other markets.
- The **Dutch Baseline Security Product Assessment (BSPA)** scheme is intended to judge the suitability of IT security products for use in the “sensitive but unclassified” domain. The BSPA scheme is in pilot phase since 2015. The pilot is expected to end in 2017 and then the scheme will be operational. In the pilot phase

---

<sup>66</sup> A list of existing certification schemes and standards is available at Annex 11.

<sup>67</sup> Length and cost of process may vary depending on the product.

6 requests for certification were received. The average cost of a certification under BSPA is € 40.000. The overall process can take up to 2 months.

- **SOG-IS MRA**<sup>68</sup> is the main certification mechanism existing at European level. It includes twelve Member States<sup>69</sup> plus Norway and has developed a few protection profiles on digital products (such as digital signature, digital tachograph<sup>70</sup> and smart cards). Participants work together to i) coordinate the standardisation of CC protection profiles; ii) coordinate the development of protection profiles<sup>71</sup> whenever the European Commission launches a legislation that covers IT-security among others. Members can participate in the MRA as i) certificate consuming<sup>72</sup> and certificate producers<sup>73</sup>. Member States often request SOG-IS certification as a pre-condition to be admitted to national public procurement tenders.
- The German Federal Office for Information Security (BSI) is developing a baseline approach for low level assurance to improve the efficiency of CC evaluation.
- According to the support study, other emerging initiatives are being developed in Italy<sup>74</sup>, Sweden and Norway.

The risk of a proliferation of national certification initiatives increases costs for businesses operating cross-border. It would generate a low incentive for them to embark on such a cumbersome process, with an overall detrimental effect on the quality and security of ICT used in Europe. Furthermore, such fragmentation would also impact the performance of evaluators, in that only a limited number of conformity assessment bodies would be able to certify against the requirements of different schemes.

In the preliminary results of a survey aimed at SMEs (see more details in Annex 2), 18 out of 46 respondents believe that the current existence of multiple ICT certification schemes represents a barrier to market entry because they are too costly and therefore not affordable for SMEs<sup>75</sup>. A recent ENISA survey on ICT security certification (see Annex 2 for the summary results) shows that 57% of respondents (19 out of 33) are aware of multiple existing ICT security certification schemes across EU Member States for the same product or service; 37% (12 out of 33) of the respondents replied 'No' to the same

---

<sup>68</sup> The Senior Officials Group – Information Systems Security (SOG-IS) agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

<sup>69</sup> Austria, Croatia, Finland, France, Germany, Italy, Luxembourg, Netherlands, Poland, Spain, Sweden, UK

<sup>70</sup> The tachograph is a device that records the driving time, breaks, rest periods as well as periods of other work undertaken by a driver.

<sup>71</sup> A Protection Profile (PP) is a technical document that defines a standard set of security requirements for a specific type of product

<sup>72</sup> Members that only accept certificates issued by other certificate producer members but do not issue such certificates.

<sup>73</sup> Members that issue and accept SOG-IS certificates issued by other producers.

<sup>74</sup> A recent Italian decree (February 2017) promotes the establishment of a national centre for the evaluation and certification of ICT products used in critical infrastructure. Available at: <https://www.sicurezza nazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html>

<sup>75</sup> Six replied "lack of reference levels" while the rest of respondents did not know.

question, but expressed their preparedness to accept one single scheme, while 2 ‘do not know’. In the same survey, 90% (30 out of 33) of respondents agreed that mutual recognition of ICT security certification schemes is desirable at European level to address further fragmentation.

In written submissions related to the public consultation on cPPP, respondents emphasized that no reliable certification scheme exists at the moment at the European level. Others pointed to the fact that existing national schemes and security requirements act as barriers to market entry, complaining about the costs of compliance. Some of the industry associations state that further fragmentation of the market with numerous certification schemes should be avoided.

#### 2.4.2. *Problem 2: Dispersed resources and fragmentation of approaches to cybersecurity across EU institutions, agencies and bodies.*

*Problem 2.a: Insufficient critical mass at EU level to complement the action of Member States.*

Despite the importance of cybersecurity on the European agenda, there is still a **lack of cybersecurity capabilities and instruments at European level** to complement the individual efforts by Member States. Overall, the EU investment<sup>76</sup> today - including in the development and the deployment of cybersecurity technology and solutions - is below the critical mass needed to protect our economy and institutions, in particular if compared to other key international players<sup>77</sup>.

While many organisations at EU level have started to include a cybersecurity perspective in their policies and/or their operations (see next section), the European Commission has no operational capabilities, (the Europol's European Cybercrime Centre (EC3) is dealing specifically with cybercrime) and CERT-EU is responsible for the protection of the EU institutions, agencies and bodies. The only organisation with some preventive operational capabilities<sup>78</sup> and with the official mandate to contribute to the overall network and information security of the Union is ENISA.

ENISA has a broad mandate (see box 3 in section 1) but it is a rather small agency with one of the lowest budgets and number of staff compared to all EU agencies (Annex 3

---

<sup>76</sup> There is no clear picture of the investment from the MSs. The investment in cybersecurity is channelled through different programmes of the EU budget: about EUR 600 million have been invested in cybersecurity and cybercrime projects under the Horizon 2020 Framework Programme for the period 2013-2020; the European Structural and Investment (ESI) Funds foresee a contribution of up to EUR 400 million for investments in trust and cybersecurity; about EUR 30 million were invested in the period 2014-2017 for cybersecurity under the Digital Service Infrastructures (DSIs) stream within the Connecting Europe Facility (CEF); under the Instrument contributing to Stability and Peace (IcSP) cybersecurity and combatting cybercrime are a priority area since 2013 with an indicative allocation of EUR 21.5 million over the period 2014-2017.

<sup>77</sup> As an example, in the U.S.A., the Government invested over EUR 19 billion for cybersecurity as part of 2017 Budget (35% increase from 2016 in overall Federal resources for cybersecurity). Source: White House, Factsheet Cybersecurity National Action Plan.

<sup>78</sup> For example: the organisation of cyber exercises, the support to the CSIRT capacity building and the development of national cybersecurity strategies, the provision of advice to MSs (upon request) in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services.

shows the detailed figures per each agency). ENISA is also the only EU agency with a fixed-term mandate, which limits long term planning of its contribution to Member States and EU institutions. Moreover, the results of stakeholders' consultations also suggested that ENISA currently does not have sufficient resources to meet its broad mandate. Looking at the future, the mandate itself, conceived in a different political, legal, technological and threat landscape, cannot take into account more recent developments, including the tasks attributed to ENISA by the NIS Directive, and it does not sufficiently empower the Agency to respond to the forthcoming cybersecurity challenges.

In particular, the results of the evaluation of ENISA show that the agency needs to prioritize the demands of Member States and EU institutions, leaving at least partially the needs of private stakeholders and in particular industry aside. The industry on the other hand sees a potential important role for ENISA as a future link between the public and private sector. It could better support European businesses by providing high quality strategic analysis of threats, developing sector-specific expertise and ensuring harmonisation baseline requirements for cybersecurity across the EU. Industry sees ENISA focusing on future priority areas such as the Internet of Things, the move to big data and machine intelligence, certification, and envisages ENISA becoming more active in the educational field. Specifically, the large majority of stakeholders that were consulted on issues related to certification, envisage a role for ENISA in future policy developments in this area.

Looking ahead, the recently established Cooperation Group and CSIRTs Network could in the future add to the European level capacity by pooling resources, expertise and information. However, these remain subject to the limitations explained in the section above.

In particular when it comes to operational capabilities for the prevention, detection and response to cyber-incidents, there is currently no EU level capacity to guarantee the speed, accuracy, efficiency and effectiveness of response needed in a case of crisis. There is furthermore no European level system which for example covers: the early warning of threats and incidents; the ability to establish a common qualified picture in case of cross-border incidents; the capacity to handle communication with the public; and the ability to pool resources to help the victims of an attack.

Among the EU institutions, agencies and bodies, only CERT-EU has response capabilities but, as explained above, its mandate is limited to the protection of the institutions. CERT-EU also does not have 24/7 capabilities.

*Problem 2.b: Insufficient coordination of the action of EU institutions, agencies and bodies.*

The pervasiveness of digital technologies in all spheres of economy and society warrants the **mainstreaming of cybersecurity issues** into EU policies. The strategic importance of this objective, set out in the 2013 EU Cybersecurity Strategy, has been reaffirmed in the NIS Directive – that specified which organisation operating in specific ‘critical’ sectors would be subject to security and notification requirements<sup>79</sup> – and in the 2016

---

<sup>79</sup> Annex II of NIS Directive includes the following sectors: Energy: electricity, oil and gas. Transport: air, rail, water and road. Banking: credit institutions. Financial Market Infrastructures: trading venues, central counterparties. Health: healthcare providers. Water: drinking water supply and distribution.

Communication on Strengthening Cyber Resilience, which highlighted the need for continuous efforts to find cross-sectoral synergies and to mainstream cyber requirements in all relevant EU policies.

A number of instruments have already been put in place to mainstream cybersecurity issues at EU level covering: horizontal legislation, sectoral policy initiatives (e.g. in the energy and transport field), international relations, research & innovation, and EU agencies and bodies. As a consequence, many organisations in the EU ecosystem are involved and some are gaining competence in cybersecurity. Within the European Commission, two main Directorate Generals<sup>80</sup> are tasked with addressing overall cybersecurity and cybercrime; while at least eight Directorate Generals have started initiatives at sectoral level (see Annex 9 for detailed information). The European External Action Service (EEAS), which manages the EU's diplomatic relations with other countries outside the EU and conducts EU foreign & security policy, handles cyber defence as it relates to state activities and multinational or multilateral organisations (UN, NATO, OECD, etc.).

The same picture applies to EU agencies and bodies, where it is possible to identify four main actors dealing with cybersecurity, cybercrime and cyber defence (see table 4 below) and at least a further four which are gaining competences in cybersecurity in sectors like energy, transport and finance (see Annex 9).

**Table 4 Mission of relevant EU agencies and bodies in the cybersecurity field**

Body	Core Mission/activities
CERT of the EU institutions, agencies and bodies (CERT-EU)	To contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies ('the constituents') by helping to prevent, detect, mitigate and respond to cyber-attacks. It is also a member of the CSIRT Network.
European Union Agency for Network and Information Security (ENISA)	To contribute to a high level of network and information security within the Union. It is the EU network and information security agency and it works closely together with Members States and private sector to deliver advice and solutions in areas like policy, cooperation, capacity and community building. ENISA is the Secretariat of the CSIRT Network.
EUROPOL/European Cybercrime Centre (EC3)	To strengthen the law enforcement response to cybercrime in the EU and thus to help protect

---

Digital Infrastructure: internet exchange points (which enable interconnection between the internet's individual networks), domain name system service providers, top level domain name registries.

<sup>80</sup> Within the European Commission, DG CONNECT and DG HOME approach the challenges of cyberspace from a slightly different perspective. In particular, DG CONNECT is responsible for legislation, policy and R&I on cybersecurity (with a focus on cybersecurity resilience). DG HOME, with its focus on criminal law, works on reducing vulnerabilities, (criminal) threat alerts, awareness raising, ransomware-prevention advice etc. and deals with issues related to deterring and investigating cybercrime as well as the judicial follow-up.

	European citizens, businesses and governments from online crime. It provides operational and analytical support to Member States' investigations; it supports training and capacity-building; it represents the EU law-enforcement community in areas of common interest.
European Defence Agency (EDA)	To support the and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy. The EDA has a dedicated Project Team on Cyber defence with a variety of initiatives and reports as well as research activities in this area.

One of the results is that information and expertise are dispersed across several entities. As shown in Annex 4, there are over ten organisations that produce, collect and disseminate information and analyses, in some cases on the same topic and addressing the same public. Furthermore, the coordination mechanisms, where they exist, are not always adequate. For example, a conclusion from the evaluation of ENISA and the stakeholder consultations is that a good level of cooperation and coordination has been achieved between ENISA and EC3: There is almost no overlap between the two organisations, which seem to cooperate well. On the other side, there is still room for improvement in the coordination between ENISA and sectoral agencies, and between ENISA and CERT-EU. In particular, the evaluation highlighted that in spite of different scope of their mandate (one EU-wide, the other targeted to EU institutions) there is a risk of overlap between ENISA and CERT-EU in the areas of direct support and assistance to Member States' CSIRTs and cross-border operational cooperation.

Without increased cooperation and a more coordinated approach between the EU institutions, agencies and bodies, there is the risk of dispersing the efforts and decreasing the effectiveness and efficiency of their contribution to the EU's overall cyber resilience.

2.4.3. *Problem 3. Insufficient awareness and information of citizens and companies.*

*Problem 3.a: Citizens' and companies are not sufficiently aware of cyber threats.*

Those who want to learn and/or specialize in cybersecurity can nowadays enrol in almost 500 university courses and trainings across Europe<sup>81</sup>.

At least 18 Member States organise national awareness campaigns, mostly targeting public sector (80%) but also SMEs and citizens; adults, children, adolescents<sup>82</sup>. At EU level, ENISA, together with partners in Member States and the European Commission, has been running the European Cyber Security Month (ECSM) since 2013. This is an EU advocacy campaign designed to raise awareness about cybersecurity issues throughout

<sup>81</sup> <https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities>

<sup>82</sup> Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.

the month of October and which promotes a sense of shared responsibility towards safe and informed behaviour on the Internet<sup>83</sup> among citizens.

The findings of a recent survey reveal that Member States' authorities believe that European cooperation needs to be extended towards more learning and support, and that the coordination role of ENISA and Europol should be strengthened, with more funds provided to these bodies for such activities<sup>84</sup>.

However, despite cybersecurity gaining increasing prominence in the political agenda, companies' discourse and in the media, and in spite of Member States and EU actions, European citizens and companies still lack awareness and knowledge of cybersecurity issues. This knowledge gap ranges from basic steps to secure one's online presence to the financial and economic impact of cyber incidents. As an example of the first aspect, very recently a cyberattack on the UK Parliament has compromised dozens of email accounts belonging to parliamentarians who reportedly did not respect guidance issued by the Parliamentary Digital Service regarding password strength<sup>85</sup>.

According to the Norton Cyber Security Insights Report<sup>86</sup>, over six in ten (62%<sup>87</sup>) end-consumers said they believe connected home devices were designed with online security in mind. However, Symantec researchers identified security vulnerabilities in 50 different connected home devices ranging from smart thermostats to smart hubs that could make the devices easy targets for attacks.

---

<sup>83</sup> ENISA provided the following data with regard to the ECSM for the period 2013 – 2016: i) the number of cybersecurity activities taking place in October across Europe and the online outreach of the campaign increased at annual growth rate of 41%; featured press articles of European Cyber Security Month increased at an annual growth rate of 44% reaching 429 articles.

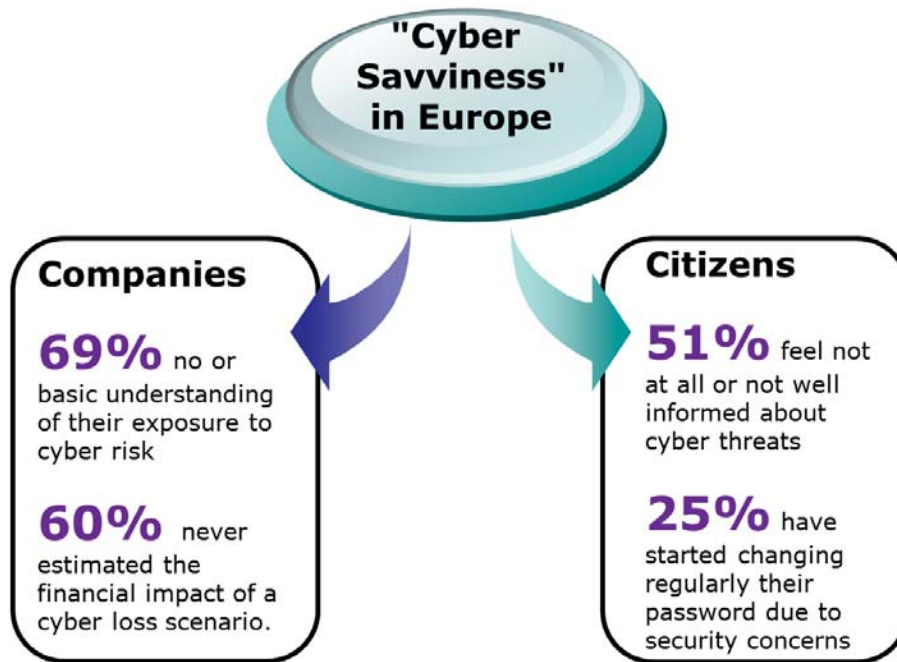
<sup>84</sup> Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.

<sup>85</sup> <https://www.parliament.uk/business/news/2017/june/cyber-incident/>.

<sup>86</sup> <https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf>

<sup>87</sup> This Report is based on an online survey of 20,907 consumers in 21 markets.

Figure 5 Some issues on awareness and knowledge of cybersecurity issues in Europe



Sources: "Special Eurobarometer 464", 2017, Attitudes towards the impact of digitisation and automation on daily life" Eurobarometer 2017, Continental European Cyber Risk Survey 2016 Report

At macro (industry) level, there is still lack of sufficient independent, neutral, EU-wide, reliable data and analyses on cyber threats, be it cross-sector or sector specific, and lack of exchange of best practices for the security of the critical infrastructures, including Internet infrastructure. Furthermore, there is a lack of systematic and reliable information on the economic impact of cyber incidents<sup>88</sup>. This affects investment in cybersecurity, and makes it very difficult to determine return on investments for instance from staff trainings or from equipment.

At micro (organisational) level, low security awareness of employees is considered the first factor inhibiting organizations from adequately defending themselves against cyber threats<sup>89</sup>. It is widely acknowledged that successful attacks are often the result of poor basic cyber "hygiene"<sup>90</sup>. Regular, simple security measures could significantly reduce the risks of an attack and, in the current interconnected business models, spreading the impact of a cyber-attack to other organisations. However, current cyber hygiene programmes across Europe vary and do not have a common approach<sup>91</sup>.

The low level of awareness of cyber threats and their possible impact is a serious issue that translates in the proliferation of incidents due to human mistakes and it also contribute to the more general lack of adequate risk management practices within organisations.

<sup>88</sup> The cost of incidents affecting CIIs, ENISA, 2016.

<sup>89</sup> Cyber threat Defence Report, CyberEdge Group, 2017

<sup>90</sup> 'Cyber hygiene' is meant as the practice of proactively and routinely taking cybersecurity measures—to resist cyber threats and prevent online security issues.

<sup>91</sup> Review of Cyber Hygiene practices, ENISA, 2016.



*Problem 3.b: Citizens' and companies do not have sufficient information concerning the security properties of ICT products and services they purchase (insufficient use of certification).*

The security properties of an ICT product or service are difficult to assess. There is an information asymmetry between designers and vendors on one side, and customers/users of ICT solutions on the other; whereby the former has greater information than the latter regarding the security properties of an ICT product or service.

Customers lacking information cannot select their products on the basis of their real security qualities. In a targeted survey, operators of critical infrastructures<sup>92</sup> report that ascertaining the accuracy of the security information provided by the vendors on a specific ICT product is a major obstacle. As such, the selection of products and services tends to be based on the reputation of the vendor or on price rather than on security properties. This leads to a potential race to the bottom with regard to investments and resources allocated to security. Such a sub-optimal outcome would, in a worst case scenario, increase vulnerability. Currently, Industrial Control Systems (ICS) products - used to monitor and control electricity generation plants or transportation systems - often rely on commercial, uncertified off-the-shelf software. This results in a reduction of costs and improved ease of use, but at the same time the exposure to computer network-based attacks is increased. Such a circumstance creates a vulnerability that can be exploited to shut off power to large areas or directing cyber-attacks against power generation plants<sup>93</sup>.

Furthermore, the co-existence of multiple schemes and standards for security certification hinders the ability of market operators and public authorities to compare and judge which ones best satisfy their particular security requirements. In April 2017, ECSO has published a State-of-the-Art Syllabus which presents an overview of certification schemes and standards in various sectors and for various products and services. For example, the document lists six schemes and two standards for security certification in the area of cloud services. Such a plethora of certification instruments translates into a missed opportunity in the digital single market. As a targeted survey shows<sup>94</sup>, operators in the energy and finance sectors refrain from the use of cloud services due to insufficient clarity and guarantees that the available standards and schemes can satisfy certain security requirements (e.g. secure data storage).

Against this background, formal processes such as certification can contribute to increase transparency of information on the security properties of a product or a service. According to a recent ENISA survey, 81% (27 out of 33) of respondents from the certification community<sup>95</sup> say that, if properly designed, certification can be an effective tool to increase transparency of the level of assurance of ICT products and services and enhance trust across the digital single market (see Annex 2 for the details of the survey results). In the same survey, 66% (22 out of 33) of respondents say that greater efforts are needed to promote certification, while 21% of respondents believe that certification is a pure market issue. In the result of another survey aimed at SMEs (see Annex 2), 39 out of

---

<sup>92</sup> Preliminary results of this survey are available in Annex 7.

<sup>93</sup> For example, the Dragonfly attack in 2014 targeted energy grid operators, electricity generation firms, pipeline operators, across numerous countries including, Spain, France, Italy, Germany, Romania, Poland, Turkey, and United States and potentially could have led to damage or disruption to energy supplies in affected countries.

<sup>94</sup> Preliminary results of this survey are available in Annex 7.

<sup>95</sup> National certification authorities, ICT vendors, Security certification laboratory, users of ICT products and services.

46 respondents were in favour of a common label for certified ICT products<sup>96</sup>. According to Eurobarometer, the majority of respondents said that the security and privacy features of an ICT product play a role in their choice; 27% are ready to pay more for better security and privacy features, while 34% are not willing to pay more but these aspects have a role in their choice<sup>97</sup>.

The suboptimal use of certification impacts the intrinsic security of the products, but also the level of information on security features of the products. To give an example, if a proper certification system had been in place throughout the EU, hospitals and other critical operators affected by the latest Wannacry attack (see section 1) would have been able to compare IT systems' security levels and, most importantly, the IT vendors' commitment to providing on-going support to users, which is not the case today.

A number of factors can explain this situation. First, existing certification schemes are to a large extent inefficient due to their high costs and lengthy processes. In addition, the current complexity of the certification landscape exacerbates such inefficiency, where separate schemes co-exist or are emerging across the EU without being mutually recognised.

These are some of the main factors which explain why ICT certification is only used in a systematic way in certain very specific domains, such as public procurement, defence and critical sectors. In many other cases, certification is left to private sector initiative, often without any involvement from public authorities and therefore without a proper monitoring on their suitability and functioning. As such, commercial/mass consumption products are rarely cyber-certified. The ever-increasing connectivity of poorly secured devices (including systems that control our cars, factories, homes, farms and critical infrastructures) could further increase the level of vulnerability of ICT devices used in Europe.

Overall, the lack of adequate information on the security properties of an ICT device can adversely affect the capacity of buyers to procure more secure products and can create a low incentive to produce more secure ICT devices. This would have a detrimental result on the level of cybersecurity of our society and economy.

## **2.5. Who is affected by the problem and to what extent?**

Section 2.2 above presented the possible scale of cybersecurity incidents and their far-reaching impact on the economy and society. Possible failures or attacks could have an impact on a vast number of stakeholders, comprising large and small businesses, public authorities, administrations and individual citizens. In other words, everyone is concerned and potentially affected by cybersecurity issues.

### Businesses

The existing gaps in the cooperation and information-sharing mechanisms within the private sector and between public and private actors limit the access to key information on cyber threats and to possible solutions for businesses to handle cyber incidents.

---

<sup>96</sup> 3 replied "no", 4 replied "don't know".

<sup>97</sup> Attitudes towards the impact of digitisation and automation on daily life, Eurobarometer, 2017.

They are also impacted by the dispersed resources and approaches across EU institutions, agencies and bodies since they lack adequate EU-level technical support, for example to identify threats, and to learn from EU-wide good practices. Also, businesses operating cross-border may face additional costs and different policies established at EU level if required to comply with different national security requirements.

In addition, the insufficient awareness of cyber-threats of employees and poor cyber hygiene practices within the organisations can lead to the proliferation of incidents due to human behaviour which can seriously harm the network and information security of small and large companies.

All these factors contribute to increased vulnerability of companies to cyber-threats, which, in case of significant incidents can lead to potentially huge direct financial losses, a loss of productivity, reputational damages and loss of competitiveness<sup>98</sup>. Beyond the costs that are currently best known – such as technical investigations, customer breaches notifications, replacement of hardware/software, legal expenses – there are less "visible" costs that can occur also once the incident has been solved: insurance premium increases, increased costs to raise debts, value of lost contract revenues, just to give a few examples<sup>99</sup>.

Manufacturers/vendors of ICT products or providers of ICT services are affected by the emergence of multiple certification schemes since they may need to certify their products or services in several Member States. Moreover, they may find it difficult to compete for public contracts, as the tender conditions refer to specific and different security and certification requirements. In general, the fragmentation of security and certification schemes and requirements leads to additional costs for businesses operating cross-border and may thus favour local firms.

Businesses who are buyers of ICT products and services, in particular operators of essential services, are affected by inadequate certification schemes as they have little information on the security properties of the ICT devices used in their infrastructures.

Conformity assessment bodies are affected by the fragmentation of security and certification schemes as they may find it difficult to penetrate other national markets where different local security requirements and/or certification schemes are present.

### Public authorities

National authorities can be impacted by the the lack of adequate European capacity to complement Member States action. This refers both to insufficient technical support, for example for the establishment of best practices or the implementation of EU policies at national level, and to the lack of hands-on support, especially for the less equipped Member States needing assistance in prevention, detection and response to cyber incidents. This situation creates inefficiencies, due to duplication of efforts (many Member States tackling issues individually) on the one side, and to limited yet dispersed resources for cybersecurity on the other.

---

<sup>98</sup> Companies do not systematically make public the costs they bear due to cyber incidents, also due to the difficulty to calculate those, but they can be very high. For example, the British telecom company Talk Talk, that had suffered an attack in October 2015, revealed to have lost 101,000 customers and suffered costs of £60m as a result of that attack. <https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave>

<sup>99</sup> Beneath the surface of a cyberattack - A deeper look at business impacts, Deloitte, 2016.

National and European public authorities can also be victims of cyber incidents and are therefore also impacted by fragmented approaches to cybersecurity and insufficient awareness of cyber threats. This can, result in direct financial losses, loss of productivity and reputational damages including critical breaches concerning national security.

Public authorities are also affected as important category of buyers of ICT products and services by the lack of sufficient information on the level of assurance of these products. Given the public interest dimension of their activities, they may wish to receive particular assurance that the solutions they procure provide a certain cyber-security assurance. They may insert in their public procurement contracts a requirement that only certified solutions are used. In case these requirements act as a barrier to foreign bidders, public bodies cannot reap the full benefits of unfettered competition and cross-border free trade across the Union.

### Citizens

Citizens are still not sufficiently aware of cyber threats and how to handle them. Very often they have only a limited knowledge of basic measures, such as the need to regularly change passwords or avoiding opening attachments in suspicious emails (see section 2.2.3). According to the UK government document “Using behavioural insights to improve the public’s use of cyber security best practices”<sup>100</sup>, even people aware of security risks continue to ignore best practices (e.g. leave devices always on and online).

Citizens are therefore exposed to significant risks to bear the costs of repairing or replacing damaged software or hardware, to lose and expose personal data and to direct financial losses (for example as a result of identity theft). Citizens are also affected by the lack of information on the level of assurance of ICT products and services that are on the market as they are rarely certified (see problem 3.b above). Security concerns can influence citizens' choices and prevent them to fully benefit from the advantages of digital economy and society.

EU citizens are also indirectly impacted by the multiple approaches to cybersecurity across Member States and across the EU institutions, as these can contribute to an insufficient protection of critical infrastructures and hence prevent citizens from accessing essential services (e.g. healthcare, water, energy, transport) in case of significant incidents.

---

<sup>100</sup> [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/309652/14-835-cyber-security-behavioural-insights.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf)

## 2.6. How will the problem evolve?

The number, complexity and scale of cybersecurity incidents and their impact on economy and society are growing over time and they are expected to further increase in parallel to technological developments, for example the proliferation of the internet of things. It is predicted that cybercrime will continue rising and cost businesses globally more than \$6 trillion annually by 2021<sup>101</sup>.

This implies that the need for increased common effort from Member States, EU institutions and private stakeholders to face cybersecurity threats can only be expected to increase in the future.

With regard to the issue of cooperation across Member States, between public and private actors and across EU institutions, agencies and bodies, some progress may happen over time but at the time of drafting there is no existing plan or benchmarks in this respect. In particular, the voluntary cooperation mechanisms foreseen by the NIS Directive do not present specific targets to be achieved for both the strategic and operational levels and the level of ambition depends on work plans adopted by Member States for both the Cooperation Group and the CSIRT Network.

In absence of intervention, maintaining the status quo would imply that ENISA would remain a small agency with a broad while temporary mandate and yet key activities in the area of resilience (for example linked to policy implementation and operational cooperation) and market (in particular certification) would not be refocused according to the new context or not included at all. The Agency would therefore not be able to provide long term sustainable support to the Member States and the EU to address new threats which are horizontal in nature impacting on multiple industrial sectors.

The information asymmetry and ineffectiveness/inefficiency of the current certification schemes is unlikely to be solved in the absence of intervention. In fact, as technology becomes increasingly complex and pervasive, it will be increasingly difficult for buyers to ascertain the security qualities of ICT products and services in absence of adequate certification. Furthermore, in the absence of action, the market fragmentation is very likely to increase in the short-medium term (next 5-10 years). As technology evolves so do the cyber-threats and vulnerabilities and with them a number of national and sectorial certification schemes and requirements keep on emerging. The lack of coordination and interoperability across such initiatives on certification is an element which decreases the potential of the digital single market.

The number and scale of cyber incidents and attacks are expected to lead to a modest natural increase in the level of awareness, due to the rising attention paid to cybersecurity issues at the level of public authorities and enterprises.

More details on the expected evolution of the problem can be found in section 5 where baseline scenarios are presented.

---

<sup>101</sup> Cybercrime Report, Cybersecurity Ventures, 2016. The estimate is based on historical cybercrime figures.

### 3. WHY SHOULD THE EU ACT?

#### 3.1. Legal basis

The legal basis for EU action is Article 114 TFEU, which deals with the approximation of laws of the Member States in order to achieve the objectives of Article 26 TFEU, namely, the proper functioning of the internal market.

The internal market legal basis for ENISA has been recognised by the Court of Justice (C-217/04, judgment of 2 May 2006) and was further confirmed by the 2013 Regulation setting the current mandate of the Agency. In addition, activities that would reflect the objectives to increase cooperation and coordination and EU level capabilities to complement the action of Member States, they fall within the field of "operational cooperation". This is specifically identified by the NIS Directive (for which art 114 TFEU is the legal basis) as an objective to be pursued in the context of the CSIRT Network where "ENISA shall provide the secretariat and shall actively support the cooperation" (Article 12(1)). In particular, Article 12 (f) further identifies as tasks of the CSIRT Network: identifying further forms of operational cooperation, including in relation to: (i) categories of risks and incidents; (ii) early warnings; (iii) mutual assistance; (iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents.

The current fragmentation of the certification schemes for ICT products and services is a result of the lack of a common legally binding and effective framework process applicable to the Member States. This hinders the creation of an internal market for ICT products and services and hampers the competitiveness of the European industry in this sector.

#### 3.2. Subsidiarity

The subsidiarity principle requires the assessment of the necessity and the added value of the EU action.

Cybersecurity is an issue of common interest of the Union. The interdependencies between networks and information systems are such that individual actors (public and private, including citizens) very often cannot face the threats, manage the risks and the possible impacts of cyber incidents in isolation. On one hand, the interdependencies across Member States, including with regard to the operation of critical infrastructures (energy, transport, water, just to name a few) make public intervention at the European level not only beneficial but needed. On the other hand, the EU intervention can bring a positive "spill over" effect due to the sharing of good practices across Member States, which can result in an enhanced cybersecurity of the Union.

In summary, in the current context and looking at the future scenarios, it appears that to **increase collective cyber-resilience of the Union individual actions by Member States and a fragmented approach to cybersecurity** will not be sufficient.

The respect of subsidiarity in this area was also recognised when adopting the current ENISA Regulation<sup>102</sup>.

---

<sup>102</sup> Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

EU action is deemed necessary also to address the fragmentation of the current certification systems. It would allow manufacturers to fully benefit from an internal market with significant savings regarding testing and redesign costs. While the current SOG-IS Agreement has achieved important results, it has also shown important limitations to be a long term suitable and sustainable solution.

The added value of acting at EU level, in particular to enhance cooperation between Member States but also between NIS communities, has been recognised by the 2016 Council Conclusions<sup>103</sup> and it also clearly emerges from the evaluation of ENISA.

None of the options analysed in this Impact Assessment go beyond what is necessary to achieve the objectives set in the following section in a satisfactory manner. Furthermore, the scope of EU intervention would not impede any further national actions in the field of national security matters.

EU action is therefore justified on grounds of subsidiarity and proportionality.

#### **4. OBJECTIVES: WHAT SHOULD BE ACHIEVED?**

Based on the problems identified in section 1, the following policy objectives for the current initiative have been set:

##### **4.1. General objectives**

The main policy objectives of this initiative are to:

1. **Increase the cyber resilience** of the Member States, businesses and the EU as a whole.
2. Ensure the **proper functioning of the EU internal market** for ICT products and services.
3. **Increase the global competitiveness** of the EU companies operating in the ICT field.

##### **4.2. Specific objectives**

With the general objectives in mind, in the broader context of the new Cybersecurity Strategy the initiative intends to achieve the following specific objectives:

1. Increasing **capabilities and preparedness** of Member States and businesses
2. Improving **cooperation and coordination** across Member States and EU, institutions, agencies and bodies.
3. Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.
4. Increasing **awareness** of citizens and businesses on cybersecurity issues.

---

<sup>103</sup> Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

5. Increasing the overall **transparency of cybersecurity assurance**<sup>104</sup> of ICT products and services to strengthen trust in the digital single market and in digital innovation.
6. Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.

## 5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

### 5.1. What is the baseline from which options are assessed?

The instruments currently available to support Member States capabilities, cooperation and the EU cyber resilience, including those of the current ENISA Regulation and the NIS Directive, are insufficient for the current cybersecurity challenges. As presented earlier in the problem statement, although the NIS Directive entered into force only in July 2016, and consequently it is too early to give conclusive assessment of its effectiveness, it does not cover all sectors and it does not necessarily include sufficient mechanisms to stimulate fully fledged EU-wide cooperation for the future cyber challenges. Also, the NIS Directive does not address the topic of ICT security certification and it does not include provisions for handling of large scale cross border incidents.

With the (upcoming) adoption of the 2017 September Communication, new instruments would be in place, in particular in the field of cybersecurity resilience and response (see paragraph 1 of the report). For the purpose of this analysis, the baseline scenario would be affected by the adoption of the Recommendation on the EU cybersecurity blueprint and the (forthcoming) legal instruments to implement the European Cybersecurity Research and Competence Centre and possibly also on the Emergency Fund.

With regard to the blueprint, it is assumed that the EU will have in place a framework for coordinated response to possible large scale cross-border cyber incidents. However, the role of ENISA envisaged in the blueprint – from supporting situational awareness to handling communications – goes beyond the current mandate of the Agency. Therefore, the blueprint could not be implemented effectively without a revised mandate of the Agency or a replacement of the Agency with other similar body to perform those functions. In the context of EU response to cybersecurity crisis situations, the baseline scenario would include – upon its adoption in the context of the next Multiannual Financial Framework - the Cybersecurity Emergency Fund that would allow Member States to seek help at the EU level in case of major incident, provided that the Member State had put in place a prudent system of cybersecurity prior to the incident, including full implementation of the NIS Directive, mature risk management and respective supervisory frameworks at national level. The Fund could deploy a rapid response capability in the interests of solidarity and finance specific emergency response actions such as replacing compromised equipment or deploying mitigation or response tools to assist victims.

---

<sup>104</sup> Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.



In the field of research and development, upon the adoption of the related legal instrument, ENISA (both in case of existing and revised mandate) would link its efforts in the area – mainly advisories on EU needs – to the work of the European Cybersecurity Research and Competence Centre, which would become a major player by pooling and shaping research efforts and supporting the development of industrial capabilities.

Article 36 of the current ENISA Regulation includes a sunset clause, fixing the duration of the agency mandate for seven years until June 2020. For the purpose of this analysis, the status quo, which sees the existence of an EU decentralised agency with a fixed term mandate, is considered as baseline scenario. The sunset clause and thus termination of ENISA is also explored among the possible options.

With specific regard to certification, the baseline scenario translates into non-EU action. In this case, it is unlikely that ICT producers would establish self-regulatory measures to allow buyers to better ascertain the security qualities of ICT products and services. It is however possible that Member States take action, which could result in even more national and sectoral only certification schemes. In this case, fragmentation is expected to widen in the short-medium term (5-10 years) with a negative impact on the full potential of the digital single market.

The current SOG-IS agreement and the CCRAs are also unlikely to constitute a possible solution to the problem in the short and medium term. As explained above, the SOG-IS MRA is based on the methodology of CC, thus it shares similar criticism related to the length of process, high cost, unsuitable for products requiring low level of assurance, suitable to certify products rather than services. For these reasons, only a few protection profiles related to digital products have been developed under the current SOG-IS MRA. These are for example, digital tachographs, digital signatures and smart cards.

## **5.2. Policy options related to ENISA**

The policy options on the possible future of ENISA, including those that were discarded as result of the impact assessment exercise, are presented below.

### **Option 0 – Baseline scenario**

This option is about the preservation of the status quo. ENISA would continue to be an Agency with a mandate limited in time. ENISA's mandate would be extended in a manner similar to the previous renewals (Regulation (EC) No 1007/2008 and Regulation 580/2011) and the objectives and tasks of the Agency would be largely similar to the ones of today subject to adaptations based on acts that entered into force after the adoption of the current ENISA Regulation in particular the NIS Directive and the Regulation on electronic identification and trust services for electronic transactions in the internal market<sup>105</sup> (eIDAS Regulation). It might also include provisions from the Electronic Communications Code, which is currently in the legislative process and therefore not yet adopted. Preserving the status quo would also imply maintaining a fixed-term mandate for ENISA. Therefore, the activities described in the box below would also be subject to a time limit.

---

<sup>105</sup> Regulation EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

1. ENISA's mandate, currently expiring in 2020, would be extended for a fixed term period based on previous mandates.
2. The current mandate, objectives, governance and organisation of the Agency would remain unchanged.
3. The tasks of the Agency would remain mostly unchanged, except for additional tasks due to alignment with the specific provisions of relevant laws:
  - As provided by the NIS Directive, ENISA would support Member States at their request, in developing national strategies or national CSIRTs.
  - As provided by the NIS Directive, ENISA would provide the secretariat of the CSIRTs network and actively support the cooperation among national CSIRTs. ENISA will also be part of the Cooperation Group, with a view of supporting strategic cooperation between national competent authorities.
  - As provided by the Framework Directive for Electronic Communications (the new Electronic Communication Code is currently in the legislative process), ENISA would be required to contribute to an enhanced level of security of electronic communications by providing expertise and advice, and promoting the exchange of best practices.
  - As provided by the eIDAS Regulation, ENISA would collect summary information from supervisory bodies on the notifications of security breaches.

**Option 1 – No policy intervention –Expiry of ENISA’s current mandate without renewal and termination of ENISA**

This option would not entail a new legislative proposal to amend or repeal the current ENISA Regulation. This would lead to the termination of ENISA at the end of its mandate in June 2020 (seven years from 19 June, 2013 in accordance with article 36 of ENISA Regulation). The Commission would then need to decide on the possible redistribution of competences/activities at EU and/or national level. To be noted that according to the provisions of the Common Approach on decentralised agencies "closing down an agency could be a solution for dealing with underperforming agencies unless the agency is still the most relevant policy option, in which case the Agency should be reformed"<sup>106</sup>. In this case and in the absence of a new proposal, in accordance with the current Regulation (recital 54 to be in footnote) the Commission should take the relevant measures addressing in particular issues relating to staff contracts and budget arrangements.

1. If a decision is taken not to extend ENISA's mandate, pursuant to art. 36 of the ENISA

<sup>106</sup> Joint Statement of the European Parliament, the Council of the European Union and the European Commission on decentralised agencies – Common Approach – 2012.

Regulation, it would expire as of 19 June, 2020.

2. As provided by the 'sunset clause'<sup>107</sup> of the ENISA Regulation, the Agency and the Commission should take the relevant measures towards the end of the current mandate, addressing in particular issues relating to staff contracts and budget arrangements.
3. The tasks currently attributed to ENISA would be terminated and, in the absence of EU intervention, fall back under the responsibility of Member States.
4. The tasks attributed to ENISA by subsequent legislation, in particular by the NIS Directive, would have to be re-assigned to other EU or national bodies. This would entail the repeal of the Regulation and a new proposal for NIS Directive with a new arrangement for what concerns ENISA. Such a proposal would need to be prepared in time for there not to be a gap affecting the proper implementation of NIS Directive due to take place in May 2018.

### **Option 2 – 'Reformed ENISA'**

This option would reform the Agency building on the strengths emerged in the course of the current mandate and addressing shortcomings and weaknesses. The new mandate would take into account new threats, policy, actors and technology changes as well as the results of the evaluation.

In particular, this would imply a redefinition of ENISA's role, competences and functioning, scope, the duration of the mandate, as well as the synergies with other EU agencies and bodies.

1. ENISA would be granted a permanent mandate and thus be put on a stable footing for the future. The mandate, objectives and tasks would still be subject to regular reviews.
2. The mandate would further clarify the role of ENISA as the EU agency for cybersecurity and as the reference point in the EU cybersecurity ecosystem, acting in close cooperation with all the other relevant bodies of such ecosystem.
3. The organisation and the governance of the Agency, which were overall positively judged in the course of the evaluation, would be moderately reviewed, in particular to make sure that the needs of the wider stakeholders' community are better reflected in the work of the Agency. This would imply, for example, the need that the Executive Director and the Management Board take into utmost account the opinion of the Permanent Stakeholder Group (PSG) in the preparation of the annual and multiannual work programme, as well as enabling the participation of a limited number of PSG members as observers in the Management Board, upon request of the Chair.
4. The scope of the mandate would be delineated, strengthening those areas where the agency has shown clear added value and adding those new areas where support is needed in view of the new policy priorities and instruments, in particular the NIS Directive, the review of the EU Cybersecurity Strategy, the upcoming EU Cybersecurity Blueprint for cyber crisis cooperation and ICT security certification:

---

<sup>107</sup> According to the Common Approach on decentralised agencies, founding acts should include review or sunset clauses. The sunset clause refers to the possible termination of the activities of an agency at the end of the mandate, as established in its founding act.

- EU policy development and implementation: ENISA would be tasked with proactively contributing to the development of policy in the area of Network Information Security, as well as to other policy initiatives with cybersecurity elements in different sectors (e.g. Energy, Transport, Finance, etc.). To this end, it would have a strong advisory role, including the provision of independent opinion and preparatory work for the development and update of policy and law. ENISA would also support the EU policy and law in the areas of electronic communications, electronic identity and trust services, with a view of promoting an enhanced level of cybersecurity. In the implementation phase, in particular in the context of the Cooperation Group, ENISA would assist Member States in achieving a consistent approach to the NIS Directive implementation across borders and sectors as well as other policy and laws where cybersecurity is involved. In order to support the regular review of policy and law in the area of cybersecurity, ENISA would also provide regular reporting on the state of implementation of the EU legal framework.
- Capacity building: ENISA would be contributing to the improvement of EU and national public authorities' capabilities and expertise, including on incident response and supervision of cybersecurity related regulatory measures. The agency would also be required to contribute to the establishment of *Information Sharing and Analysis Centres (ISACS)* in various sectors by providing best practices and guidance on available tools, procedures as well as appropriately addressing regulatory issues related to information sharing.
- Knowledge and information, awareness raising: ENISA would have a new task in developing the information hub of the EU. This would imply the promotion and sharing of best practices and initiatives across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies; the Agency would also make available advice, guidance and best practices on the security of critical infrastructures. In the aftermath of significant cross-border cybersecurity incidents, ENISA would also compile reports with a view of providing guidance to businesses and citizens across the EU. This stream of work would involve also the regular organisation of awareness raising activities in coordination with Member States authorities.
- Market related tasks: ENISA would perform a number of functions specifically supporting the internal market, which would include new tasks: cybersecurity 'market observatory', by analysing relevant trends in the cybersecurity market to better match demand and supply; support the EU policy development in the ICT standardisation and ICT security certification areas. In particular, it would facilitate the establishment and uptake of security standards. ENISA would also execute the tasks foreseen in the context of the future framework for certification (see below section 5.3 – options for certification).
- Research and innovation: ENISA would contribute its expertise by advising EU and national authorities on priority-setting in research and development, including in the context of the contractual public-private partnership on cybersecurity. ENISA's advices on research would feed into the new European Hub of Excellence in Cybersecurity, as developed in the context of the review of the Cybersecurity Strategy, ENISA would also be involved, when asked to do so by the Commission, in the implementation of research and innovation EU funding programmes.
- Operational cooperation and crisis management: this stream of work would build on the existing preventive operational capabilities, in particular the pan-European

cybersecurity exercises (Cyber Europe), and a supporting role in operational cooperation as secretariat of the CSIRTs Network (as per NIS Directive provisions) by ensuring, among the others, the well-functioning on the CSIRTs Network IT infrastructure and communication channels. In this context, a structured cooperation with CERT-EU, EC3 and other relevant EU bodies would be required.

Furthermore, a structured cooperation with CERT-EU should result in a function to provide technical assistance in case of significant incidents and to support incident analysis. Member States that would request it would receive assistance to handle incidents and backend support for analysis of vulnerabilities, artefacts and incidents in order to strengthen their own preventive and response capability. In cooperation with the CSIRT Network, ENISA would also conduct ex-post technical enquiries of significant incidents with a view to issue recommendations in order to prevent future incidents.

ENISA would also play a role in the upcoming EU cybersecurity blueprint, setting the Commission's proposal to Member States for a coordinated response to large-scale cross-border cybersecurity incidents and crises at the EU level<sup>108</sup>. ENISA would facilitate the cooperation between individual Member States, in dealing with emergency response by analysing and aggregating national situational reports based on information made available to the Agency on a voluntary basis by Member States and other entities.

### **Option 3 – EU cybersecurity agency with full operational capabilities.**

This option implies restructuring ENISA according to the model that several Member States have adopted, by bringing together three main functions: 1. policy advisory 2. the centre of information and expertise and 3. the Computer Emergency Response Team. In this case, the Agency would cover the entire cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.

1. The new ENISA would be granted a permanent mandate. The mandate, objectives and tasks would be subject to regular reviews.
2. The organisation and the operations of the Agency would be reviewed, in particular to ensure that the needs of the wider stakeholders' community are better reflected in the work of the Agency.
3. To a large extent this option would imply the same change in the scope of the mandate as option 2 (policy support, capacity building, market, knowledge and awareness raising) however additional tasks would be added in the area of incident response and crisis management.
4. The new operational tasks of ENISA might require a new legal basis for the corresponding Regulation.

<sup>108</sup> The "blueprint" will apply to cybersecurity incidents whose disruption is more extensive than any Member State can handle on its own or affects two or more Member States with such a wide-ranging and significant impact or political significance that they require timely policy coordination and response at Union political level.

5. The new ENISA would be in a position to provide fully-fledged CERT services, adapted to its EU-level mission ensuring no duplication with the tasks of national CERTs, such as:

- Establish and provide its own sources of information related to cybersecurity incidents and threats.
- Produce real-time situational awareness and dynamic (live) threat intelligence feeds (accessible to national CSIRTs and possibly CSIRTs of private entities like the operators of essential services) based on ENISA's own sources as well as information that is mandatorily shared with the Agency during large scale cybersecurity incidents and crises.
- Provide active technical operational assistance, both in terms of technical expertise as well as human resources to Member States CSIRTs (and possibly to other actors like operators of essential services, EU bodies and institutions), in preventing, detecting and particularly in responding to incidents.
- Coordinate CSIRTs Network operations, pooling national resources on analysing threats and responding to incidents.

### 5.3. Options related to certification

The results of the consultations with national certification authorities, ICT vendors and providers, operators of critical infrastructures (see Annex 2) as well as inputs of technical support studies and reports (e.g. by JRC and ENISA) have been used to select the most appropriate policy options to address the problems identified in this Impact Assessment. These options respond to the need to promote security certification through agile and flexible mechanisms on the one hand, as well as the desire to support an EU-wide approach to security certification that builds as much as possible on existing mechanisms, on the other hand.

On this basis, the following policy options were considered to achieve the policy objectives and to address the problems identified.

#### **Option 0: Baseline scenario - Do-nothing.**

Under this option the Commission would not undertake any policy or legislative action. With regard to the three identified problems, this option would result in the following situation:

1. The problem of **market fragmentation is very likely to increase** in the short-medium term (next 5-10 years), as a number of national and sectoral certification schemes and competing sectoral standards are emerging<sup>109</sup>.
2. The co-existence of competing schemes and standards would undermine the ability of vendors and end-users (citizens and operators of critical infrastructures) to compare and

<sup>109</sup> For a full overview of existing cybersecurity sectoral standards and certification schemes see here: [www.upm.es/observatorio/vi/gestor\\_general/recuperar\\_archivo.jsp?idf=642&tipo=2](http://www.upm.es/observatorio/vi/gestor_general/recuperar_archivo.jsp?idf=642&tipo=2)

judge which scheme or standard would best satisfy their particular security requirements  
This circumstance would worsen the problem related to information asymmetry.

3. The lack of coordination would cause a situation where Member States continue to put in place certification requirements for their critical infrastructures through public procurements, thus creating an uneven level of protection. As Member States are increasingly interconnected, this scenario would increase vulnerability and the risk of a cross-border proliferation of attacks (esp. on critical infrastructures), even in those Member States adopting high level of security requirements.
4. The lack of coordination and interoperability across multiple schemes and standards would not contribute to create a chain of trust in the digital single market. A divide may persist between operators of critical infrastructures - which increasingly rely on digital products and services for their operations - and vendors or providers. This may hamper the digital single market
5. Agreements establishing mutual acceptance of certificates among Member States should be expected in the future. However, they will occur in an uncoordinated manner and would depend on the willingness of each Member States. For example, the German national baseline certification scheme (under development) is likely to be mutually recognized with the existing French national scheme (CSPN), but not necessarily with similar British scheme (e.g. Baseline Security, CPA). Such a piecemeal approach may turn out to be inefficient and resource-intensive
6. Market operators will put in place self-regulatory measures or embark on certification processes only in presence of strong economic incentives such as compliance with public procurements requirements which would limit the roll-out and possible positive impact of ICT certification.
7. The effectiveness and efficiency of current certification mechanisms such as SOG-IS MRA and the CCRAs will not improve in the short and medium term. The shortcomings of CC - on which SOG-IS MRA is based - related to high cost, long duration of process, limited membership and scope will remain.

**Option 1: Non-legislative ("soft law") measures.** Under this option, the Commission would use soft policy instruments to reach the objectives of this initiative (e.g. improve the level of information related to the security properties of ICT devices and reduce fragmentation). As such, the Commission could issue interpretative guidelines, encourage co- or self-regulation initiatives, promote the development of technical standards, support research or awareness rising activities. The specific contents of the individual measures cannot be delineated with precision at this stage, as they will emerge as a result of the overall process within the Commission and with the stakeholders.

1. **Issuing interpretative communications:** The Commission would provide guidance on elements of national or sectorial schemes, such as in particular requirements for certification authorities and conformity assessment bodies. The Commission would request ENISA to provide a preliminary assessment of such interpretative communications and to explore the views of public and private stakeholders by means of workshops and formal consultations.
2. **Support EU-wide co- or self-regulatory initiatives:** together with ENISA, the Commission will support, and incentivise the establishment of voluntary EU-wide schemes for the certification of ICT products and services so as to foster the emergence of EU-wide solutions. The Commission may also initiate co-regulatory activities, thus entrusting the development of a specific certification scheme to economic operators. However, under such scenario, the system in place would include a dedicated supervisory mechanism.

3. **Strengthen standardisation activity:** the Commission would further intensify and support the adoption of EU standards in the field of security of ICT products and services with a view to harmonising the substantive requirements at EU level. The Commission could define the need of EU standards on the basis of the recommendations from the Focus Group on Cybersecurity established by CEN/CENELEC/ETSI<sup>110</sup>, for example. The Group's recommendation will also take into account inputs from ENISA.
4. In order to **avoid duplication and ensure coherence**, the above activities should be carried out in close consultation with institutional actors responsible for certification initiatives stemming from other legislation (e.g. GDPR) and from other sectoral legislation on security of critical infrastructures<sup>111</sup>.
5. **Research and awareness-raising activities.** The Commission would increase the funds related to R&D projects in the field of ICT security certification. In addition, ENISA would be tasked with carrying out awareness-raising activities such as setting-up an ad hoc website, online advertising campaign, ad hoc conferences, events and training for national officials.

**Option 2: EU legislative act to create a mandatory system for all Member States based on the SOG-IS system.**

Under this policy option, the Commission would propose a legislative act that would incorporate SOG-IS MRA so that it becomes binding on all Member States. Therefore, the Management Committee of the current SOG-IS MRA will be composed of representatives from all Member States. Sectoral Working Groups will provide technical support to the Management Committee. ENISA would help run the Secretariat of the Management Committee and would support the coordination of activities of the Working Groups.

The legislative act will have the following essential content:

1. Lay down rules of **participation**: representatives from Member States can participate in two fundamental ways: as certificate consuming participants and as certificate producers
2. Lay down the requirements that Member States have to comply with when designating **certification authorities** and **testing facilities**;
3. Refer to **CC** as the applicable security evaluation criteria.
4. Establish the objectives and roles of the Management Committee such as:
  - a. Coordinate the standardisation of CC protection profiles
  - b. Coordinate the certification policies between national Certification Bodies
  - c. Coordinate the development of protection profiles whenever the European Commission launches a directive that should be implemented in national laws and that includes aspects related to information security
  - d. Define role of the Management Committee in international fora such as CCRA
5. Establish **general rules for mutual recognition** of certificates issued under the new SOG-IS system;
6. Lay down provisions to initiate consultations with other institutional actors to seek

<sup>110</sup> <https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx>

<sup>111</sup> For example, consultations may be conducted with the future European Data Protection Board or other authorities in charge of security of critical infrastructures.



coherence with other certification initiatives deriving from other legislation.

### **Option 3: EU general ICT cybersecurity certification framework**

Under this option, the Commission would propose a new European ICT Security Certification Framework laying down rules for the development of individual EU-wide cybersecurity certification schemes for specific ICT products and services or cybersecurity risks, leading to the issuance of certificates valid and recognised in the whole EU.

A European Cybersecurity Certification Framework (the "**Framework**") for ICT products and services and specifies the essential functions and tasks of ENISA in the field of cybersecurity certification. The Framework lays down common provisions and procedures enabling the creation of EU-wide cybersecurity certification schemes for specific ICT products/services or cybersecurity risks. The creation of European cybersecurity certification schemes in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.

A European cybersecurity certification scheme shall be understood as the comprehensive set of rules, technical requirements, standards and procedures defined at Union level applying to the certification of ICT products and services falling under the scope of the scheme. As such, the type of ICT product and service covered by a European certification scheme will be defined in the approved scheme itself. Moreover, it is essential to underline that certification schemes do not, as a rule, set the technical standards, i.e. they do not lay down the technical requirements that the products need to comply with. This is the task of legislation and technical standardisation.<sup>112</sup> Certification schemes set out, instead, a specific process for evaluating – at a specific level of assurance – the security properties of ICT products and services falling within the scope of the scheme<sup>113</sup> Evaluation of security functionalities of these products or services would be carried out against the requirements to which a particular scheme will refer. Existing standard can be used when considered appropriate to express these technical requirements ..

The main elements of this option are specified in more detail below:

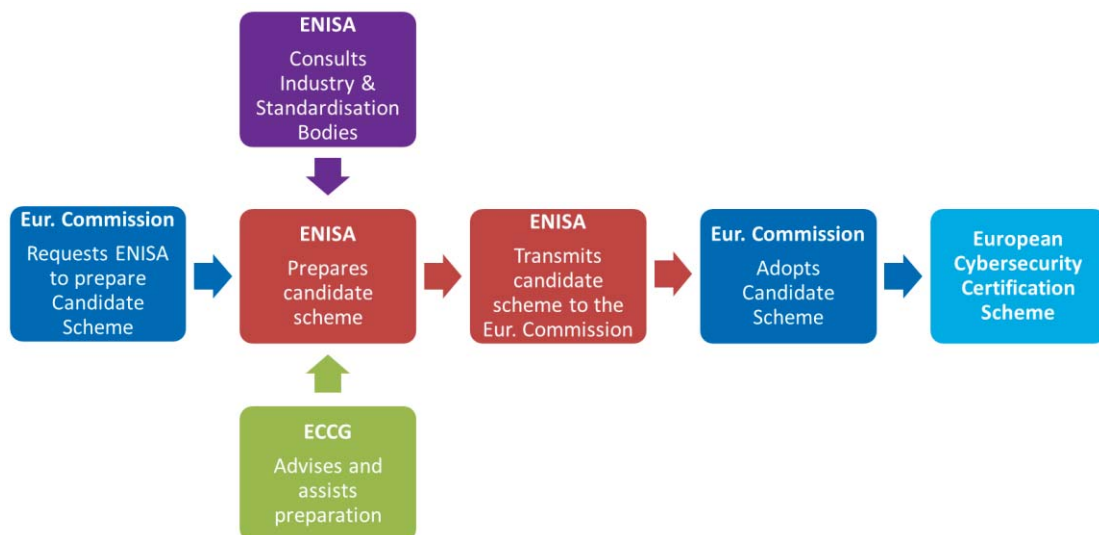
1. The proposal does not introduce directly operational certification schemes, but rather creates a system (framework) for the establishment of specific certification schemes for specific ICT products/services (i.e. "European cybersecurity certification scheme"). The creation of individual European cybersecurity certification schemes in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.
2. The framework would apply in so far as there are no specific provisions with the same

<sup>112</sup> In the case of European standards, this agreement is reached within the so-called European standardisation organisations and endorsed by the European Commission by means of its publication in the Official Journal (see Regulation 1025/2012).

<sup>113</sup> i.e. for testing the security functionalities of ICT products and therefore to establish the required level of confidence

objective in Union legislation. The priorities of the certification framework will be identified by Member States, the Commission or ENISA on the basis of the perceived needs of Member States or emerging from the market. The initial ideas on the priority areas for certification which derive from public consultations as well as discussions with Member States and the industry are presented in the 2017 September Communication that is adopted as part of the cybersecurity package<sup>114</sup>.

3. The general purpose of a European scheme would be to attest that the ICT products and services that have been certified in accordance with such schemes comply with specified requirements (as detailed for instance in an European standard) as regards their ability to resist at a given level of assurance, and actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems.
4. The proposal will lay down a specific set of security objectives, which should be taken into account in the design of a specific European scheme. They will include, for instance, the ability to protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access, disclosure, destruction, accidental loss or alteration.
5. The proposal will also provide the minimum content of European schemes. In particular, such schemes will have to include a number of specific elements setting out the scope and object of the certification, including the categories of products and services covered the specific evaluation criteria and evaluation methods, the level of assurance basic, substantial or high intended to ensure as well as a detailed description of technical security requirements, for example by reference to standards or technical specifications.
6. European schemes would be prepared by ENISA, with the assistance and close cooperation of the European Cybersecurity Certification Group (see below), and adopted by the Commission by means of delegated or implementing acts. In practice, the Commission may request ENISA to prepare a scheme for specific ICT products/services or cybersecurity risks. ENISA will work on the scheme closely in cooperation with national certification bodies represented in the European Cybersecurity Certification Group. Member States and the Group may also propose to the Commission that it requests ENISA to prepare a particular scheme.



<sup>114</sup> JOIN(2017) 450

#### **Figure 6 Overview of a how a European cybersecurity certification scheme is adopted**

7. Recourse to European cybersecurity certification would remain voluntary. However, future Union or national legislation may mandate the use of an approved European scheme for specific products or services. As such, no specific measures are foreseen nor are necessary for relevant products not covered by an EU certification scheme. However, in order to ensure harmonisation and avoid fragmentation, Member States should not introduce new national certification schemes for ICT products and services where an European cybersecurity certification scheme for the same product or service exists. Similarly, current national schemes or procedures for the ICT security certification of products and services will cease to produce effects where a European cybersecurity certification scheme for the same product or service will be established. Existing certificates issued under current national cybersecurity certification schemes shall remain valid until their expiry date. The creation of national schemes with high level of assurance remains possible if introduced on the ground of national security.
8. Once a cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services will be able to submit an application for certification of their products or services to a conformity assessment body of their choice. Conformity assessment bodies should be accredited by an accreditation body in accordance with Regulation 675/2008/EC. Accreditation bodies should revoke an accreditation of a conformity assessment body where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation.
9. Under this option, Member States would have to provide for one certification supervisory authority, tasked with supervising compliance of conformity assessment bodies and of the certificates issued by conformity assessment bodies established in their territory, with the requirements of this Regulation and of the relevant European certification schemes. National certification supervisory authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories. Moreover, they should cooperate with other certification supervisory authorities or other public authorities by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.
10. **European Cyber-certification Group (ECCG):** the proposal establishes the European Cyber-certification Group (ECCG), consisting of representatives of certification authorities of all Member States. The main task of the Group would be to advise the Commission on issues concerning cybersecurity certification policy and to work with ENISA on the development of candidate European cybersecurity certification schemes. ENISA would assist the Commission in providing the secretariat of the Group and would maintain the inventory of schemes approved under the Framework. ENISA would also liaise with standardisation bodies to ensure the appropriateness of standards used in approved schemes and to identify areas in need of certification schemes and cybersecurity standards.

#### **Option 4: ICT security internal market legislation**

Under this option the Commission would propose an EU ICT security legislation based on the 2008 internal market New Legislation Framework. As a result of this option, selected ICT products and services could only be put on the market if they comply with identified essential requirements on the basis of a prior conformity assessment. This would entail adding a new requirement for compliance with an ICT security standards to the other requirements needed to obtain the CE mark. In line with the approach of the

new legislative framework, the law would rely on standards<sup>115</sup> and would establish a presumption that compliance with such standards implies compliance with the EU internal market. The main elements of such legislation are discussed below:

1. **Essential requirements** for the **construction and provision** of ICT products and services. Such requirements would concern mainly security, privacy, transparency and safety.
2. Requirements relating to the **provision of information to Member States**, the Commission and consumers.
3. Requirements concerning the **registration and traceability** of ICT products and services.
4. Requirements that ICT products and services cannot be placed on the market if they do not comply with the requirements of the legal instrument.
5. **Specific obligations of manufacturers, importers and distributors** with regard in particular to the declaration of conformity and the affixing of the CE mark.
6. Provisions concerning **market surveillance**, including the appointment by MS of supervisory bodies, conformity assessment bodies, measures for correcting, withdrawing or recalling non compliant products and services.

#### 5.4. Options discarded at an early stage

In the course of the impact assessment exercise two of the policy options identified in the previous section were discarded at an early stage and thus were not subject to deeper analysis and assessment.

- **Option 1 'Expiry of ENISA mandate'**. This option has been discarded for several reasons. First of all from the evaluation it emerged that the Agency showed to be relevant and to provide EU added value and that, if its weaknesses are addressed, ENISA has the strong potential to contribute even more to increase cybersecurity in the EU. The need for even further cooperation, including at operational level, is one of the key findings of the evaluation. This concluded that it would not be possible to ensure the same degree of community building and cooperation across the Member States without a more centralised EU agency for cybersecurity; the picture would be more fragmented with bilateral or regional cooperation stepping in to fill a void left by ENISA. ENISA is in fact the only EU agency that currently can ensure EU coordination and the needed cross-border approach.

Secondly, the option of terminating ENISA would be incoherent with the provisions of the NIS Directive, which require ENISA to perform tasks that have no end date. Some of the tasks conferred upon ENISA by the NIS Directive could be performed by the Commission. However, this would be incoherent with the decision of the co-legislators that specifically assigned those to an independent EU agency. The termination of ENISA - and in the that case it would not be replaced by an equivalent EU level body - would also imply less EU level support

---

<sup>115</sup> This option would also encourage the development of standards, in case they do not exist for specific products

in the field of cybersecurity and, as such, be in contrast with the vision expressed in the review of the EU Cybersecurity Strategy. In particular, it would be incoherent with the EU cybersecurity blueprint for large scale cross-border incidents, which foresees a role for ENISA in supporting a cooperative Union response to such incidents.

Thirdly, with regard to the EU budget, the discontinuation of ENISA would imply the disinvestment of the current contribution to ENISA budget (about EUR 11 million per year). However, in case of a discontinuation of ENISA without replacement, this would require additional investments by national public authorities (multiplied per each Member State) and businesses as they would not benefit any longer from 'free of charge' services (for example the trainings, the publications, the good practices, the cyber exercises) that would have to be replaced either with in-house capacity or with external contracts. A recent study shows that it is considerably less costly to carry out the tasks assigned to the agencies at the EU level than it would be if these tasks were undertaken by the EU28 Member States<sup>116</sup>. In the case of the replacement of ENISA with a new EU level body, the EU would incur additional set-up and operating costs, which would be as a minimum equal to the existing ones. The establishment of a new body would require additional time: a minimum estimate would be of additional three years (including one year to develop a proposal and one to two years for a new seat agreement and logistic set-up). A significant negative impact on the efficiency would derive from the loss of the current expertise of ENISA staff and economies of experience of the organisation as a whole.

Lastly, this option has not received support by any category of stakeholders. The need for an EU-level body, in particular ENISA, to improve cybersecurity across the EU has been expressed by 98% of the respondents to the public consultation on ENISA review. The opinions expressed by stakeholders across the board (Member States authorities, CSIRTs, industry, academia, EU institutions) went in the same direction during the course of the evaluation of ENISA and the other targeted consultations (CSIRTs Network survey, stakeholder workshops, Member States roundtable – see Annex 2 for more details).

- **Option 4 'ICT security internal market legislation'**. This option could significantly solve the problems identified. However, it would entail the identification or development of a cybersecurity standard that is product-specific. Extensive analysis would be needed to identify such a product. It would be also challenging to justify the selection of a specific product or sectors over others equally in need of cybersecurity assurance. Such a 'vertical' approach may be limited in light of the high variety of ICT products and services, their specific security needs and types of employment. Rather, stakeholders' consultations and technical studies suggest focusing on identifying priorities for ICT certification across sectors. Moreover, this option was discarded because it would imply a

---

<sup>116</sup> The Cost of non-agencies with relevance to the internal market, European Parliament study, 2016. The study introduces general findings and then focuses on the case of seven fully or partially self-financed agencies.

disproportionate burden and cost, especially for industry and Member States. 72% of respondents (e.g. 24) of the ENISA survey on ICT security certification (see Annex 2) indicate 'cost' as the main issue they face when dealing with security certification. SMEs in particular will bear an unduly high costs and administrative burden. Another factor that explains this choice is related to the lack of evidence as on the impact as well as on what should be the scope of such a measure (products, services, sectors, component, and systems) and capabilities across the EU. This option will require a significant mobilization of resources to monitor and ensure compliance. In addition, this approach is not flexible enough to cope with technological changes and developments taking place in a dynamic environment.

For these very reasons, this option has very little support from stakeholders. Overall, at least at this stage, this is a very ambitious and impractical option, that could however be considered in the future, as further evidence on its impact and scope becomes available.

## 6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section analyses the economic, environmental and social impact of the options in line with the Better Regulation Guidelines together with the coherence with other policy and the views of stakeholders. The description of the impact of the options included in this section is complemented by the economic analyses conducted by external contractors in the context of two studies supporting the present impact assessment (see Annexes 5, 6 and 7). As the external studies make clear, the economic assessment faced some limitations in the collection of data, whose impact was mitigated to a maximum possible extent.

### 6.1. ENISA

#### Option 2 Reformed ENISA

Effectiveness
<p><b>Objective 1: Increasing capabilities and preparedness of Member States and businesses</b></p> <p>A <b>permanent mandate</b> would ensure that ENISA supports Member States and businesses in a sustainable manner, providing opportunities for <b>long term vision and planning</b> of the work both to the Agency and to its constituents.</p> <p>The partial revision of the Agency's <b>governance and operations</b> – in particular the closer involvement of the Permanent Stakeholder Group (PSG) in the definition of the work programme of the Agency – would allow the wider community of stakeholders, in particular businesses to receive better support in terms of what they really need to increase their capabilities.</p> <p>A very significant impact on the capabilities and preparedness of Member States is in particular expected from the provision of <b>long-term strategic analyses</b> of cyber threats and incidents. This will help identify emerging trends, provide authoritative <b>guidance and reports</b> on cybersecurity matters targetted at private organisations and citizens, assist in the <b>brokerage of expertise and good practices</b> between Member States and <b>provide trainings and training material</b> for national authorities and for CSIRTs operations, as well as guidance on <b>improving CSIRT maturity</b> according to EU and international best practices. The <b>reinforcement of the Cyber Europe exercises</b>, and the involvement in the proposed blueprint for cyber crisis cooperation (see</p>

description of the option for more details), could help achieve one key milestone for EU preparedness which is the availability of a well-rehearsed and agreed plans in case of large scale cross-border cyber incident. The involvement of ENISA in the development and implementation of EU policy on **ICT security certification** is furthermore expected to positively, although indirectly, impact EU overall preparedness. In fact, the promotion of appropriate certification guidelines supporting EU recognised schemes will not only improve the level of assurance of the security properties of ICT products and services, but it will also stimulate the uptake of adequate security standards. The impact of this policy is expected to be quite far-reaching considering the wide concerned range of stakeholders (from individual buyers to operators of critical infrastructures).

A positive impact can be inferred on the capabilities of private actors which operate within Member States and across borders, through the contribution to the establishment of **Information Sharing and Analysis Centres (ISACs)** in various sectors. ENISA would be able to provide best practices and guidance on available tools, procedures as well as support to appropriately addressing regulatory issues related to information sharing.

### **Objective 2: Improving cooperation and coordination across Member States and the EU, institutions, agencies and bodies.**

This option builds on what the evaluation identified as one of the key strengths of ENISA – bringing Member States and, more broadly, NIS communities together for the purpose of cooperation – so it is expected to fully support the objective of improved **cooperation** across Member States and EU institutions, agencies and bodies. In particular, the support for a **harmonised approach to EU cybersecurity policy**, both upstream in the development phase and downstream in the phase of implementation (starting with the key role the Agency can play under the NIS Directive), can significantly contribute to increasing effective cooperation. A positive impact is also expected in terms of enhancing **cooperation within the private sector**, in particular through increased information sharing linked to the stimulation of ISACs ( see above). The positive impact will moreover also cover the link **between public and private actors**, especially through the support through the establishment of research and innovation priorities in the context of the contractual public-private partnership on cybersecurity and the operational cooperation. Here an increased involvement of industry is expected, in particular regarding critical infrastructures.

The contribution to **policy development in the area of NIS** should furthermore support cooperation amongst national authorities and regulators across all sectors as part of the NIS Directive and should lead he telecoms sector to promote best practices and exchange lessons learned amongst sectors.

Furthermore, it is reasonable to assume that the clear positioning of ENISA in the EU cybersecurity ecosystem and the better definition of the links and ‘bonds’ with other EU institutions, agencies and bodies would result into a stronger cooperation within the EU cybersecurity ecosystem.

With respect to the aim of improved **coordination**, both across Member States and EU institutions, agencies and bodies, some activities included under option 2 are presumed to be particularly effective, in particular: the **pooling of information** on cybersecurity deriving from the EU institutions, agencies and bodies; the support to **test the blueprint** for cyber crisis cooperation; the requirement for EU and national authorities to **consult and/or take into account ENISA's opinion** when developing/implementing policies on cybersecurity; and the support for the Cooperation Group to achieve a **consistent approach to the NIS Directive implementation** across borders and sectors.

An important caveat that would influence the effectiveness of this option with regard to objective 2 is the degree of actual engagement in cooperation and coordination (besides the overall positive attitude shown in the consultation process) by both Member States and EU institutions and bodies, which otherwise can only be stimulated to a limited extent by empowering the Agency to further work in these areas.

### **Objective 3: Increasing EU level capabilities to complement the action of Member**

<p><b>States</b>, in particular in the case of cross-border cyber crises.</p>
<p>Under this scenario, the factor of change that would significantly help meet the objective of increased EU capabilities is the provision to grant ENISA a more precise mandate on the range of the operational activities it could perform.</p> <p>ENISA would develop its existing <b>prevention</b> capabilities within the <b>cybersecurity lifecycle</b> (incident prevention, detection, response) and would be able, upon request and limited to pre-identified services (see description of the option for more details) to provide additional ‘EU operational capacity’ to complement the action of Member States. This option in fact foresees an increase in the <b>existing capabilities</b>, in particular linked to: the organisation of the pan-European cybersecurity exercises; the support to operational cooperation within the CSIRT Network, including the provision, upon Member States request, of technical assistance in case of significant incident; the function related to incident analysis; the involvement of ENISA in the blueprint for cyber-crisis cooperation.</p> <p>These tasks are expected to have a positive impact on the success of incident prevention, detection and response both at Member State and Union level. While response would remain the competence of Member States, ENISA could significantly support those Member States who would request to strengthen their own capabilities and react in case of incidents and all Member States in developing a cooperative response in case of large scale cross-border incident.</p>
<p><b>Objective 4:</b> Increasing awareness of citizens and businesses of cybersecurity issues.</p>
<p>Increased cybersecurity awareness of citizens and businesses can only be achieved if all the concerned actors, from the public authorities to the individual citizens/employees, engage in the pursuit of this objectives. Under this option, an enhanced agency would partly contribute to this result by positioning itself as a centre of excellence for EU knowledge and information in this field. This would in fact entail a series of activities that are expected to positively impact the overall level of information and knowledge of cyber issues. It would include: the promotion and sharing of best practices from across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies; the provision of advice, guidance and best practices for the cyber hygiene within the organisations; and the regular organisation of awareness raising campaigns in coordination with the responsible authorities in the Member States.</p>
<p><b>Objective 5:</b> Increasing the overall <b>transparency of cybersecurity assurance</b> of ICT products and services in order to strengthen trust in the digital single market and in digital innovation.</p>
<p>Through the direct involvement of ENISA in the development and implementation of EU policy on ICT security certification, this option would contribute to achieve the objective of increasing the overall transparency of cybersecurity assurance of ICT products and services.</p> <p>The extent to which ENISA will be able to effectively contribute to this objective will depend on the policy approach finally taken with regard to certification, in particular whether it goes towards voluntary measures or mandatory requirements (see section 6.2).</p>
<p><b>Objective 6:</b> Avoiding <b>fragmentation of certification schemes</b> in the EU and related security requirements and evaluation criteria across MS and sectors.</p>
<p>Under this option, ENISA could effectively contribute to avoiding the fragmentation of certification schemes by supporting the development and maintenance of either an EU-wide scheme (as identified in section 6.2 as the extension of current SOG-IS agreement) or an EU framework for ICT security certification. In addition, linked to the possible establishment of an Expert Group (for further information see option 3 in section 6.2 below), ENISA would help the Commission provide the secretariat of the Group.</p>
<p><b>Efficiency/Economic impact</b></p>
<p>The overall <b>impact on the EU economy</b> of reinforcing an EU agency on cybersecurity could not be estimated. Indeed, the lack of reliable detailed data and analyses related to the impact both of</p>



increased network and information security and of cybersecurity incidents is widely acknowledged. As presented in this impact assessment, this is one of the key drivers of the problems this initiative aims to tackle. It is however possible to infer that a reinforced instrument supporting capabilities, prevention, cooperation and awareness at EU level, and therefore designed to increase overall EU cyber resilience, will have a positive economic impact by helping to reduce the costs of cybersecurity/cybercrime incidents, for which the estimated economic impact in the Union stands at 0.41% of EU GDP (i.e. around EUR 55 billion ).

With regard to the **EU budget** and the overall functioning of the Agency, **efficiency gains** can be expected by the reform of the Agency. It is expected that the new set-up would help address some of the weaknesses identified in the course of the evaluation. As regards to the difficulties in recruiting and retaining highly qualified experts, this issue will be mitigated by the possibility for the Agency to offer better conditions of employment. In particular, the new tasks assigned to the Agency will increase its attractiveness in the labour market. This applies both to the permanent posts, which are considered more attractive "per se", and the posts for external staff (contract agents and seconded national experts), for which the opportunity to be involved in prestigious and specialised tasks will increase future employability (after the end of the contracts). Finally, the structural links between ENISA and CERT-EU, with the co-location of ENISA's staff dealing with operational matters with CERT-EU, that ensure that ENISA benefits from the needed additional expertise in the field of operational cooperation by leveraging the existing competences in CERT-EU.

The **costs** associated to the option of strengthening ENISA would mostly be borne by the EU budget, while Member States would still be able to provide voluntary financial contributions to the Agency. Under this option, the current budget for ENISA (EUR 11 million ) would need to be increased by about EUR 9– 12 million per year and be brought to about EUR 20- 23 million, covering the costs for about 50 additional staff members, equipment and meetings required by the new activities. In terms of staffing needs, it is estimated that 36 additional FTE would be permanent posts and 14 FTEs would be external posts (contract agents and seconded national experts) Annex 6 presents detailed breakdown of economic estimates.

It has to be noted that an increase of the EU contribution to the Agency would be accompanied by economies of scale in collecting relevant information on risks, threats and vulnerabilities and possibly in stronger operational cooperation at EU level, which would in turn benefit Member States' finances.

**National public authorities and businesses** are not expected to bear costs, as under this option it is foreseen that the Agency would continue to provide its services free of charges. At the other end, public and private organisations are expected to enjoy direct and indirect economic benefits. The direct benefits would derive from the reduced investment needed in high quality commercial analyses and reports, as they could use those provided by the Agency, with the added value of receiving information, recommendations and good practices from an independent source with an EU-wide perspective. In addition, businesses would incur into indirect economic benefits deriving from a more harmonised policy approach to cybersecurity in the EU, in particular with regard to baseline security requirements, and the expected reduction of cyber incidents that would improve their overall competitiveness (see section below).

### **Impact on competitiveness, competition and SMEs**

Under this option, the Agency would perform several functions that could lead to increased competitiveness of the EU businesses, in particular for SMEs.

Providing adequate support to EU common policy objectives and standards for security and resilience could facilitate businesses' investments, including cross-borders. In particular, this applies to the role of facilitator in the establishment and take-up of European and international standards for risk management, and for the security of electronic products, networks and services. This focuses on the cooperation with Member States on technical areas concerning the security requirements for operators of essential services and digital service providers. A positive impact on

competitiveness would furthermore derive from support for increased resilience, by providing the advice, guidance and best practices for the security of critical infrastructures, by developing excellence in the security of the internet infrastructure, and by supporting the sectors identified in Annex II of the NIS Directive (energy, transport, health, water, banking, financial market infrastructure).

The businesses operating in the cybersecurity sector could also benefit from the information provided by the agency's function of market observatory, which would make the analyses of the main trends in the EU cybersecurity market available in order to enhance alignment of the demand and supply and thus enhance the competitiveness of the companies in the sector.

For SMEs and micro-enterprises, the access to free, high quality and independent information, analyses and recommendations can significantly relieve their budgets, for which investments in cybersecurity can represent a significant burden. This particularly applies to the dissemination of good practices of cyber hygiene, since this could limit the currently high incidence of incorrect human behaviours on the overall number of incidents affecting companies. It has however to be noted that the overall positive impact on SMEs/microenterprises can be limited through linguistic barriers. Unless the agency would be able to devote an increasing part of its resources to translation services or national experts, cooperating with the agency would involve translation responsibilities, and the dissemination of material exclusively in English limits its accessibility throughout the EU.

### **Environmental impact**

No significant environmental impact is expected for any of the objectives.

### **Social impact**

A positive, although indirect, impact can be attained on the social sphere. As extensively presented throughout the report, cyber incidents can have far-reaching consequences for the society. The incidents related to connected devices that are increasingly represented by consumer goods used in the everyday light further exemplify the risks incurred. A reformed EU agency can contribute to achieving increased security and trust of EU citizens and businesses in the digital society. This is in particular relevant for the protection of their access to essential services, such as energy, healthcare, water, transport, as well as the security of personal data.

### **Coherence with other policies**

#### **Internal market – NIS policies and the Digital Single Market Strategy.**

The initiative would be highly coherent with the existing and forthcoming policies, in particular in the area of the internal market. Indeed, it is designed according to the overall approach to cybersecurity, as defined by the review of the Digital Single Market Strategy, in order to complement a comprehensive set of measures, such as the review of the EU Cybersecurity Strategy, the blueprint for cyber crisis cooperation and the initiatives to fight cybercrime. It would ensure alignment with and build on the provisions of the existing cybersecurity legislation, in particular the NIS Directive, in order to pursue further the cyber resilience of the EU through enhanced capabilities, cooperation, risk management and cyber awareness.

The overall impact on the internal market can be expected to be positive. By contributing to ensure better cooperation, more harmonised approaches to EU cybersecurity policies and increased capabilities at EU level, a more effective agency will most likely help reduce market fragmentation, build trust in digital technologies and thus reinforce the internal market.

### **Impacts on Fundamental Rights.**

The initiative follows the main principles set out by the Cybersecurity Strategy, according to which fundamental rights are promoted and protected online in the same way and to the same extent as in the offline world.

By strengthening ENISA's expertise and support to EU policy makers, national authorities, businesses and citizens, this option is expected to help face threats such as those related to security

breaches and unauthorised access to data. It therefore promotes the safeguard of information-related rights enshrined in the Charter of Fundamental Rights, particularly the right to the protection of personal data and private life. These are highly critical issues, considering that only in 2016 about 183.4 million data records were lost or stolen in Europe due to security breaches (+93.5% in comparison to 2015).

### Impacts on innovation.

This option is slated to have a positive impact on innovation. A reformed ENISA can in fact be a valuable partner for both industry and academia in the field of cybersecurity research and innovation, leveraging its practical expertise in areas such as cooperation, information sharing and regulatory requirements. In particular, under this option ENISA would support the development of Cybersecurity Research Agendas at EU and national level by providing input to the strategic analysis of trends with regard to threats, incidents and available solutions and feed into the new European Hub of Excellence in Cybersecurity, as developed in the context of the review of the Cybersecurity Strategy.

### Stakeholders' support

The **vast majority of stakeholders** across all categories appear to **welcome this option**. In particular, the results of the public consultation show that ENISA is perceived by all stakeholders as having the potential to help bridge the most important gaps in the current EU by fulfilling a number of roles, such as support for: stronger cooperation between different authorities and communities; stronger EU cooperation mechanisms between MS, including at operational level; improving capacity in Member States through training and capacity building; and improving research to address cybersecurity challenges. Respondents from national authorities, in contrast to those from the industry, also specifically singled out a role for ENISA in the development of a harmonised framework for ICT security certification.

This has been further confirmed by the meetings and the interviews held with representatives of Member States' authorities and industry stakeholders. The evaluation also clearly showed that often ENISA's stakeholders express different needs which could lead to a more or less strong desire for intervention by an EU body. However, there is common agreement on the need to have (as a minimum) a well functioning agency, with a permanent mandate, which is adequately resourced and mandated to face the present and future cybersecurity challenges.

Further information on stakeholders' views is presented in Annex 2.

## **Option 3 EU cybersecurity agency with full operational capabilities**

### Effectiveness

#### **Objective 1: Increasing capabilities and preparedness of Member States and businesses.**

This option would significantly contribute to achieving the objective. In addition to the positive impacts described in Option 2, this option would increase the capacity of both Member States and the private sector to handle and respond to incidents by **providing CERT-like services**. By creating and maintaining the capacity to provide technical operational assistance to Member States CSIRTS, operators of essential services, EU bodies and institutions, the reformed ENISA could significantly step up the capabilities and preparedness of Member States and businesses.

These additional operational (responsive) capabilities can be considered a real added-value, since it would be provided to those organisations that are expressing a need and it would ensure, among the other things, that in the case of an incident or an attack, the agency can be called upon to intervene and to issue EU-level flash reports that would inform the public of the situation and, if need be, provide guidance to citizens and businesses. This would help strengthen the capabilities

of those Member States that are currently less resourced and equipped and support the more advanced Member States in gaining an EU-wide picture in crisis situations. Furthermore, in a context where organisations network and the information systems are so interconnected, bringing additional capabilities to those who are in greater need would result in an overall increased preparedness of the EU.

**Objective 2: Improving cooperation and coordination** across Member States and EU institutions, agencies and bodies.

This option would significantly contribute to achieve objective 2. The impact described for option 2 equally apply to this option. In addition, an EU cybersecurity agency with full operational capabilities is expected to achieve **increased operational cooperation and coordination**. Building on its role of secretariat of the CSIRT Network but enhanced with capacity for **real time monitoring of threats and response**, the reformed ENISA would be able to **contribute to the information exchange within the CSIRT Network**. It would maximise its output by providing real time **situational awareness reports and dynamic threat intelligence feeds accessible to all CISRTs** and, in times of crisis, to the operators of affected critical infrastructures.

Furthermore, a higher degree of coordination would be achieved, as the Agency would pool the national resources, in terms of available information, to **coordinate the operations** of the CSIRTs in case of incidents with cross-border dimension. This would avoid overlaps and maximise the possible synergies in handling the situation and mitigating its effect. In this context, there would be **full operational coordination with the EU institutions**, ensured by structural cooperation with **CERT-EU** (integration) within the context of the CSIRT Network, but also in relation to capacity building of the EU institutions (see below).

**Objective 3: Increasing EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.

This option would fully meet objective 3. In fact, it would ensure that the Agency would provide the function of **European CERT**, providing all Member States and operators of essential services with support throughout the cybersecurity lifecycle - from incident prevention to response. While currently ENISA does not have CERT functions, the capacity for it could be built, for example by building on the existing competences in CERT-EU.

This approach would bring about a more radical change in the current scope of ENISA's mandate and the way operational cooperation is organised at EU level. It is expected to effectively achieve objective 3 by:

- Ensuring that the expertise and the information generated by the **operational** ('on the ground') side would **feed into strategic analysis**, the advisories and the function of facilitating enhanced EU-wide operational cooperation;
- Increasing the **overall cybersecurity capacity**, currently below the needed critical mass, and by **consolidating the competences at EU level**;
- **Granting the Member States**, with effective **ongoing hands-on support** on operational matters, in particular in terms of incident response.

In addition to option 2, under this scenario ENISA would take a **coordination role** in the implementation of the blueprint for cyber crisis cooperation.

**Objective 4: Increasing awareness** of citizens and businesses of cybersecurity issues.

This option, as presented above in option 2, will partly contribute to achieving objective 4. In addition to the impact described earlier in relation to 'Reformed ENISA', it would lead to a more effective situation awareness of citizens and businesses. In fact, the Agency would provide a service that currently does not exist at EU level, which refers to **fast information and guidance** in

a format accessible to the general public in the case of a significant cross-border incident.
<b>Objective 5:</b> Increasing the overall <b>transparency of cybersecurity assurance</b> of ICT products and services in order to strengthen trust in the digital single market and in digital innovation.
The expected impact is the same presented for Option 2 (see above).
<b>Objective 6:</b> Avoiding <b>fragmentation of certification schemes</b> in the EU and related security requirements and evaluation criteria across MS and sectors.
The expected impact is the same presented for Option 2 (see above).
<b>Efficiency/Economic impact</b>
<p>The impact on the EU economy, as well as the one on the investment needed by public authorities and businesses, is expected to be to some extent higher than what is presented under option 2. It is possible to infer that adding more operational capabilities at EU level to complement the action of Member States can only be beneficial to the overall cyber resilience of the Union. This support would be provided to the organisations where and when it is most needed. As it has been extensively presented throughout the report, an increased resilience is conducive to higher economic prosperity.</p> <p>This option would entail efficiency gains due to the new functioning of the Agency as presented in the previous section assessing the efficiency of option 2.</p> <p>The <b>costs</b> associated to the option of reforming ENISA to make it an agency with full operational capabilities would mostly be borne by the EU budget, while Member States would still be able to provide spontaneous financial contributions to the Agency. Under this option, the current budget for ENISA (EUR 11 million) would need to be increased by about EUR 17 million and be brought to about EUR 28 million. This would include the costs needed for the initial set-up of the unit providing real time threat monitoring and the set-up of the team dealing with EU-wide support for incident response. In terms of human resources, a total of about 70 additional staff members (44 permanent posts and 26 external staff) are estimated during the start-up phase, which could further increase after some years depending on the assessment of the requests received by Member States. Further information on the analysis of the economic impact is presented in Annex 6.</p>
<b>Impact on SMEs, competitiveness and competition</b>
The expected impact is the same as presented for Option 2 (see above).
<b>Environmental impact</b>
No significant environmental impact is expected.
<b>Social impact</b>
The expected impact is the same as presented for Option 2 (see above).
<b>Coherence with other policies</b>
<b>Internal market – NIS policies and Digital Single Market Strategy.</b>
The expected impact is the same as presented for Option 2 (see above).
<b>Impacts on Fundamental Rights.</b>
The expected impact is the same as presented for Option 2 (see above).
<b>Impacts on innovation.</b>
The expected impact is the same as presented for Option 2 (see above).
<b>Stakeholders' support</b>
The <b>stakeholders expressed divergent views</b> on this option. The different needs of ENISA's stakeholders, as they emerged from the evaluation and the consultation process, lead to a lack of

consensus on whether the Agency should take on a more operational role - expanding into real time monitoring of threats and incident detection and response - or continue to remain strictly on the prevention side of the cybersecurity landscape. In particular, industry stakeholders are more positive about ENISA becoming more "hands on" in handling threats and incidents. The same applies to some Member States, in particular those that are less equipped and resourced, as they count on additional support at EU level and this could at least partially help bridge the gaps with other countries. On the other hand, the Member States that are more advanced in terms of capabilities and preparedness expressed concerns about a more radical transformation of the Agency. This departs from a model of the cybersecurity agency with full operational capabilities which is increasingly used at national level, but which is not deemed appropriate for ENISA due to, among the other things, the possible overlaps with the mission of national agencies.

Further information on stakeholders' views is presented in Annex 2.

## 6.2. Certification

### Option 1: Non-legislative ("soft law") measures

<b>Effectiveness</b>
<b>Objective 1: Increasing capabilities and preparedness of Member States and businesses.</b>
Under this option, voluntary activities related to certification may be promoted intermittently. This may produce some positive impact on the increase of cyber resilience in the EU, but in a limited and indirect manner.
Option 1 would provide a low incentive to invest resources to developing relevant expertise and facilities (e.g. conformity assessment bodies) - which involve high economic impact. In light of the fast-moving threat landscape and increased complexity of attacks, this option would have a detrimental effects on the capabilities and level of preparedness of Member States, business and critical infrastructure, which would remain uneven.
In the case of co-regulation, there is a risk that the entrusted market operator may decide to promote new certification schemes that are designed to minimise its costs of compliance rather than to satisfy a public need for better ICT security. In addition, co-regulation may not be a viable political option given the high sensitivity that Member States attach to issues such as of security of their critical infrastructures.
<b>Objective 2: Improving cooperation and coordination across Member States and EU institutions, agencies and bodies.</b>
In the absence of an institutional mechanism fostering a European approach on the policy priorities in this field, Member States are likely to generate uncoordinated approaches to certification . In addition, cooperation and coordination would be undermined as Member States are likely to promote their national scheme and boost its reputation. This may trigger competition among similar national schemes with Member States failing to accept certificates from foreign or private schemes.
<b>Objective 3: Increasing EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises.</b>
This option will not produce any significant impact to increase EU level capabilities that complement the actions of Member States.
<b>Objective 4: Increasing awareness of citizens and businesses of cybersecurity issues.</b>
A soft-law approach may offer quick and cost-effective ways to embark on cybersecurity certification. This can incentivise businesses to resort to certification as a way to make customers and citizens aware of cybersecurity threats and solutions. Public authorities can lend support and encourage this approach, therefore strengthening overall awareness levels. This option may

however at the same time, have some negative impact on reaching this objective. Due to their flexibility, the soft laws instruments envisaged in this option would not act as a deterrent to the proliferation of schemes and standards. As a result, **businesses** and **end-users** (e.g. operators of critical infrastructures and citizens) may still be in a situation where multiple schemes or standards exist. Such a variety engenders lack of readability and comparability, meaning that these actors will face difficulties to judge which scheme or standard would best satisfy their particular requirements. This would increase the risk that these actors use inappropriate products or services, thus lowering the level of security of their operations.

Similarly, the development of a EU scheme through soft law would materialize on condition that public authorities, vendors and operators are highly committed and ready to mobilize resources. It is generally expected a long period of time for these conditions to occur and thus for a EU scheme to emerge. As a result, only few products and services certified according to a EU schemes would be available on the market for end-users (citizens and operator of critical infrastructures).

**Objective 5:** Increasing the overall **transparency of cybersecurity assurance** of ICT products and services so as to strengthen trust in the digital single market and in digital innovation.

While the soft measures identified in this option may to a certain extent contribute to improving the current lack of overall transparency of information of ICT products and services, they also present a number of limitations. Essential elements of certification schemes would not be binding and would therefore only act as best practice recommendations. Similarly, self-regulatory initiatives typically lack legal regulatory oversight and regular monitoring systems. This circumstance increases the risks of deceptive behaviours, that can ultimately undermine the trust in and effectiveness of these type of initiatives.

European Commission support, coordination and encouragement of industry-driven initiatives is indeed expected to help private operators in their effort to establish schemes. However, the success of these initiatives depends on the goodwill and agreement of the participating stakeholders. In addition, negotiations among stakeholders may occur on an ad-hoc basis, may take considerable time, or may fail, while there is no guarantee that newly established schemes are widely accepted across national authorities. All self and co-regulatory efforts would necessarily follow a piecemeal approach rather than a well defined strategic design, and could entail a cumbersome and resource-intensive process. This option may therefore cause a low incentive to embark on voluntary activities, with detrimental effect on the overall need for more transparency of information on the cybersecurity of ICT products and services.

Research and raising awareness in the field of ICT certification would be very helpful as a collateral measure, but would not fully address per se the main issue of the lack of transparency on the security assurance levels of ICT products and services.

**Objective 6:** Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across Member States and sectors.

Under this option, the existing national certification schemes will still use different procedures, unless Member States agree on ad hoc mutual recognition agreements. In addition, sectorial certification initiatives are expected to proliferate, as the need to ensure cybersecurity becomes more pressing across sectors. This would lead to a possible scenario of a twofold fragmentation across Member States and sectors. Such a fragmentation is also likely to persist as each MS would continue to use and improve its national scheme; thus creating a strong legacy and reluctance to adopt equivalent schemes from other Member States.

The effects of this uncoordinated proliferation of multiple approaches to cybersecurity certification are likely to be that **vendors** as well as **consumers and end-users** making cross-border purchases will not necessarily be able to compare and understand the security properties of the devices purchased.

## Efficiency/Economic impact

The Commission would need to bear costs related to the implementation of the measures proposed under this Option: e.g. bear costs to issue guidance, follow the standardisation efforts, facilitate self / industry led-initiatives to the extent possible, and launch awareness raising campaigns. It is estimated that this would require two administrators and one assistant working full time on these matters (running cost).

The launching of an awareness raising campaign may require the help of an external contractor or EU agency such as ENISA. The cost may be estimated in the region of EUR 250-400,000 depending on the tools employed (one-off cost).<sup>117</sup> The funding of projects under the CEF may be dedicated to upgrade existing testing facilities or building new ones.

**National authorities** should be involved in the co-regulatory efforts on a voluntary basis. This cost would vary according to the number of meetings and the degree of cooperation. Assuming that many issues may be steered by the Commission (e.g. a conservative estimate of three meetings a year for three years), the cost may be estimated to be between EUR 2,500 and 7,000 per authority/per annum (running cost)<sup>118</sup>. Similarly, national authorities would need to finance participation in efforts towards coordinated enforcement. Assuming in this case two meetings per year, the annual cost would be between EUR 1,700 and 4,700 (running cost). Minimal compliance costs for Member States' authorities to get familiar with the new implementing/soft law measures would be around EUR 1,000 per authority (1 day of training) (one-off cost)<sup>119</sup>.

Businesses would benefit from a fast and cost-effective approach for the development of voluntary tools. A soft law approach would also imply a higher level of engagement and greater influence of business in the process of developing tools (e.g. guidelines, certification schemes etc) that better suit market sensitivities. As such, this may produce an incentive for industry to resort to ICT certification as a way to improving the quality of their products and possibly increasing their market share. However, industry will incur some costs for the participation in activities, such as establishing codes of conduct and standard-setting etc. Considering past similar exercises, it could be assumed that the increase of cost would be moderate, as participation would be voluntary and normally only a relatively small proportion of businesses participate in such activities (running cost for the duration of the standardisation activities). Indeed, some businesses already participate in such activities<sup>120</sup>. Businesses would be more extensively affected by the specification of EU standards, to the extent that they would implement the new standards (one-off cost and lower running cost ensuring updates). Depending on the content of such standards, companies concerned may be more significantly affected. However, the implementation of such standards will essentially depend on the decision of each and every firm (i.e. it will be voluntary). Therefore, it is not possible to provide a clear and precise estimate of the magnitude of the impact. Some cost savings (especially for industry already subject to certification requirements) would occur if a EU-wide certification schemes in specific sectors is established. This would enable industry to certify their products and services only once and against a scheme that is recognised in the whole of the EU. However, given the voluntary nature of this option and the absence of a formal governance structure for ICT certification in the EU, industry will have to invest significant resources (both human and financial) to reach consensus among various actors (both private and national) on the development of a ICT certification scheme that is widely accepted across Member States.

In conclusion, this option presents *moderate/low* implementation costs for the Commission and

<sup>117</sup> This means that costs will be lower in case e.g. only an online campaign would be launched. In case e.g. an EU-wide awareness-raising campaign is launched with printed materials, informative events, discussion rounds etc., the costs will of course be higher than this estimate.

<sup>118</sup> This is based on the assumption that between one and two persons per MS might join, that they need to spend time on travel, the meeting itself and preparation considering the hourly salary quoted by the Commission and that they need to pay for flight and in some cases for one night accommodation.

<sup>119</sup> Familiarisation/training costs= 3 staff-members per authority needing training \* hours spent on training per staff (8 hours) \*staff costs per hour (hourly wage rate EUR 41.5, Eurostat data 2012).

<sup>120</sup> Examples are the cloud computing group and the C-ITS group.



Member States. In particular, the weak benefits/cost savings for businesses in Option 1 would indeed materialize, but only after a successful completion of a scheme. However, such a process would imply additional costs and generate some inefficient allocation of resources. At the same time, the dissemination of additional guidance may contribute to enhance legal certainty.

#### **Impact on SMEs, competitiveness and competition**

The impact on SMEs under this option would depend on their willingness to participate in the development of guidelines, certification schemes, standards and best practices recognized across Member States.

SMEs and microenterprises already subject to ICT security certification requirements would have a significant interest in following these voluntary activities. Possible outcomes of soft law activities may improve SME's access to markets. However, contrary to larger businesses, these actors typically have limited budgets. Unless they are willing to bear the costs deriving from participation, microenterprises and SMEs would be mere recipients of the outcome of voluntary initiatives. This implies that they need to understand and apply new guidelines and standards developed by other actors. In addition, under this option any initiative or proposed processes for security certification will be defined without paying attention to the needs of SMEs, with unfavourable effects on their competitiveness.

#### **Environmental impact**

No significant environmental impact is expected for any of the objectives.

#### **Social impact**

To the extent that multiple certification schemes remain in place and the process of developing new European schemes is uncoordinated, the incentive to encourage ICT certification will be low. As a consequence, this option would provide limited support to mitigate the current asymmetry of information among various stakeholders (e.g. **manufacturers, operator of critical infrastructure, citizens**) and foster trust in the Digital Single Market. In particular, ad hoc voluntary initiatives promoted by the Commission would provide limited support to increase the level of assurance of critical infrastructures. Operators would not be able to rely on an institutional framework to express their need for more security, rather they will have to bear the burden of gathering consensus among vendors and national authorities.

#### **Coherence with other policies**

##### **Internal market – NIS policies, digital single market, trade.**

The impact on the internal market may be considered mildly positive. Interpretative communications from the Commission, self and co-regulation initiatives, as well as standardisation activity at EU level would contribute to a certain extent to greater harmonisation and to reducing fragmentation. International trade is promoted to the extent that these voluntary activities adhere to internationally recognized standards.

However, there are also important limitations to the harmonising effects that these measures could achieve. The development of private and national schemes will not be discouraged, leading to detrimental effects on the digital single market. In addition, as measures are not binding, it will rest ultimately on the national authorities and buyers whether or not to propagate the usage of these schemes/measures. Moreover, the success of self-regulatory measures depends on a number of circumstances, such as the degree of participation and compliance by the industry concerned. Finally, since the use of IT certification would not be directly promoted, this option would not help reduce the risk that Member States set different security requirements to demonstrate compliance with the NIS Directive.

#### **Impacts on Fundamental Rights.**

To the extent that ICT security certification will contribute to increase cybersecurity online, these proposed actions will produce a mild increase in the protection of fundamental rights, such as rights to privacy, data protection, security and life.

**Impacts on innovation.**

To the extent that it raises funding for R&D activities in the field of security research and that it encourages the establishment of industry initiatives promoting cyber-certified security solutions, **Option 1** is slated to have a positive impact on innovation.

**Stakeholders' support**

The majority of stakeholders would welcome soft-law initiatives and Commission support to industry-driven initiatives across all categories. However, they are also widely convinced that, in the absence of an overarching European legal framework for certification, these types of initiatives would not by themselves be sufficient to significantly discourage the proliferation of certification schemes and would not increase transparency. Member States have also stressed the risk that providers of essential services operating cross-border could be subject to different security requirements in relation to IT certification.

**Option 2: EU legislative act to create a mandatory system for all Member States based on SOG-IS.**

**Effectiveness****Objective 1: Increasing capabilities and preparedness of Member States and businesses.**

This option would provide Member States with an institutional fora, enabling all Member States to express their security needs related to certification. As a result, Option 2 is expected to help Member States improve their capacity and preparedness, thus generating an overall positive effect on the cybersecurity resilience in the EU.

The SOG-IS MRA community gathers national officials from 12 Member States plus Norway with long-standing expertise in the field of IT security. As such, new members – who will be required to join SOG-IS MRA - are enabled to gain relevant competence in this area. However, any concrete action to increase both capabilities and level of preparedness remains at discretion of each Member State. In addition, it is important to note that new members are expected to join the SOG-IS MRA as 'certificate consumers' from the outset, with a view to becoming a 'certificate producers' once adequate expertise and facilities will be built. Once again, such a decision would be voluntary. In addition, the impact of this option on level of capabilities and preparedness of critical infrastructures may depend on the extent to which Member States decide to foster the use of SOG-IS-certified products (e.g. through public procurement) for the operation of critical infrastructures in their territory.

For business, the positive impact on their capabilities and preparedness will highly depend on their level of commitment to adopt the certification methodology promoted under the new SOG-IS MRA.

**Objective 2: Improving cooperation and coordination across Member States and EU institutions, agencies and bodies.**

This option would improve cooperation and coordination among Member States within its product scope, since it provides an institutional mechanism that enables exchange of information and consensus on the policy priorities in the field of security certification. However, in line with the experience of the current SOG-IS MRA, cooperation and coordination may be limited to high level product certification. National and uncoordinated approaches can still proliferate for a wide range of products and services requiring medium to low level of assurance. This is already happening in countries which are members of the SOG-IS MRA. Examples of national schemes include: CSPN in France, CPA in UK and a baseline scheme in Germany. Currently, these schemes are not mutually recognised.

ENISA would help run the Secretariat of the EU-wide SOG-IS. The choice of ENISA for this role is consistent with the need to ensure cooperation and coordination in the area of

cybersecurity (see Option 3, section on effectiveness, for analysis of alternative to ENISA).

**Objective 3:** Increasing EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises.

This option would mildly help meet this objective, to the extent that all Member States agree on the creation of capabilities for certification at EU level. However, this could only be envisaged in the long term. Initially, Member States would be simply encouraged to improve their national capabilities.

**Objective 4:** Increasing awareness of citizens and businesses of cybersecurity issues.

The current SOG-IS MRA has to date undertaken only limited awareness raising activities. This situation is likely to remain unchanged if the MRA is extended to all Member States, unless Member States specifically allocate budget for these activities.

**Objective 5:** Increasing the overall transparency of cybersecurity assurance of ICT products and services so as to strengthen trust in the digital single market and in digital innovation.

**Option 2** would partially contribute to achieve this objective. The SOG-IS MRA, which relies on the testing methodology of CC<sup>121</sup>, has been used to certify only a few digital products requiring high level of assurance (e.g. tachographs, digital signatures and smart cards). This is due to the depth of the evaluation<sup>122</sup> of CC, which generates high costs, and lengthy processes. As such, the CC methodology used by SOG-IS MRA is unsuitable for the security certification of products requiring medium and low level of assurances.

It is therefore expected that this option would foster transparent information only for products requiring high levels of assurance. In addition, there will not be an increase of transparency of cybersecurity of ICT services as the current CC methodology is only suitable for the security certification of products.

**Objective 6:** Avoiding fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across MS and sectors.

Option 2 would partially contribute to achieving the objective. The creation of a mandatory system for all Member States under the SOG-IS agreement would imply that certificates issued under the extended SOG-IS MRA would be recognised in all Member States and not only in the 13 members of the current SOG-IS MRA. However, as SOG-IS certificates are used for products (not services) requiring high level of assurance, the proliferation of national schemes to certify commercial products as well as services – normally requiring a low level of assurance - can still be expected. If not addressed, each Member State would continue to use and improve its national scheme for low levels of assurance; therefore creating a strong legacy and reluctance to adopt equivalent schemes from other Member States.

As previously explained, this is already happening in countries which are members of the SOG-IS MRA. Examples are: CSPN in France, CPA in UK and a baseline scheme in Germany. Currently, these schemes are not mutually recognised.

This scenario is expected to worsen as the demand for some form of IT security covering also commercial products and services grows worldwide.

Overall, the positive impact of Option 2 in solving fragmentation is potentially significant, but limited to high level certification. Not only national schemes for medium, and low level of assurance can proliferate outside the extended SOG-IS MRA, but they can also compete. In this last scenario, Member States may have a little incentive to turn to the mutual recognition of a similar, competing scheme.

<sup>121</sup> For an overview of criticism related to CC, see JRC study Annex 8, pp. 24-26.

<sup>122</sup> The CC methodology is based on third-party evaluation for all its 7 levels of assurances. As such it does not envisage self-evaluation.

### Efficiency/economic impact

The costs for the **Commission** are not very high and essentially coincide with the legislative process. The Commission would have to invest resources to oversee the implementation and extension of the current SOG-IS MRA. It is estimated that this would require two administrators and one assistant working full time on these matters (running cost).

**Member States** will have to implement the new rules. The 13 Member States which are already members of the SOG-IS will not have to bear any significant additional cost. Costs will be more significant for those Member States that are not currently members. According to the data produced by the Interim Report of the technical study, the costs of participation in the SOG-IS MRA for a Certification Authority are approximately EUR 58,000. This includes the participation in Management Committee meetings (1-2 times per year) and the JIWG meetings (3-4 times per year). It also includes yearly travelling costs for three members attending six meetings, the preparation of meetings, attendance and national reporting.

Other costs are related to the start-up of an IT certification (e.g. process setup, development and accreditation of evaluation facilities, institutional communication). However, it should be considered that the SOG-IS MRA provides the possibility for its members to act as certificate 'consumers'<sup>123</sup> as well as certificate 'producers'<sup>124</sup>. Consumers would be able to benefit from a situation in which they simply accept certificates issued from producers, and will have little incentive to invest resources to build the appropriate facilities and expertise to become a producer. As a consequence, existing producing members may face a raise in the demand for certification which will trigger the need for an economic investment aiming to upgrade the existing facilities. However, producers would gain more expertise to set priorities and shape the course of IT security certification in Europe. Conversely, new members of the SOG-IS are expected to join as consumers in order to avoid upfront investment costs related to capacity building and training. As such they would have little incentive to build extensive expertise.

This Option would not imply significant additional costs for **industry**, namely because security certification will remain essentially a voluntary tool. As it is the case today, businesses will remain free to choose whether to certify their products. By contrast, whenever a SOG-IS certificate will be required (e.g. public procurement), business would benefit from a EU-wide mechanism. This would certainly act as a cost-reductor especially for those firms that already use SOG-IS certificates.

### Impact on SMEs, competitiveness and competition

**Option 2** may have a positive effect on SMEs that already rely on the SOG-IS mechanism as they can use certificates throughout the entire EU. In addition, this option may provide an incentive for those SMEs willing to certify their products, as they can rely on such an EU-wide mechanism. However, these positive effects are limited due to the shortcomings of the current SOG-IS MRA (e.g. fit for high level of assurance, duration of process and costs). SMEs would likely not have the resources to go through such a time-consuming and potentially expensive process. It is therefore reasonable to expect that the competitiveness gains will not very high for market operators.

### Environmental impact

No significant environmental impact is expected.

### Social impact

This option would increase the security of our critical infrastructures. Member States may wish

<sup>123</sup> E.g. national authorities accepting certificates issued by other authorities who are members of the SOG-IS MRA.

<sup>124</sup> E.g. national authorities issuing and accepting certificates from other authority's members of the SOG-IS MRA.

to include SOG-IS certificates in public procurements requirements, with a view to enhance the assurance level of critical infrastructures. For their part, vendors would be able to certify their products by relying on a one-stop shop mechanism. This would foster a chain of trust among vendors and operators of critical infrastructures. However, asymmetry of information would persist between vendors and citizens for commercial products requiring medium to low level of assurance.

### Coherence with other policies

#### Internal market - NIS policies and digital single market, trade and international aspects

**Option 2** would have a positive effect on the internal market. The measures at stake would cover some gaps of the existing European certification landscape, partially solving the problems related to its lack of transparency, inconsistency and fragmentation. Accordingly, the option is expected to slightly or moderately enhance harmonisation of certification requirements in the digital single market. The increased cooperation may foster consistency across Member States and possibly promote a common use of ICT certification as a way to demonstrate compliance with the NIS directive. Finally, as the CC methodology relies on an international standard, this option would be aligned with the terms of international trade. This effect is however limited to products requiring high level of assurance.

Option 2 would also lead to a strengthened European position in the international context, and may become a model for other world's regions.

#### Impacts on Fundamental Rights

To the extent that ICT certification will contribute to increase cybersecurity online, these proposed actions will also increase the protection of fundamental rights such as rights to privacy, data protection, security and life.

#### Impacts on innovation

As the constraints of the current SOG-IS would be transferred to its upgraded EU-wide version (e.g. fit for high level of assurance; focus on products rather than services), firms may not consider the extended SOG-IS MRA as a suitable tool to ensure the cybersecurity of their innovative commercial products and services requiring a low level of assurance. They would rather look for more agile (national or private) certification schemes. However, as these schemes are usually used within national boundaries and may not be widely accepted, there would be an incentive to avoid ICT certification in order to cut administrative costs related to multiple certification processes.

#### Stakeholders' support

While stakeholders generally praise the work of SOG-IS MRA and are willing to see SOG-IS scheme thrive in the future as a tool of mutual recognition based on internationally recognised standards (e.g. CC), the majority of stakeholders (especially Member States and industry) are aware of the limitations of the current SOG-IS MRA and therefore consider that a significant adaptation and upgrades would be needed.

### Option 3: EU general ICT security certification framework

#### Effectiveness

##### Objective 1: Increasing capabilities and preparedness of Member States and businesses

Procedures for security certification would be simplified through an EU-wide framework leading to mutual recognition of certificates issued under a European cybersecurity certification scheme. This would provide a strong incentive for Member States and operators of essential services to increasingly resort to security certification (e.g. through public procurements) as a tool to reduce

the vulnerability of critical infrastructures and increase their preparedness.

Rules are simplified and certificates will be valid across Member States. This will incentivise businesses (especially those with cross-border operations and digital service providers) to use security certification as a way to increase preparedness of their operations.

**Objective 2: Improving cooperation and coordination** across Member States and EU institutions, agencies and bodies.

This option would improve cooperation among Member States, since it provides an institutional framework that enables the development of European cybersecurity certification schemes and the development of a common policy in this crucial field. National and uncoordinated approaches in this field would be highly discouraged. Contrary to Option 2, such a positive effect is expected to cover products as well as services at all levels of assurance (high, medium, low). However, the use of European schemes may vary across Member States. For example, some may resort to European schemes to better protect a critical infrastructure while other may not. In an interconnected digital market, this scenario increases the risk of vulnerability and proliferation of threats, even in those Member States adopting higher level of protection through certification. It is therefore expected that, Member States not adequately using certification schemes would face pressure to align with those that do.

Moreover, assigning a role to ENISA in the area of ICT security certification is consistent with the need to ensure cooperation and coordination in the area of cybersecurity. Over the years, the Agency has acquired significant expertise in the area of security certification and standardisation. It has engaged with private sector, notably providers of cybersecurity products and solutions by means of workshops and targeted surveys. It has established channels of dialogue with the national certification bodies and standardisation bodies through participation in the Management Committee meetings of the current SOG-IS MRA and it is in regular contact with the Cybersecurity Coordination Group created by CEN CENELEC and ETSI. The Agency has also authored a number of technical studies on certification and standardisation. In particular, in the area of cloud computing certification, ENISA has developed a meta-framework, which maps the security requirements in existing cloud certification schemes<sup>125</sup>.

DG JRC has been considered as an alternative to ENISA. DG JRC has considerable expertise in this area since it currently hosts testing laboratories for certification of digital tachographs and has published a number of studies that have informed this initiative, among others. However, stakeholders' consultations suggest that JRC's unique technical competence in relation to cybersecurity would be best utilized in support to EU's endeavours in research and development, which are necessary to keep pace with the dynamic nature of digital security. For example, JRC may explore more efficient testing methodologies to carry out ICT security certification. Moreover, resorting to JRC as an alternative to ENISA may be discarded on the ground of political considerations. As security certification may interfere with sensitive areas, national authorities may resist the option of conferring a coordination role to a Commission DG.

**Objective 3: Increasing EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.

If needs arise and on condition that financial resources are available in the future, a specialized European testing laboratory supervised by ENISA could be built to support the capabilities of Member States lacking such facilities. A future European laboratory may also act as a centre of

<sup>125</sup> The Commission has already used the outcome of this project in a large cloud services procurement tender (2500 cloud virtual machines and 2500 Terabyte of cloud storage), which builds upon the 27 security objectives identified in the meta-framework.

competence to conduct experiments with a view to advance the state-of-the-art in the field of security certification.

**Objective 4:** Increasing awareness of citizens and businesses of cybersecurity issues.

ENISA would be tasked with activities related to communication and dissemination of best practices and raising awareness in the field of cybersecurity certification. ENISA has acquired extensive experience in this type of activities and is bound to further reinforce its role and resources in this area. This option would, therefore, greatly improve the awareness of citizens and businesses of cybersecurity issues.

**Objective 5:** Increasing the overall **transparency of cybersecurity assurance** of ICT products and services so as to strengthen trust in the digital single market and in digital innovation.

**Option 3** would partially contribute to achieve this objective. Similarly to the other options presented in this section, in the absence of mandatory requirement to certify, the creation of a framework alone does not have a direct effect on the increase in transparency of cybersecurity assurance of ICT products and services. Nevertheless, a European certification framework increases the value of security certificates as they can be used across Member States through a single process. This creates an incentive for vendors to embark on such a process with a view to increase the quality, and market share of their innovative products and services without the administrative costs of multiple processes. In this respect, initiatives such as the IoT trust label, which aims to satisfy the need for more transparency, would normally fit within the scope of such a framework.

This option would also enable operators of essential services to have more information on the security properties of the digital devices used in their infrastructures, by undergoing the relevant certification procedures for their products and services in accordance with European scheme,

**Objective 6:** Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.

**Option 3** would highly contribute to achieving this objective. This Option would remove the possibility of coexistence of national certification schemes for products and services covered by a European scheme and make the creation of private outside of the future European certification framework significantly less attractive. Certificates issued from schemes outside the framework would face acceptance problems. Similarly, the creation of national schemes remains possible, but limited to national security, which is a narrow and sensitive area. For this reason, these national schemes are expected not to interfere with future EU schemes under the framework, that would be mainly designed for improving the security of the digital single market.

### Efficiency/economic impact

The costs for the **EU** institutions, **ENISA** and **Member States** coincide with the establishment and maintenance of this European Framework. In particular, the European Commission would have to place resources to support the establishment of the framework, notably for the adoption of the European schemes by means of delegated acts or implementing acts. It is estimated that this would require three FTEs working full time basis (e.g. two administrators and one assistant)

The EU institutions would also bear the costs related to the set up of the Expert Group. Typically, the Commission allocates 600 Euro per expert who will qualify for travel reimbursement. Since each Member State will appoint a representative, the total cost of the group is estimated to be in the region of 16,000 - 17,000 Euro per year.

ENISA is expected to bear the bulk of the costs related to both the functioning and maintenance of the framework, as it will be in charge of a) preparing the candidate schemes and b) issuing

guidelines and c) help the Commission provide the secretariat for the Group. The institutional costs related to ENISA are included in the economic estimates for ENISA (see Annex 6).

As an alternative to ENISA, it has been estimated that establishing a new body with the appropriate expertise in such a complex area would take between 5-7 years. Approximately, the costs of setting up a new European body amount to EUR 21,9 million. ENISA as the EU agency for cybersecurity with strong links with Member States has been considered to be best placed to ensure a coordinated and efficient approach to any European effort on security certification, for example by bringing all relevant stakeholders together, coordinating their work on certification schemes, preparing certification schemes and provide technical expertise.

Member States appointing a competent certification authority are expected to bear costs that would approximately amount to 1,600,000 Euro per year<sup>126</sup>. This estimate include costs related to personnel, equipment, subcontracting, operations (incl. training conferences) as well as set up of evaluation facilities. The operational management of a certification authority would also require investments for carrying out enforcement and supervision activities. Costs related to these activities are in the region of 290,000-300,000 Euro (per year) Generally, the overall impact will be significantly lower (or neutral) on Member States that are already part of the SOG-IS MRA and that have a supervision authority already in place.

This Option would not impose additional costs for the industry in the short term, namely because certification will remain essentially a voluntary tool. As is the case today, businesses will remain free to choose whether to certify their products or services. By contrast, the possibility to obtain an EU wide certificate would certainly act as a cost reductor for those firms that already certify their products or as an incentive for those that are willing to do so.

Since the certification process involved in future European schemes would depend on the associated level of assurance, cost and duration would be reduced compared to the current SOG-IS MRA, built on the lengthy and complex CC methodology.

### **Impact on SMEs, competitiveness and competition**

**Option 3** would have a very positive effect on competitiveness, as it would significantly reduce costs and administrative burden for SMEs that already certify or are willing to certify their products and services at various level of assurance. This option would also eliminate a potential market-entry barrier (for both new business and SMEs) and enable access to a wider cybersecurity market.

The mutual recognition mechanism would also boost the competitiveness of firms operating cross-borders, by providing an incentive to certify their products and thus help them reap the advantages of increased trust in the digital solutions and gaining access to market segments where certification is required (e.g. some areas of public procurement).

In addition, this option would foster expertise in the field of IT certification, in particular among the business community operating in Europe. A security-by-design approach also for mass products and services would be encouraged as a consequence. Since the demand for more secure solutions is expected to raise worldwide, industry (incl. SMEs) operating under the European framework would enjoy a competitive advantage to satisfy such a need, therefore potentially gaining shares in the global market.

### **Environmental impact**

No significant environmental impact is expected.

<sup>126</sup> Approximately amount for the first 3 years. More details can be found in the support study (Annex 7)



## Social impact

Certification of products and services at various level of assurances will enable end-users to make more informed purchase decisions. This would also help maintain a chain of trust among various stakeholders - from the manufacturer to the operator of critical infrastructure up to the final end-user (public authorities, citizens). The current asymmetry of information would be reduced. In particular, this option would enhance the level of assurance of critical infrastructures, since operators would have an institutional structure to express their need for ICT certification.

## Coherence with other policies

### Internal market – NIS policies, digital single market, trade and international aspects

**Option 3** would have a positive effect on the internal market. The measures at stake would address the potential fragmentation caused by existing and emerging national certification schemes, therefore contributing to the development of the digital single market. Accordingly, this option is expected to promote convergence on the creation of new European certification schemes whenever a need arises, thus addressing the risk of multiple approaches across Member States.

Moreover, this option supports and complements the implementation of the NIS Directive by providing the undertakings subject to the Directive with a tool to demonstrate compliance with the NIS requirements in the whole Union. In developing new cybersecurity certification schemes, the Commission and ENISA should pay particular attention to the need to ensure that NIS requirements are reflected in the certification schemes. The undertakings subject to the NIS rules may thus use certificates issued under the European schemes as an element to be taken into to demonstrate their compliance with the NIS Directive.

Under this option, the functioning of the European ICT security certification framework will be designed to ensure full coherence with the General Data Protection Regulation (GDPR)<sup>127</sup> and in particular with the relevant provisions on regarding certification<sup>128</sup> as they apply to the security of the processing of personal data.

An EU level ICT security certification framework which is proportionate and wherever possible based on international standards would significantly contribute to an international trade-friendly level playing field for products and services.

To the greatest extent possible the schemes proposed in the future European framework would rely on international standards as a way to avoid creating trade barriers and ensure coherence with international initiatives. For example, the current SOG-IS MRA, which coordinates the standardisation of the international Common Criteria methodology among its European members, is likely to be included in the future Framework as the European scheme for high level certification. In addition, a European framework will support the coordination of certification policies among European certification bodies, thus promoting a common position in the international CCRA ,

### Impacts on Fundamental Rights.

To the extent that ICT certification will contribute to increasing cybersecurity online, these proposed actions will also increase the protection of fundamental rights such as rights to privacy, data protection, security and life.

<sup>127</sup> Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

<sup>128</sup> Such as Articles 42 (Certification) and 43 (Certification Bodies) as well as Articles 57, 58, and 70 regarding respectively the relevant tasks and powers of the independent supervisory authorities and the tasks of the European Data Protection Board.

### Impacts on innovation.

**Option 3** would promote the production of innovative, more secure, digital solutions for which a high demand is expected globally. The development of an innovative solution may not be sufficient to acquire market shares if its cybersecurity is neglected. For example, Fabasoft (an innovative Austrian SME) has used security certification<sup>129</sup> to build its credibility as provider of secure eGov solutions, and gain access to other markets (Germany) through public procurements<sup>130</sup>

Furthermore, the cooperation between ENISA and standardisation bodies would enable to monitor the appropriateness of standards used in a European scheme so that they ensure an adequate level of both security and technological innovation. Such a monitoring exercise would mitigate the risks related to the obsolescence of standards that may provide buyers with a false sense of security.

### Stakeholders' support

The majority of stakeholders are in favour of the creation of a voluntary, scalable European framework based on a mutual recognition of certificates, and including all Member States. However, representatives from industry and national authorities have stressed the necessity to provide adequate staff in order to support the functioning of this Framework. For this purpose, it was suggested that ENISA, among other tasks, helps carry out secretarial tasks.

## 7. HOW DO THE OPTIONS COMPARE?

This section presents a comparison of the options in the light of the impacts identified. The options are assessed against the three core criteria of effectiveness, efficiency and coherence, as well as taking into account the support expressed by the different stakeholders.

### ENISA

Table 5 below presents a comparison of the options based on the analysis of the options 0 and 1 and the detailed assessment of the options 2 and 3. The comparison is mostly based on a qualitative analysis, while quantitative data support the assessment of the economic impact and efficiency. With regard to this criterion, it is assessed the expected impact on the EU economy as well as the financial implications for the EU budget. As stressed since the beginning of this report, **the impacts of the options for the future of ENISA cannot be considered as generated exclusively by the Agency, as no entity can have a standalone impact** in cybersecurity. Therefore, the effort here made is to focus as much as possible on the impact that can be attributed to the Agency, while taking into account the contextual elements and the other known instruments.

Having regard to the **effectiveness**, it appears that both option 0 (baseline) and option 1 (expiry of ENISA mandate) would not be able to achieve the objectives of the initiative which call for increased capabilities, cooperation, transparency and reduced fragmentation. With respect to the baseline, both option 2 and 3 are clearly more effective. A 'Reformed ENISA', which builds on the NIS Directive, including in terms of

<sup>129</sup> A list of security certificates acquired by Fabasoft are available here: <https://www.fabasoft.com/en/group/transparency/certifications-audits>

<sup>130</sup> Certification is obviously not the only criteria taken into account, but fostered a reassurance that Fabasoft innovative solutions are also secure.

operational cooperation, and the key strengths highlighted in the evaluation (such as the cyber exercises and the community building) and provides support in such a key area for the market as security certification for ICT products, is expected to effectively contribute to most objectives. Option 3 is deemed more effective than both baseline and option 2 in relation to meeting the objective of increasing EU level capabilities to support Member States and the overall preparedness of the EU, especially in times of crisis.

The **economic impact** of option 0 and option 1 is deemed to be negative. Under the baseline scenario, ENISA would continue for a fixed number of years to receive funding from the EU budget – which being rather small in comparison to the investment in other agencies can be judged as 'efficient' – but with its current mandate and resources would not be able to properly support Member States, EU institutions and businesses, with indirect negative consequences on the economy. In comparison to the baseline, both option 2 and 3 bear advantages. A 'Reformed ENISA' is expected to bring positive effects for the cyber resilience and the internal market while still staying an agile organisation which would require a financial contribution from the EU higher than it is currently the case but still fairly below other agencies that also operate in critical areas (in the range of about EUR 23 million per year). The option 3 is expected to have further reaching economic benefits than option 2 (and the baseline) because the Agency would be able to provide an extra operational help to both Member States and operators of critical infrastructures. At the other end, the option of a cybersecurity agency with full operational capabilities would put higher pressure on the EU budget (associated costs estimated at about EUR 28 million per year, including the costs needed for the initial set-up). Both option 2 and option 3 are still considered efficient as potentially conducive of 'high value for money'.

In terms of **social impact**, option 1 is expected to have negative consequences in comparison to the baseline, while option 2 and 3, as presented earlier can provide increasing level of cyber resilience and thus positively impact the social sphere.

According to the criterion of **coherence**, option 1 would have a negative impact because it would imply reducing the EU effort in cybersecurity, while option 0 is considered moderately incoherent with NIS policy, because a fixed term mandate (in contrast to the tasks conferred to ENISA by the NIS Directive) and no update to the tasks/resources to match the new needs would not be consistent with the EU priorities set in the Cybersecurity Strategy and the Digital Single Market. Option 2 and 3 are both positively assessed against this criterion, as completely aligned to the objectives of EU policy.

The impact assessment exercise has shown that among all options the **stakeholders favour option 2** the most. There is in fact widespread consensus that an EU cybersecurity agency is needed and that the current ENISA (baseline) does not fulfil the conditions to exercise the roles that are needed and to face the present and future cybersecurity challenges, but that it has a large potential to do so if appropriately mandated and resourced. As presented above in section 6.1, there is consensus across all categories of stakeholders for a reformed Agency, for which the main pillars can be found in existing NIS policy/law and the key strengths emerged from the evaluation. Adding full operational capabilities to ENISA would be a welcome development for some stakeholders, while it would be seen as 'unnecessary revolution' by others, in particular the most equipped Member States.

### *Certification*

As the table 6 shows, **baseline and option 1** would not produce effective results to achieve the objectives. National and private schemes would continue to proliferate and create fragmentation. Such a trend is expected to continue, unless Member States agree on mutual recognition of their schemes or - together with the Commission - work on the development of a voluntary European scheme. However, this will occur on an *ad hoc* basis. In addition, as Member States would continue to use and improve their national schemes; they would also create a strong legacy, therefore making harmonisation more difficult.

End-users making cross-border purchases will not necessarily understand or have access to the information regarding the security properties of the devices they have purchased. Business segments already subject to certification requirements will continue to bear costs related to multiple processes. Conversely, businesses that are currently not subject to certification requirements will not bear any upfront costs and remain free to choose whether or not to be involved in any certification process. Costs for them may arise in the future as requirements for ICT certification would be progressively put in place. No substantial upfront costs are envisaged for Member States.

These options would also yield unsatisfactory results in terms of increasing the level of assurance of critical infrastructures. The coherence with policies related to the Digital Single Market, the internal market and the NIS Directive are not fully supported, while international trade is promoted to the extent that actors concerned commit to use international standards. However, these options are expected to have positive impact on innovation and competitiveness at least in the short term. Finally, these options enjoy some support from industry, especially large, international corporations while Member States see the risk that providers of essential services operating cross-border could be subject to different security requirements in relation to ICT certification.

**Option 2** would produce some effective results to achieve the objectives. The extension of the membership of the current SOG-IS MRA to all Member States provides an institutional framework that ensures mutual recognition. However, such a positive effect is expected to be limited to certification at high level of assurance. National and private schemes would continue to proliferate for a wide range of commercial products and services, thus increasing fragmentation. In addition, end-users of these products may not have the necessary information on the cybersecurity properties of these products and services. This option would produce efficient results for industry already applying for SOG-IS certificates; businesses that are currently not subject to certification requirements for their commercial products and services will not bear any upfront costs and remain free to choose whether or not to be involved in any certification process. As for efficiency, costs for Member States would vary depending on the status that they would achieve in the SOG-IS MRA (certificate consumer or producer). Existing members of SOG-IS MRA may face an increase in demand for certification, which may translate in higher costs to accommodate such a demand but also higher revenues. This option would also produce satisfactory effects regarding the increase of the level of assurance of critical infrastructures as well as the coherence with other policies such as NIS Directive. To the extent that it ensures mutual recognition for certification of high level of assurance and it continues to utilise international standards such as CC, this option provides some support to the internal market and international trade. Finally, industry representatives as well as existing members of SOG-IS MRA agree on the need to shape future certification initiatives in Europe building on the experience of the SOG-IS MRA, but they also stress the need to significantly reform such a EU-wide mechanism.

**Option 3** achieves the objectives **effectively**. This option builds on the Option 2 (e.g. extension of the existing SOG-IS MRA) but it goes much further as it envisages the creation of an institutional, voluntary framework that would allow the Commission to adopt schemes for ICT security certification, prepared by ENISA in cooperation with national authorities - represented in a dedicate Group - at various levels of assurance, thus potentially covering a wide range of products and service as the need arise. In other words, the proposed framework differs from SOG-IS MRA as the latter is one scheme while the framework is a "system" of many schemes for different product categories, different assurance levels<sup>131</sup> using different evaluation methods. Moreover, as it emerged from consultations and technical studies underpinning this Impact Assessment, SOG-IS MRA (a scheme built on specific CC standards) does not cover or does not respond well to market needs for a faster and cheaper certification at lower assurance levels.

In addition, Option 3 would help promote information on the cybersecurity of ICT products and services. This would be in line with the results of a Eurobarometer survey in which the majority of respondents consider that security and privacy features of an ICT product play a role in their choice. As for its **efficiency**, this Option would not imply additional, upfront costs for the industry (incl. SMEs). Rather, it would generate significant savings for those firms that already certify their products (or that are willing to carry out security certification), with beneficial effects on their competitiveness worldwide.

On the other side, it would involve some budgetary commitment to ensure the full operation of the framework at Commission, but mostly at ENISA level. Member States will have to bear the necessary costs to ensure the implementation and supervision of the framework at national level.

This option is expected to significantly support internal market by significantly reducing fragmentation. Positive impacts are also expected on international trade to the extent that the Framework backs international standards.

---

<sup>131</sup> The expression 'assurance level' should not be confused with CC EAL

Table 5 Overall impact of the various policy options for ENISA.

Impacts	Option 0: Baseline – Keep Status Quo	Option 1: Expiry of ENISA Mandate (Terminating ENISA)	Option 2 'Reformed ENISA'	Option 3: EU cybersecurity agency with full operational capabilities
Effectiveness	*	**	✓✓	✓✓✓
Economic/Efficiency	* (economy) ✓ (EU budget)	** (economy) ✓ (EU budget)	✓ ✓ (economy) * (EU budget)	✓✓✓ (economy) ** (EU budget)
Environmental	0	0	0	0
Social	0	**	✓✓	✓✓
Coherence	*	***	✓✓✓	✓✓✓
Stakeholders' support	*	***	✓✓ (industry) ✓✓✓ (Member States)	✓ (industry) ✓ (Member States)
Total	***	*****	✓✓✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓✓✓

The symbols "✓" and "\*" indicate respectively positive (✓) and negative (\*) impacts. For each symbol a maximum a scale 1 to 3 (maximum positive or negative assessment) is used.

Table 6 Overall impact of the various policy options for certification.

Impacts	Baseline Option 0	Option 1: Soft law measures	Option 2: extension of SOG-IS agreement to all MS	Option 3: European ICT security certification framework
Effectiveness	✘	✘	✓	✓
Economic/efficiency	0	✓	✓	✓✓
Environmental	0	0	0	0
Social	0	0	✓	✓
Coherence	0	0	✓	✓
Stakeholders' support	0	✘ (Member States) ✓ (industry)	✓ (Member States) ✓ (industry)	✓ (Member States) ✓ (industry)
<b>Total</b>	✘	0	✓✓✓✓✓✓	✓✓✓✓✓✓✓

The symbols "✓" and "✘" indicate respectively positive (✓) and negative (✘) impacts; the number of the symbols is the net result of the summing-up of the respective individual ratings of the policy option as indicated in Annex 13 and indicates the magnitude of the change.

## 8. PREFERRED OPTION

Based on the above comparison, it appears that a combination of **Option 2** with regard to **ENISA** and **Option 3** for **certification** is the best option to achieve the objectives, while taking into account the criteria of efficiency and coherence.

Under this scenario, the EU would have a reformed agency for cybersecurity, focused on providing support to Member States, EU institutions and businesses in areas where it would bring the most added value: i.e. policy development and implementation; information knowledge and awareness; research; operational cooperation and crisis; market. Moreover, ENISA would play a paramount role in the field of EU cybersecurity certification policy, as it will prepare (in cooperation with MS certification authorities) candidate European cybersecurity certification schemes. The reformed ENISA would also see addressed its current weaknesses in the new mandate.

Under Option 3 for certification, the legislative proposal would provide the EU with a much needed framework of rules for establishing European cybersecurity certificates valid and recognised in 28 Member States. The framework will put the right conditions in place for effectively addressing the problem related to the co-existence of multiple certification procedures in various Member States, reducing certification costs and thus making certification in the EU overall more attractive from a commercial and competitive perspective. Altogether, this should facilitate and improve (in the short-medium run) businesses' cyber-certification practices, thereby contributing to the spreading of better cybersecurity practices in the design of ICT products and services (security by design).

The solution to combine these options is therefore considered the most effective for the EU to reach the identified objectives of: increasing cybersecurity capabilities, preparedness, cooperation, awareness, transparency and avoiding market fragmentation.

This combination of options is also the most coherent with policy priorities, as it is entrenched in the Cybersecurity Strategy and related policies (e.g. NIS Directive), and the Digital Single Market Strategy. In addition, from the consultations carried out so far, it clearly emerges that the preferred options enjoy the favour of the majority of stakeholders.

Furthermore, the analysis conducted in this impact assessment demonstrates that the combination of these two options would reach the objectives through a reasonable employment of resources. In particular, a 'reformed ENISA' would provide Member States with a more adequate support to achieve cyber resilience, and will only have a limited impact on the EU budget. At the same time, a voluntary European certification framework will help promote the cybersecurity of digital products and services in the EU, with a limited impact on the resources of Member States and EU budget, and no upfront costs for industry.

In line with the principle of proportionality, the preferred option proposes actions that are not considered going beyond what is necessary to achieve the objectives defined in this impact assessment. In addition, the nature of the objectives is such that they cannot be achieved sufficiently by a unilateral action of Member States. For this purpose, an intervention at Union level is necessary.

Finally, linking the review of the ENISA mandate with the measures on certification is a coherent way to address the common problem mainly related to insufficient cyber awareness, and the fragmentation of policies and approaches towards cybersecurity across Member States. As explained throughout the document, security certification is an area in which such a fragmentation is increasingly emerging and greater awareness is



particularly needed. This creates a negative impact on the internal market. As an internal market agency, and as further confirmed in the evaluation process and the stakeholders consultations, ENISA is best placed to support a coherent approach to security certification across the EU.

The establishment of a European legal framework would be a first step to develop a common policy in this field, build consensus on new priority areas to tackle and plan future activities, as needs arise. In a fast-moving, dynamic market, such as the one of ICT products and services, this approach would create the conditions for key decisions to be taken in the future by the competent authorities, such as the matching between the products/services and the needed level of security.

The preferred option entails EU legislative intervention as only a binding instrument can guarantee the translation into practice of the measures proposed and the achievement of the related specific objectives. The chosen legal instrument is a Regulation that will cover the new mandate for ENISA and lay down a European ICT security certification framework.

**Table 7 Overview of main changes in the tasks between current ENISA and preferred option**

Areas	Before	Factors of change	After
Policy development and implementation	<ul style="list-style-type: none"> <li>Assisting and advising on all matters relating to Union NIS policy and law</li> <li>preparatory work, advice and analyses relating to the development and update of Union NIS policy and law</li> <li>Analyzing publicly available NIS strategies and promoting their publication</li> </ul>	<ul style="list-style-type: none"> <li>Strengthen/refocus existing mandate</li> <li>New tasks/align to subsequent legislation (e.g. NIS Directive , eIDAS, Electronic Communications Code)</li> </ul>	<ul style="list-style-type: none"> <li>Actively contribute its independent opinion to policy development and implementation in the area of cybersecurity including in sectoral law and policy where cybersecurity is involved</li> <li>contribute to the work of the Cooperation Group, pursuant to Article 11 of NIS Directive, by providing its expertise and assistance</li> <li>supporting the development and implementation of Union policy in the area of electronic identity and trust services (eIDAS)</li> <li>supporting the promotion of an enhanced level of security of electronic communications (Code)</li> <li>supporting regular</li> </ul>

			review of the EU cybersecurity policy and law (annual report including summary notifications as per NIS Directive, eIDAS and Code)
Capacity building	<ul style="list-style-type: none"> <li>supporting MSs at their request, to develop and improve the prevention, detection and analysis of and the capability to respond to NIS problems and incidents</li> <li>assisting the EU institutions, bodies, offices and agencies in their efforts to develop the prevention, detection and analysis of and the capability to respond to NIS problems and incidents, in particular by supporting the operation of a CERT for them.</li> <li>Offering NIS training for relevant public bodies,</li> <li>supporting the raising of the level of capabilities of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices</li> </ul>	<ul style="list-style-type: none"> <li>Strengthen/refocus existing mandate</li> <li>Align to NIS Directive</li> <li>New tasks</li> </ul>	<ul style="list-style-type: none"> <li>Keep mandate with regard to trainings, CSIRTs maturity and general principle of assistance to Member States and EU institutions</li> <li>support the development and review of EU cybersecurity strategies, promoting their dissemination and tracking progress of their implementation</li> <li>assist Member States in developing national NIS strategies pursuant to Article 7(2) of Directive (EU) 2016/1148</li> <li>assist Member States, upon their request, in developing national CSIRTs pursuant to Article 9(5) of NIS Directive</li> <li>assist the Cooperation Group, with exchanging of best practices, in particular with regard to the identification of operators of essential services, including in relation to cross-border dependencies, regarding risks and incidents, pursuant to Article 11(3)(l) of NIS Directive</li> </ul>
Market	Facilitating the	<ul style="list-style-type: none"> <li>Strengthen/refocus</li> </ul>	1)Standardization: keep

	<p>establishment and take-up of European and international standards for risk management</p>	<p>existing mandate</p> <ul style="list-style-type: none"> <li>Align with NIS Directive</li> <li>New tasks</li> </ul>	<p>mandate and align with Article 19 (2) of NIS Directive with regard to collaboration with Member States to draw up advice and guidelines regarding the technical areas to be considered.</p> <p>2) Certification: support Union policy development and implementation; contribute to development and maintenance of the ICT security certification framework.</p> <p>3) Market Observatory: analyses and dissemination of the main trends in the cybersecurity market.</p>
Operational cooperation	<ul style="list-style-type: none"> <li>Promoting dialogue and exchange of information between national/governmental CERTs, including CERT-EU</li> <li>Provide advice to EU institutions and Member States, upon request, in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services</li> <li>Organizing Cybersecurity exercises</li> <li>supporting the development of a Union early warning mechanism that is complementary to MSs' mechanisms</li> <li>promoting and facilitating voluntary cooperation among Member States and between EU institutions and the Member States in their efforts to prevent, detect and</li> </ul>	<ul style="list-style-type: none"> <li>Strengthen/refocus existing mandate</li> <li>New tasks</li> <li>Align to subsequent legislation (NIS Directive) and the new initiatives (Blueprint)</li> </ul>	<ul style="list-style-type: none"> <li>Establishing systematic cooperation on operational matters with EU institutions, agencies and bodies, in particular CERT-EU and EC3</li> <li>Providing the secretariat of the CSIRTs network as per NIS Directive and actively facilitating the information sharing and the cooperation.</li> <li>Contribute to operational cooperation within the CSIRT Network, providing, in cooperation with CERT-EU, support to Member States that would request it by: <ol style="list-style-type: none"> <li>Advising on how to improve their capabilities to prevent, detect and respond to incidents.</li> <li>Providing technical</li> </ol> </li> </ul>

	<p>respond to cross-border incidents</p>		<p>assistance in case of significant cybersecurity incident.</p> <p>3. Ensuring backend support for analysis of vulnerabilities, artefacts and incidents in order to strengthen preventive and response capabilities of Member States</p> <ul style="list-style-type: none"> <li>• Organizing Cybersecurity exercises</li> <li>• Contribute to the blueprint, supporting a cooperative EU response to large scale cross-border cybersecurity incidents and crises, mainly by: <ol style="list-style-type: none"> <li>1. Aggregating reports from national sources with a view to establish common situation awareness;</li> <li>2. Ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRT Network and the technical and political decision makers;</li> <li>3. Supporting technical handling of the incident, including facilitating sharing of technical solutions between Member States;</li> <li>4. Supporting the handling of the Union public communication around the incident;</li> </ol> </li> </ul>
--	--	--	---

			5. Testing the Union cooperation plans to respond to cross-border incidents and crises
Research and Innovation	Advising the Union and the Member States on research needs in the NIS area	<ul style="list-style-type: none"> <li>• Strengthen/refocus existing mandate</li> <li>• New task</li> </ul>	<ul style="list-style-type: none"> <li>• Advice on research needs and priorities and feed into the Hub of Excellence</li> <li>• Upon request of Commission participate in implementation of R&amp;I Programmes</li> </ul>
Knowledge, information, awareness	<ul style="list-style-type: none"> <li>• assisting the Union institutions, bodies, offices and agencies and the MSs in their efforts to collect, analyse and, in line with MSs' security requirements, disseminate relevant NIS data</li> <li>• providing Member States with the necessary knowledge to improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents.</li> <li>• promoting the development and sharing of best practices</li> <li>• promoting best practices in information sharing and awareness raising</li> <li>• supporting the EU and the Member States in organizing awareness raising</li> </ul>	<ul style="list-style-type: none"> <li>• Strengthen/refocus existing mandate</li> <li>• New Tasks</li> </ul>	<ul style="list-style-type: none"> <li>• Analyses of emerging technologies and assessment of economic, societal, legal, regulatory impacts on cybersecurity</li> <li>• Advice, guidance and best practices, in cooperation with Member States experts, for the security of NIS, in particular internet infrastructures and those related to sectors listed in NIS Directive</li> <li>• Information Hub: one-stop-shop for information on cybersecurity deriving from EU institutions, agencies and bodies.</li> <li>• Compile reports based on public information after cyber incidents to provide guidance to citizens and businesses</li> <li>• Raise awareness about cyber hygiene good practices</li> <li>• Keep mandate on awareness raising campaigns (e.g. Cybersecurity</li> </ul>

## Case studies on the preferred option:

An example of Reformed ENISA in the event of a cyber crisis

### Box 5 – Before/after (fictional) scenario of large scale cross-border cyber incident

#### 1. "Before" scenario

A new computer virus infects the systems of the national branch office of a major accounting firm. Citizens and companies are not sufficiently aware of cyber threats and do not have sufficient information of cyber hygiene practices, so the virus spreads with phishing emails to clients across the EU. National experts scramble to determine how the virus works and how to stop its spread, information is shared only between a few members within the CSIRT Network and ENISA does not have the capacity to monitor the situation and provide assistance to those Member States who do not have sufficient resources. There is no rehearsed coordination plan between ENISA, CERT-EU and EC3 and between Member States and the EU bodies. The lack of a common EU situation awareness slows down the identification of the root causes and the estimation of the scale of the event. The computer virus continues to spread rapidly across the EU and the affected companies take their IT systems off-line to contain the damage. Incident responders are overwhelmed by the increasing number of incidents at national level and there is no assistance available at EU level to help technical handling of the incidents. In the aftermath of the event, some countries do not have the necessary resources to conduct incident analysis. Some Member States authorities publish reports and recommendations, in national language, for the future targeting businesses and citizens.

#### 2. "After" scenario

A new virus infects systems of the national branch office of a major accounting firm. Citizens' and companies are better informed of cyber threats and how to address them: ENISA, in cooperation with experts from Member States, regularly provides guidance and best practices, for the security of network information systems and it provides cyber hygiene recommendations targeted. As a consequence, the spread of the virus is somehow contained in comparison to scenario 1 as more users are able to detect phishing emails. However, some Member States are still severely affected. The CSIRT Network swiftly goes into information sharing mode, ENISA runs efficiently the communication channels and ensures that the competent actors at EU level are kept informed so to allow swift decision making. Operational cooperation and coordinated activities allow for faster identification of the causes of the incident. The spread of the computer virus continues to slow across the EU. The infected companies across the EU have at hand good practices and guidance about how to deal with incidents and are able to maintain key services running. ENISA and CERT-EU experts provide assistance to national incident responders that request help with mitigating measures, based on the solution adopted in other Member States. They are also assisted with restoring IT services and incident analysis. Based on a thorough analysis of the incident and the information made available at Member State level, ENISA compiles an EU wide report on the event with recommendations for future.

**Examples of how the EU Cybersecurity Certification Framework would change the present situation.**

## 1. Smart meters

	Now	Future
<b>Requirements</b>	<ul style="list-style-type: none"> <li>• <i>In order to sell in UK and France manufacturers have to certify against different schemes:</i> <ul style="list-style-type: none"> <li>○ <i>CPA (Commercial Product Assurance) in UK,</i></li> <li>○ <i>CSPN (Certification de Sécurité de Premier Niveau) in France</i></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Manufacturers will need to undergo a single certification process, as envisaged in the future European certification scheme for smart meters. The resulting certificate will be accepted by all public authorities in Member States.</li> </ul>
<b>Cost</b>	<ul style="list-style-type: none"> <li>• The overall cost is at least 300 thousand euros for the two markets (about 150 thousand euro in UK and about 150 thousand euros in France).</li> </ul>	<ul style="list-style-type: none"> <li>• The estimation of costs saving ranges up to <b>80% of current costs</b></li> </ul>
<b>Time</b>	<ul style="list-style-type: none"> <li>• <b>6 to 18 months.</b> This estimate takes into account: <ul style="list-style-type: none"> <li>○ Completion of multiple certifications processes and supporting documentation</li> <li>○ Identification of various requirements that a vendors needs to comply with.</li> <li>○ limited number of conformity assessment bodies able to certify against the requirements of different schemes.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Faster process</b> that takes into account: <ul style="list-style-type: none"> <li>○ Role of ENISA that provides information needed for compliance with the European scheme (e.g. specialised conformity assessment; documentation)</li> <li>○ Completion of single process : no multiple certifications are needed and capacities of existing CABs can be used more efficiently</li> </ul> </li> </ul>
<b>Other</b>	<ul style="list-style-type: none"> <li>• <b>Different methodologies</b> for risk assessment and definition of security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Standard methodologies</b> for risk assessment and definition of security requirements</li> </ul>

## 2. Cloud Computing

	Now	Future
<b>Requirements</b>	<ul style="list-style-type: none"> <li>In order to sell Cloud Computing Products / Services in France and Germany providers have to certify against: <i>SecNumCloud</i> <b>and</b> <i>Compliance Controls Catalogue (C5)</i></li> </ul>	<ul style="list-style-type: none"> <li>Providers need to undergo a single certification process, as envisaged in the future European certification scheme for cloud computing. The resulting certificate will be accepted by all public authorities in Member States</li> </ul>
<b>Cost</b>	<ul style="list-style-type: none"> <li>Costs associated to compliance with different technical rules and multiple testing is estimated around 1.2 billion euro, that accounts for <b>2% to 10%</b> of companies' annual expenditures.</li> </ul>	<ul style="list-style-type: none"> <li>An increased level of competition, introducing an EU wide Certification Scheme, would result in a <b>yearly saving of € 1.1 billion in the EU public sector alone</b></li> </ul>
<b>Time</b>	<ul style="list-style-type: none"> <li><b>Around 7-9 months</b> due to the multiple audit and testing processes to obtain several certifications</li> </ul>	<ul style="list-style-type: none"> <li><b>Reduced time:</b> duration of a single process is estimated to take around 4 to 6 months. ENISA would accelerate the process by providing the information needed for compliance with the European scheme</li> </ul>
<b>Other</b>	<ul style="list-style-type: none"> <li>Faced with co-existence of multiple schemes and standards<sup>132</sup>, end-users (esp. in the banking sector) are not able to compare and judge which scheme or standard would best satisfy their particular security requirements. This deteriorates the trust in cloud computing services.</li> </ul>	<ul style="list-style-type: none"> <li>The existence of a security certification scheme for cloud computing agreed at EU level, increases the trust in this service</li> <li>Competitive gain for cloud providers due to cost and time reduction</li> </ul>

## 9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

This section describes the monitoring and evaluation that could be applied to assess the impact of the objectives and the preferred option.

Monitoring will start right after the adoption of the legal instrument and it will focus on its application. The Commission will organise meetings with ENISA, Member States representatives (e.g. group of experts) and the relevant stakeholders in particular to

<sup>132</sup> ECSO has published a State-of-the-Art Syllabus listing 6 different schemes and 2 standards to certify the security of cloud computing services.



facilitate the implementation of the rules concerning certification such as the establishment of the Cybersecurity Certification Group.

In particular, monitoring activities on certification will consider the widening of the product and services scope covered by EU certification schemes. This would help better evaluate the potential uptake and interest in the setting up of EU-level certification schemes. Moreover, an eventual decrease of national initiatives or industry-driven schemes would equally provide an indication of a reduced level of fragmentation in the certification landscape in the EU. Similarly, it would signal a positive move towards a proper functioning of the EU internal market for ICT products and services. Transparency elements such as publication of cybersecurity market trends in Europe and surveying the awareness of security features of ICT products and services among end-users and businesses would provide further indications.

The first evaluation should take place five years after the entry into force of the legal instrument, provided sufficient data is available. An explicit evaluation and review clause, by which the Commission will conduct an independent evaluation, will be included in the legal instrument. The Commission will subsequently report to the European Parliament and the Council on its evaluation accompanied where appropriate by a proposal for its review, in order to measure the impact of the Regulation and its added value. Further evaluations should take place every five years. The Commission Better Regulation methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted, expert discussions, studies and wide stakeholders consultations.

ENISA's Executive Director should present to the Management Board an ex-post evaluation of ENISA's activities every two years. The Agency should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress bi-annually to the Commission. The Management Board should be responsible to vigilate on the adequate follow-up of such conclusions.

Alleged instances of maladministration in the activities of the Agency may be subject to inquiries by the European Ombudsman in accordance with the provisions of Article 228 of the Treaty.

The list of monitoring indicators that could be used to monitor progress towards meeting the general and specific objectives is presented in table 8 below. The data sources for planned monitoring would mostly be ENISA, the European Cyber-Certification Group, the Cooperation Group, the CSIRT Network and the Member States' authorities. Besides the data deriving by the reports (including the annual activity reports) of ENISA, the European Cyber-Certification Group, the Cooperation Group and the CSIRTs Network, specific data gathering tools will be used when needed (for example surveys to national authorities, Eurobarometer and reports from Cybersecurity Month campaign and the pan-European exercises).

Table 8 List of indicators to monitor progress towards general objectives

General Objectives	Specific Objectives	Operational objectives	Monitoring indicators	Source of data
<p>Increase the cyber resilience of the Member States, businesses and the EU as a whole.</p>	<p>Increasing capabilities and preparedness of Member States and businesses, in particular the critical infrastructures</p>	<ul style="list-style-type: none"> <li>To contribute effectively to the development of policy in the area of NIS as well as policy initiatives with cybersecurity elements in key sector (e.g. Energy, Transport, Finance, etc).</li> <li>To support the development and necessary updates to National and EU Cybersecurity Strategies.</li> <li>To contribute to improvement of national public authorities' capabilities expertise, in particular in cybersecurity incident response (CSIRTs) and supervision of cybersecurity related regulatory measures.</li> <li>To provide Member States and businesses with long-term strategic analyses of cyber threats, incidents to identify emerging trends.</li> <li>To facilitate the establishment and take-up of European and</li> </ul>	<ul style="list-style-type: none"> <li>Number of trainings organised by ENISA</li> <li>Geographical coverage (number of countries and areas) of the direct assistance provided by ENISA</li> <li>Level of preparedness reached by Member States in terms of CSIRT maturity and supervision of cybersecurity related regulatory measures</li> <li>Number of EU-wide good practices for critical infrastructures provided by ENISA</li> <li>Number of EU-wide good practices for SMEs provided by ENISA</li> <li>Publication of annual strategic analysis of cyber threats and incidents to identify emerging trends by ENISA</li> <li>Regular contribution of ENISA to the work of cybersecurity working groups of the European Standardisation</li> </ul>	<p>ENISA</p> <p>ENISA</p> <p>CSIRT Network and ENISA</p> <p>ENISA</p> <p>ENISA</p> <p>ENISA</p> <p>ENISA</p> <p>European Cybersecurity Certification Group (ECCG)</p>

		international standards for risk management and for the security of electronic products, networks and services	Organisations (ESOs). <ul style="list-style-type: none"> <li>Number of conformity assessment bodies specialized in ICT certification, across Member States</li> </ul>	
	improving cooperation and coordination across Member States and EU, institutions, agencies and bodies	<ul style="list-style-type: none"> <li>To ensure the coherence and the adequacy of the EU regulatory approach to cybersecurity</li> <li>To contribute to the evaluation and review of cybersecurity related policies in the EU.</li> <li>To establishing information exchange networks between administrations, industry and end user representatives in the NIS community</li> <li>To contribute to the establishment of Information Sharing and Analysis Centres in various sectors.</li> <li>To pool, organize and make available information on cybersecurity deriving from the EU institutions, agencies and bodies.</li> <li>To provide</li> </ul>	<ul style="list-style-type: none"> <li>Number of Member States having made use of ENISA recommendations and opinions in their policy making process</li> <li>Number of EU institutions, agencies and bodies having made use of ENISA recommendations and opinions in their policy making process</li> <li>Regular implementation of CSIRT Network work programme and well-functioning on the CSIRTs Network IT infrastructure and communication channels</li> <li>Number of technical reports made available to and used by the Cooperation Group</li> <li>Consistent approach to the NIS Directive implementation across borders and sectors</li> <li>Number of regulatory compliance assessments performed by ENISA</li> </ul>	<ul style="list-style-type: none"> <li>Survey of Member States authorities (study)</li> <li>Survey of EU institutions, agencies and bodies (study)</li> <li>ENISA and CSIRT Network</li> <li>ENISA</li> <li>ENISA</li> <li>ENISA and ECCG</li> <li>ENISA</li> </ul>

		<p>recommendations to Member States and the Commission on priority-setting in research and developments.</p> <ul style="list-style-type: none"> <li>To achieve a structural cooperation with CERT-EU and EC3, in particular on operational matters.</li> </ul>	<ul style="list-style-type: none"> <li>Number of ISACS in place in different sectors, in particular for critical infrastructures</li> <li>Establishment and regular running of information platform disseminating cybersecurity information deriving from the EU institutions, agencies and bodies</li> <li>Regular contribution to the preparation of EU research and innovation work programmes</li> <li>Cooperation agreement between ENISA, EC3 and CERT-EU in place</li> <li>Number of certification schemes included and developed under the Framework</li> </ul>	<p>Commission</p> <p>Commission</p> <p>ENISA</p> <p>ECCG</p>
<p>Increasing EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises.</p>		<ul style="list-style-type: none"> <li>To assist Member States in proactively identifying cybersecurity risks and vulnerabilities and monitoring and reporting incidents</li> <li>To Assist Member States in establishing appropriate response mechanisms</li> </ul>	<ul style="list-style-type: none"> <li>Publication of annual strategic analysis of cyber threats and incidents to identify emerging trends by ENISA</li> <li>Publication of aggregated information of incident reported under NIS Directive by ENISA</li> </ul>	<p>ENISA</p> <p>ENISA</p>

		<ul style="list-style-type: none"> <li>To support a cooperative EU response to large scale cross-border cybersecurity incidents and crises</li> </ul>	<ul style="list-style-type: none"> <li>Number of pan-European exercises coordinated by the Agency and number of Member States and organisations involved.</li> <li>Number of requests to support emergency response by Member States to ENISA and performed by the Agency</li> <li>Number of analyses of vulnerabilities, artefacts and incidents performed by ENISA in cooperation with CERT-EU.</li> <li>Availability of EU-wide situational reports based on information made available to ENISA by Member States and other entities in case of large scale cross-border cyber incident.</li> </ul>	<p>ENISA</p> <p>ENISA</p> <p>ENISA and CERT-EU</p> <p>ENISA</p>
	<p>Increasing awareness of citizens and businesses of cybersecurity issues.</p>	<ul style="list-style-type: none"> <li>To raise awareness of citizens and businesses of cybersecurity threats and cyber hygiene practices.</li> <li>To promote and share cybersecurity best practices from across the EU</li> </ul>	<ul style="list-style-type: none"> <li>Regular running of EU-wide and national awareness raising campaigns and regular update of the topics according to the emerging learning needs.</li> <li>Increase of cyber awareness among EU citizens</li> <li>Regular running of</li> </ul>	<p>ENISA</p> <p>Eurobarometer ENISA</p>

			<p>cybersecurity awareness quiz and increase over the time of the percentage of correct responses.</p> <ul style="list-style-type: none"> <li>Regular publication of cybersecurity and cyber hygiene good practices targeted to employees and organisations.</li> </ul>	ENISA
<p>Ensure the <b>proper functioning of the EU internal market</b> for ICT products and services.</p>	<p>Avoiding <b>fragmentation of certification schemes</b> in the EU and related security requirements and evaluation criteria across MS and sectors.</p>	<ul style="list-style-type: none"> <li>To develop an EU ICT Security Certification Framework based on mutual recognition of certification schemes</li> <li>To support ICT security certification policy development and implementation</li> </ul>	<ul style="list-style-type: none"> <li>Number of schemes that adhere to the EU framework</li> <li>Guidelines for certification according to the EU framework in place</li> <li>Set-up of the European Cybersecurity Certification Group and regular organisation of meetings</li> <li>Reduced cost of obtaining a certificate for ICT security.</li> </ul>	<p>ECCG, ENISA</p> <p>ECCG, ENISA</p> <p>ENISA</p> <p>Survey of EU companies (study)</p>
		<ul style="list-style-type: none"> <li>To support alignment of demand and supply of cybersecurity market in the EU</li> </ul>	<ul style="list-style-type: none"> <li>Regular publication of analyses of the main trends in the EU cybersecurity market</li> </ul>	ENISA
<p>Increasing the overall <b>transparency of cybersecurity assurance</b> of ICT products and services so as to strengthen trust in the digital single market</p>		<ul style="list-style-type: none"> <li>To widen the scope of the products that are certified</li> <li>To ensure better information for the buyers of the</li> </ul>	<ul style="list-style-type: none"> <li>Number of certified ICT products and services according to the rules of the European ICT security certification framework</li> </ul>	ENISA

	and in digital innovation	security features of ICT products and services	<ul style="list-style-type: none"> <li>Increase in the number of end-users who are aware of security features of ICT products and services</li> </ul>	Eurobarometer and survey of EU companies (study)
<p><b>Increase the global competitiveness</b> of the EU companies operating in the ICT field.</p>		<ul style="list-style-type: none"> <li>To avoid that EU companies lose competitiveness due to the need to undergo several certification procedures</li> </ul>	<ul style="list-style-type: none"> <li>Number of schemes that adhere to the EU framework.</li> </ul>	ENISA

## Annex 1: Procedural information

### 10. LEAD DG, DECIDE PLANNING / CWP REFERENCES

This Impact Assessment Report was prepared by Directorate H "Digital Society, Trust and Cybersecurity" of the Directorate General "Communications Networks, Content and Technology" (DG CNECT).

The Decide Planning reference of the initiative "Proposal for a Regulation of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA), repealing Regulation (EU) No. 526/2013 and laying down a European security certification framework for Information and Communications Technology (ICT) Products and Services" is 2017/CNECT/005.

The initiative on the review of ENISA was included in the Commission Work Programme for 2017.

### 11. ORGANISATION AND TIMING

Several services of the Commission with an interest in the assessment of the initiative have been associated in the development of this analysis.

An Inter-Service Steering Group (ISG), consisting of representatives from various Directorates-General of the Commission and the European External Action Service (EEAS), was set up in 2016 to steer the evaluation of ENISA during all key phases. In 2017, this group was further enlarged to discuss the review of the initiative involving the review of ENISA Regulation and the European ICT security certification framework.

In 2016, two meetings of the ISG on the review of ENISA were held. The first meeting took place on 24 June 2016. DG CNECT, DG HOME, JRC, DG JUST, the Secretariat General (SG) and EEAS participated in the meeting. The second meeting was held on 9 December, 2016. The representatives from DG CNECT, DG DIGIT, SG and EEAS were present.

The third ISG meeting was dedicated to the review of ENISA and the set-up of a European ICT security certification framework, and took place on 24 May, 2017. The meeting was chaired by SG, and DG CNECT was flanked by DG BUDG, DG COMP, DG DIGIT, DG EMPL, DG ENER, DG FISMA, DG GROW, DG HOME, DG HR, DG NEAR, DG TRADE, and EEAS.



The fourth ISG meeting took place on 22 June, 2017. This was the last meeting of the ISG before the submission to the Regulatory Scrutiny Board (RSB) on 28 June, 2017. The meeting was chaired by SG and the participants were the following: DG BUDG, DG DIGIT, DG EMPL, DG ENER, DG GROW, DG HOME, DG HR, DG JUST, the Legal Service (LS), DG MOVE, DG TAXUD, and DG TRADE. DG CNECT has updated the Impact Assessment Report by taking into account the comments received at - and following - the ISG meeting, in particular the comments made by, DG GROW, DG JUST, LS, DG TRADE, and SG. Following a positive opinion issued by the RSB, a final Fast Track ISG meeting was held on 30 August

## **12. EXCEPTIONS TO THE BETTER REGULATION GUIDELINES**

DG CNECT has identified one exception to the Better Regulation Guidelines. Specifically, a dedicated public consultation focussing on ICT security certification in the EU has not been conducted. However, stakeholders were given the opportunity to express their views on the issue of ICT security certification in the following public consultations:

- The public consultation on the public-private partnership on cybersecurity and possible accompanying measures that took place in 2016; and
- The public consultation on the review and evaluation of ENISA, conducted in 2017.

Additionally, two surveys regarding ICT security certification have been organised in 2017 to complement the results of the past consultations:

- The survey on ICT security certification, targeting the certification community and organised by ENISA; and
- The small and medium enterprises survey on ICT certification and security framework was closed on 30 June, 2017 and final results were used in the revised report. The survey is currently also being broadened and results may be available in September.

## **13. CONSULTATION OF THE REGULATORY SCRUTINY BOARD (RSB)**

The Impact Assessment report was examined by the Regulatory Scrutiny Board on 19 July, 2017. On 25 August the Board issued a draft positive opinion with reservations. The table below summarises how the comments of the Board and of other Services have been addressed.

<b>Board's Recommendations in the Opinion</b>	<b>Implementation of the recommendations</b>
---	--

<p><b>of 25 August 2017</b></p>	<p><b>into the revised IA Report</b></p>
<p>The report does not describe the EU cybersecurity context well, e.g. the blueprint on large scale cross-border incidents. In addition, some ambiguity remains concerning the current application of mutual recognition (e.g. why it does not apply by default to ICT products) and the resulting limits to free movement of goods and reported market fragmentation</p>	<p>The report has been updated, in particular with regard to the glossary, the section 1 (context), section 5.1 (baseline scenario) and the section 5.3 (options related to certification).</p> <p>The meaning of cybersecurity for the purpose of the analysis and how it interrelates with network and information systems and their security. More details on the EU cybersecurity context, in particular the measures that are included in the Communication on Cybersecurity (September 2017<sup>133</sup>) and have a special relevance for ENISA: the EU cybersecurity blueprint, where the Agency is expected to play a major role in supporting the development of a cooperative approach to respond to large scale cross-border incidents; and the European Cybersecurity Research and Competence Centre, to which the Agency would link its advisories on EU research needs.</p> <p>It is also clarified that the policy options for</p>

<sup>133</sup> JOIN(2017) 450

	<p>certification refer to shortcomings related to the mutual recognition of certificates resulting from national certification schemes and not of products themselves. Such a mutual recognition may occur in an uncoordinated manner and would depend on the willingness of each Member States.</p> <p>It is further specified that, in absence of mandatory requirements for certification, uncertified products and services can still circulate. Requirements for certification are not necessary mandatory but can be market-driven. In the latter case, customers are presumably more willing to purchase certified products, as they assign a high value to the information provided by certification.</p>
<p>The report ignores the evaluation findings on ENISA weaknesses. It overlooks risks associated with ENISA's ability to absorb additional resources and to deliver effectively on an enlarged mandate.</p>	<p>The report has been further integrated to provide clarifications on the new obligations in the policy options related to ENISA (section 5.2) and on how some weaknesses related to ENISA efficiency, highlighted in the evaluation, are expected to be addressed (section 6.1. assessments of the impact). In particular explanations are provided on how the reform of the Agency, including the new tasks, the better conditions of employment and the structural cooperation with CERT-EU, would improve its attractiveness as employer and help tackle problems related to</p>

	<p>the recruitment of experts. Annex 6 to the report also presents a revised estimate of costs (for ENISA) associated to policy options 2 and 3.</p>
<p>The preferred option regarding certification is unclear. The report does not spell out how certification would work in practice. This makes it hard to assess potential value added, feasibility and cost. There is a risk that ENISA would not deliver much on certification.</p>	<p>Section 5.3 (description of the preferred policy option on certification) and 6.2 (assessment of the impact of policy options) have been revised in order to provide a more detailed explanation of option 3, including a graphic. The section on impact of option 3 also includes estimates on the costs for Member States, associated with supervising and enforcement activities as well as on the staff and resource implications for the Commission related to the new certification framework (e.g. set up of Expert Group).</p> <p>In addition, section 7 on option comparison and 6.2 on impact of option 3 (section on efficiency), includes an explanation of how the proposed framework differs and improves the current SOG-IS system.</p> <p>The rationale for the choice of ENISA as expert in the field and the only EU level agency on cybersecurity has been detailed in section 6.2</p>
<p>The range of products to which certification could apply remains unclear and so do the</p>	<p>The revised description of Option 3 explains that the type of ICT product and service</p>

<p>resulting impact</p>	<p>covered by a European certification scheme will be defined in the approved scheme itself.</p>
<p>What are the risks and consequences of Member States not adopting or using EU schemes?</p>	<p>The section on the impact of option 3, (objective 2) for certification specifies that Member States not using European certification schemes may face pressure from other Member States using these schemes to protect their assets</p>
<p>While the report provides additional information of costs, it does not sufficiently describe the magnitude of expected tangible benefits and how they compare across options</p>	<p>The sections on the impact of option 1 and 2 have been revised to better describe the benefits of these options. In particular Option 1 would help deliver the policy objectives faster and in a more cost-effective manner. Option 2 would provide Member States with institutional fora, enabling all Member States to express their security needs. Option 2 would also lead to a strengthened European position in the international context, and may become a model for other world's region.</p>
<p>The monitoring and evaluation framework lacks criteria and benchmarks for measuring success.</p>	<p>Section 9 of the report had been previously updated to address the comment of the Board according to which the table for M&amp;E was useful and detailed but it lacked information on the origin and frequency of data collection. Further elements to evaluate the positive impact of the initiative on certification (e.g. monitoring of decrease of fragmentation and uptake of EU-level</p>

	schemes) have been added
Presentation	Newly introduced abbreviations (e.g. IPCR and ARGUS) have been added to the glossary

#### 14. EVIDENCE, SOURCES AND QUALITY

The Commission gathered qualitative and quantitative evidence from various sources:

- (1) Two public consultations (a summary of which is attached to Annex 2 to this report) regarding:
  - a. The evaluation and review of ENISA; and
  - b. The public-private partnership on cybersecurity and possible accompanying measures (included a Section on ICT security certification).
- (2) Four stakeholder workshops with Member States and industry:
  - a. Three regarding ICT security certification; and
  - b. One regarding the ENISA review.
- (3) Fifty expert interviews regarding the ENISA review.
- (4) A survey on the ENISA review to the Computer Security Incident Response Teams Network.
- (5) A survey to the ENISA Management Board, Executive Board, Permanent Stakeholder Group, and ENISA staff.
- (6) Three technical studies:
  - a. One final draft report on the evaluation and review of ENISA prepared by an external contractor; and
  - b. Two studies regarding ICT security certification (one conducted by the Joint Research Centre (JRC), and another one by an external contractor).
- (7) A survey on certification and labelling addressed to small and medium enterprises (SMEs).
- (8) A survey for national cybersecurity authorities, industry and consumer associations on certification and labelling conducted by ENISA;

- (9) Inputs regarding ICT security certification from the European Cybersecurity Organisation (ECISO);
- (10) Direct dialogue with stakeholders, in particular through ad hoc meetings with representatives of interested industries, in particular regarding ICT security certification.
- (11) A roundtable with European Commission Vice-President for the Digital Single Market, Andrus Ansip, on 25 April 2017.
- (12) Desk research and literature review done in-house by DG CONNECT.

With regard to the quality of the evidence, the following three points must be noted:

- The survey on certification and labelling addressed to SMEs closed on 30 June 2017;
- The ENISA study is a final draft report;
- There are limitations with regard to gathering data. For instance, the public consultation on the ENISA review received 90 submissions, and CNECT has not received much input from SMEs in our input-gathering exercise. With a total of 90 responses, the results of the public consultation cannot be considered to be fully representative of all stakeholders concerned. However, the views of national authorities of 15 Member States (including the position paper provided by France) are represented. The private sector is represented by 27 respondents which include eight umbrella organisations, thus representing a significant number of European enterprises whose activities are linked with cybersecurity;
- The quality of the studies is impacted by the overall lack of evidence in the field of cybersecurity as a whole. In particular, companies are reluctant to share information regarding cybersecurity, considering that reporting on these topics could potentially harm them. In addition, there is no overall agreed taxonomy. This is one of the issues that the initiative is aiming to tackle.
- As regards to the survey on ENISA that was addressed to CERTs and CSIRTs, and the survey on the European ICT security certification framework addressed to SMEs, the answers in both surveys were anonymous. Thus, it is not possible to know whether some of the respondents might have started the survey and only partially completed this, and might then have reopened it using a different browser or device to complete the survey then. This would result in a double counting of the answers.





## Annex 2: Stakeholder Consultation

### 15. STAKEHOLDER CONSULTATION STRATEGY

In order to make sure that the Union's general public interest – as opposed to special interests of a narrow range of stakeholder groups – is well reflected in the assessment of the initiative, the Commission developed a stakeholder strategy to ensure the widest consultation possible. This strategy ensures transparency and accountability in the Commission's work.

In order to identify the most appropriate mix of consultation methods, the first step has been to identify the relevant stakeholder groups and the best way to consult them in order to gather relevant input.

The Commission pays attention to differentiate data gathering tools and adapts them to different types of contributions the stakeholders might have (See Section 2.2 below). Furthermore, in order to allow for wide participation, the consultation period spanned over a long period - from July 2016 to May 2017 approximately.

In view of the wide variety of sources and stakeholders consulted, and the relatively high degree of responses and input received from all stakeholders' group, the stakeholders views hereby discussed are considered as overall representative.

As regards the methodology and tools, the basic analysis approach has been largely adopted. Responses have been mostly grouped into broad stakeholder groups (e.g. Member State authorities, respondents from private sector, other respondents, etc.). Responses from a particular group on a particular issue helped provide an overview of the most recurrent points being made.

### 16. IDENTIFICATION OF GROUPS OF STAKEHOLDERS CONSULTED, MEANS OF CONSULTATION, AND CONSULTATION TOPICS

#### 16.1. Whom has the Commission consulted?

A non-exhaustive list of stakeholders that have been consulted (for both the review of ENISA and the EU ICT security certification framework, unless otherwise indicated below), includes the following bodies:

- The EU Member States national authorities as well as those from European Free Trade Association (EFTA) Countries;
- Standardisation bodies;
- Senior Officials Group – Information Systems Security (SOG-IS) members (mostly regarding certification);
- The members of ENISA's Management Board, Executive Board, Permanent Stakeholder Group and Network of Liaison Officers;
- Trade associations and industry representatives, including the European Cybersecurity Organisation (ECISO), Alliance for Internet of Things Innovation (AIOTI), DigitalEurope, and the Enterprise Europe Network (in particular for small and medium enterprises (SMEs));
- Consumers' representatives;
- Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) (mostly regarding ENISA);
- European Commission's services;
- The European External Action Service, the European Parliament, the Council of the European Union, the European Economic and Social Committee, the Committee of the Regions; the European Court of Auditors;
- Other EU Agencies and bodies, such as Computer Emergency Response Team for the EU institutions (CERT-EU), Europol and its European Cybercrime Centre (EC3), European Defence Agency, Body of European Regulators for Electronic Communications (BEREC), European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (Eu-LISA) (mostly regarding ENISA);
- International Organisations; and
- Citizens.

#### **16.2.** How has the Commission consulted stakeholders?

Depending on the stakeholder group identified, different tools and methods were used in order to conduct the consultation.

- During a 4-week period, all interested stakeholders were able to provide feedback on the ENISA evaluation [roadmap](#).
- Public Consultations:

- In 2016, a 12-week online [public consultation](#) was carried out at the occasion of the launch of the contractual public-private partnership on cybersecurity, which included specific questions / section on the topic of certification (approx. 240 respondents).
- In 2017, a 12-week online [public consultation](#) was carried out to seek views from the wider public (approx. 90 respondents) on ENISA evaluation and review. The consultation included also questions on the future needs and priorities in the area of cybersecurity, including the topic of certification.
- Survey targeted at ENISA staff and management, Management Board, Executive Board, Permanent Stakeholder Group, Network of Liaison Officers to cover more in-depth issues related to the efficiency and the effectiveness of the Agency and to its governance and organisation.
- Survey on ENISA targeted at the Computer Security Incident Response Teams Network (CSIRTs), for which the Agency provides the secretariat according to the NIS Directive.
- In-depth interviews, with approximately 50 key players in the cybersecurity community on the ENISA review, including on its role in certification.
- Stakeholder workshops:
  - In 2016, 2 workshops with national authorities were held on the topic of certification;
  - In 2017, 2 workshops were carried out on the ENISA review and certification respectively.
- Survey of national certification authorities, industry, consumers associations on the topic of certification and labelling, conducted by ENISA and the Commission.
- A targeted questionnaire on the topic of ICT security certification and labelling was conducted in June 2017.
- Inputs from the European Cyber Security Organisation (ECSO) on the challenges of certification and labelling. Working Group 1 of ECSO on certification and labelling includes 236 registered experts.
- Direct dialogue with individual stakeholders reaching out to the Commission on ENISA review and certification.

## **17. HAVE THE COMMISSION STANDARDS BEEN MET?**

The Commission standards as set in the Better Regulation Guidelines have been met. However, please see the exception to the Better Regulation Guidelines identified in Annex 1, points 3 and 5.

## **18. SUMMARY OF RESULTS FROM THE CONSULTATIONS REGARDING ENISA**

### **18.1.** Results of the public consultation on the evaluation and review of ENISA

The open public consultation on the evaluation and review of ENISA took place between 18 January and 12 April 2017. The public consultation aimed to gather the views of stakeholders and interested parties to assess ENISA's overall contribution to the cybersecurity landscape for the period 2013 to 2016. The public consultation also contributed to a reflection on potential policy options for the revision of ENISA's mandate. For this purpose, the consultation was structured around two sections:

- Backward looking – ex-post evaluation of ENISA; and
- Forward looking – focusing on evolving needs and challenges in the cybersecurity landscape and the possible role of an EU body to meet them in the future.

Respondents were allowed to answer either one or both sections. In addition, respondents had the possibility to send position papers.

With a total of 90 responses, the results of this public consultation cannot be considered to be fully representative of all stakeholders concerned. However, the views of national authorities of 15 Member States (including the position paper provided by France) are represented. The private sector is represented by 27 respondents which include eight umbrella organisations, thus representing a significant number of European enterprises whose activities are linked to cybersecurity.

*Main results related to the backward looking questions:*

- The overall performance of ENISA during the period 2013 to 2016 was positively assessed by a majority of respondents (74%). A majority of respondents furthermore considered ENISA to be achieving its different objectives (at least 63% for each of the objectives).

- ENISA’s services and products are regularly (monthly or more often) used by almost half of the respondents (46%) and are appreciated for the fact that they stem from an EU-level body (83%) and for their quality (62%).
- A majority of respondents considered ENISA’s size in terms of staff members to be insufficient (59%).

*Main results related to the backward looking questions regarding specific topics:*

#### *1. Interaction with ENISA*

- Among the respondents, 50% interacted with ENISA’s products and services “a few times per year” or only “on to two times per year”, while 46% of respondents interacted “on a weekly basis” or “on a monthly basis”.
- When comparing the frequency of interaction with ENISA or the use of ENISA’s products and services within a given group, 47% of the national authority respondents interact “on a weekly basis”, while the largest proportion of private enterprise and business association respondents (50%) do so “a few times per year” and 35% of “other respondents” interact “one to two times per year”.
- National authorities most frequently indicated “Guidelines & recommendations, including on standards” as being either “relevant” or “very relevant” to their work / activities.
- Among private enterprises or business associations, the products or services most frequently selected as being “(very) relevant” to respondents’ work / activities were “Reports & Research Publications” as well as “Events”. “Training material or toolkit” was most often selected as being only “somewhat” or “not relevant”. The group of “other” respondents gave the same assessment for this service.

#### *2. ENISA’s contribution to NIS in the EU*

- All respondents to the public consultation indicated that ENISA had achieved its targeted objectives to some or to a great extent.
- The objective of “Developing and maintaining a high level of expertise in cybersecurity” was selected as being achieved to a “great extent” or to “some extent” by the highest number of respondents (86% or 56), followed by “Supporting cooperation in the cybersecurity community, e.g. through public-private cooperation, information sharing, enhancing community building, coordinating the Cyber Europe Exercise” (79% or 51).

- When comparing the responses of different stakeholder categories, the results showed that the three categories felt different about which objectives had been met to a “great” or to “some extent”.
  - All national authorities (100% or 15) indicated that “Supporting the implementation of EU policy” had been achieved “to a great extent” or “to some extent”.
  - Private enterprises or business associations (71% or 17) most frequently indicated that ENISA had achieved “Supporting cooperation in the cybersecurity community e.g. through private-public cooperation, information sharing, enhancing community building”.
  - “Other” respondents (85% or 22) most frequently indicated that ENISA had achieved “Developing and maintaining a high-level of expertise in cybersecurity”.
- Respondents were asked to comment on what they perceived as ENISA’s main achievements over 2013-2016. In total 55 open responses were received of which 13 came from national authorities, 20 from private enterprises and business associations and 22 from “other” respondents. Respondents from all groups perceived the following as ENISA’s main achievements:
  - The coordination of the Cyber Europe exercises.
  - The provision of support to CERTs/CSIRTs through training and workshops fostering coordination and exchange.
  - ENISA’s publications that were considered as useful to create and update national security frameworks, as well as for reference to policy makers and cyber practitioners.
  - Assisting with the work under the NIS Directive.
  - Efforts to increase awareness on cybersecurity via the European Cybersecurity Month.

### 3. *Coherence of ENISA’s activities with those of other organisations*

- 83% respondents considered ENISA’s activities to be to a “large extent” or to “some extent” coherent with the policies and activities of their organisation (i.e. take into account, do not overlap, do not conflict with).

#### 4. Location and organisational structure

- Respondents were asked whether they felt that ENISA’s split location between Heraklion and Athens affected its ability to conduct its work effectively and efficiently. There were mixed perceptions expressed in relation to this question with 28% judging that the split location affected ENISA’s ability to conduct its work effectively and efficiently to “some extent” or to “a large extent”, while 20% stated “not at all”.

#### *Main results related to the forward looking questions:*

- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU, in particular the top 5 (in a list of 16) were: cooperation across Member States in matters related to cyber security; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks; skills development, education and training of professionals.
- A large majority (88%) of respondents considered the current instruments and mechanisms available at EU level to be insufficient or only partially adequate to address these. A large majority of respondents (98%) saw a need for an EU body to respond to these needs and among them ENISA was considered to be the right organisation to do so by 99%.

#### *Main results related to the forward looking questions regarding specific topics:*

##### 1. Future needs and challenges

- Respondents were asked to select the most urgent needs or gaps in the cyber security field in the EU over the next ten years among a list of 16 needs and gaps. From the assessment made by 84 respondents, the largest number of respondents identified “Cooperation across Member States in matters related to cyber security” and the “Capacity to prevent, detect and resolve large scale cyber-attacks” as a main gap or need in the cybersecurity field in the EU over the next ten years. A majority of respondents within each respondent category (i.e. national authorities, private enterprise or business association and “other”) identified these as needs or gaps.

- The views of the different respondent groups in relation to each of the options were relatively balanced, with the notable exception - among the most referred to gaps or needs - of “Cooperation and information sharing between different stakeholders, including public-private cooperation” where only two national authority respondents (out of a total of 14 national authority respondents) identified it as one of the most urgent needs or gaps.
- 55 respondents elaborated further on their answers to the question of what the most urgent needs or gaps in cybersecurity field will be in the next ten years. Out of the respondents to this open question, six were national authorities, 21 represented private enterprises or business associations, and 29 belonged to the group of “other” respondents. The contributions below represent the responses of all respondents given that little to no divergence was found in the answers among the different respondent categories:
  - Respondents commenting on the need for increased cooperation across Member States suggested that cooperation was necessary not only to bridge the security gaps that arise from a lack of cross-country cooperation, but also to build trust and confidence within the EU in matters of cybersecurity. Some respondents pointed to additional benefits of such cooperation, including increased market integration through the provision of internet services, support to the increase in cybersecurity capacity of less advanced Member States, and innovation for responses to current and future threats.
  - Closely linked to the identified need for cooperation were the identified needs for harmonised standards and certification in the field of cybersecurity, where respondents stated that the establishment of a common certification framework would help bridge inconsistencies and gaps in the implementation of security controls as well as to achieve trust across Europe.
  - Comments on the need to increase capacity to prevent, detect and resolve attacks pointed to the fact that the EU should step up the detection and real-time response to cyberattacks in information, communication technology (ICT), critical infrastructures, SMEs, government and public agencies.
  - Another largely discussed need or gap relates to skills development and education in the field of cybersecurity. Respondents commenting on this priority saw the need to increase the skills for cybersecurity professionals, particularly to address the changing market needs where industries increasingly need a highly skilled workforce. Respondents further commented that increasing citizen awareness on the importance of cybersecurity was a gap to be necessarily filled in given that “the human element” is the weakest link in cybersecurity.



- In this context, respondents from the groups of private enterprises and business associations and “other” respondents proposed a set of roles that ENISA could take on to address the identified needs or gaps. These included:
  - Promote coordination among EU institutions, Member States and the private sector, facilitating cooperation and effective flow of threat and incident information for swift responses and adaptation of security defensive solutions.
  - Support towards Member States to further cybersecurity research.
  - support the harmonisation of standards and certification by promoting existing internationally agreed standards and frameworks.
  - support government efforts related to the development of cybersecurity workforce through the development of guidelines-supporting cybersecurity experts across Europe.
  - ensure that the NIS Directive transposition across Member States is homogeneous.
- Respondents were also asked if the current instruments and mechanisms at the European level are adequate to promote and ensure cybersecurity in relation to the needs previously identified. Only 6% of the respondents judged the current instruments and mechanisms at the European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be “fully adequate” to promote and ensure cybersecurity. 83% of respondents regarded them as either “partially” or only “marginally adequate” and 5% found them “not at all adequate”. National authority respondents appear to be more positive about the adequacy of these instruments and mechanisms in comparison with representatives of private enterprises or business associations and “other” respondents.
- Based on the identified needs or gaps, respondents were asked what the priorities for EU action should be from now on and select up to three responses out of a list of 15. “Stronger EU cooperation mechanisms between Member States, including at operational level” was most frequently selected as a top priority, followed by “Stronger public-private cooperation in cybersecurity” and “improving research to address cybersecurity challenges”.

## 2. *The role of an EU body in the future EU cybersecurity landscape*

- 98% of respondents saw a role for an EU-level-body in improving cybersecurity across the EU. Furthermore, almost all of the respondents (81 out of 82) who saw a role for an EU-level body in improving cybersecurity considered that ENISA could fulfil a role in bridging the different gaps in the future.
- Respondents have given examples of what ENISA’s future role could be in addressing identified gaps and needs. The role seen for ENISA covered the following activities: fostering cooperation between Member States at international level and between the public and private sector; having a stronger role in policy development and implementation; ensuring harmonisation of approaches and setting baselines; certification and standardisation; providing incident response information; ensuring awareness raising, training and capacity building; supporting the private sector; ensuring the transposition of the NIS Directive; and fostering research. These activities were suggested by all respondent groups. Some national authorities underlined that ENISA should not take on an operational role in providing incident response activities, considering potential overlaps with CERT-EU and the need for the Agency to focus its resources on its core activities.

## 18.2. Results of the survey to CERT / CSIRT

The survey was conducted in January 2017 and targeted CERT / CSIRT representatives from all 28 Member States.

28 respondents completed the survey and 7 partially completed it. 1 partially completed response was deleted as it only answered the first question of the survey. The other partially completed answers were kept as they answered all of the mandatory questions except the ones in the section on “degree of coherence and complementarity”.

*Main results:*

- 88% of respondents assessed that ENISA proactively supported cooperation among CERTs/CSIRTs to some or high extent during the 2013-2016 period. 82% of respondents assessed that ENISA covered the needs of the CERTs/CSIRTs to some or high extent.
- A very large majority (97%) expressed the view that ENISA’s capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) for CERTs/CSIRTs’ development were either important or very important.

- Looking at the future, 85% of respondents assessed that the new roles foreseen for ENISA by the NIS Directive would enable ENISA to better cover CERTs/CSIRTs' needs to either some or high extent.
- Respondents were asked to provide more details, in concrete terms, of what they would foresee ENISA doing as part of its new role as secretariat for the CSIRTs Network (as foreseen in the NIS Directive); 16 respondents provided answers in the following categories:
  - Facilitating cooperation (standardization in data sharing at EU level; providing the link between the Cooperation and CSIRT Network Groups ; coordination of the CSIRTs' network activities)
  - Direct Support (e.g. contributing to the work program development)
  - Helping CERTs implement the NIS Directive (e.g. providing best practice recommendations on technical, organisational and legal issues concerning CSIRTs)
  - Capacity Building
  - Understanding Needs

### 18.3. Results of the survey to ENISA's staff and direct stakeholders

The survey addressed to ENISA's staff and direct stakeholders took place in January 2017.

The link to the survey was sent to a total of 173 stakeholders. We obtained 106 responses made up of 83 complete answers and 23 partially complete answers. Only the partially completed answers which responded to 50% or more of the mandatory questions were taken into account for the analysis. This led to a total of 88 answers, of which 83 were complete answers and 5 were partially completed answers. The responses provided a good representation of ENISA staff, Management and Executive Board members (71%) as well as Permanent Stakeholder Group (PSG) and Network of Liaison Officers (NLOs) representatives (29%).

*Main results:*

1. ENISA's organisational set-up
  - When asked whether the size of the Agency is appropriate for the work entrusted to ENISA and adequate for the actual workload, the majority of respondents gave a negative opinion: 14.8 % not at all; 36.4% to a limited extent; 30.7% to some extent. Respondents provided similar views across all categories; however ENISA staff (including management) were slightly more negative than Management Board (MB), Executive Board (EB), PSG and NLOs.

- The majority of ENISA staff found that the recruitment and training procedures are appropriate for the work entrusted to ENISA and adequate for the actual workload only to a limited extent (20.5%) or some extent (43.2%). The PSG expressed similar views, while Management Board and Executive Board were more positive, with almost 90% considering the recruitment and training procedures adequate to some or high extent.
  - The staff composition was judged adequate to some or high extent by the majority of respondents (64.8%), with similar opinions expressed across all categories of respondents.
2. ENISA's effectiveness and efficiency
- The majority of respondents (85,2%) found that the current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the effective and efficient functioning of the Agency to some or high extent. The respondents from the Management Board, Executive Board and PSG were slightly more positive than the ENISA staff and the NLOs.
  - The establishment of an Executive Board was found to lead to a more efficient functioning of the Management Board. This view has been supported in particular by the representatives of the MB and EB, while about 40% of the representatives of the staff, the PSG and NLOs said they did not know.
  - ENISA's management practices are considered conducive to creating an effective and efficient organisation to some or high extent respectively by 73% and 74% of respondents across all categories. ENISA's staff was slightly more critical than the other categories: 7% of the respondents found the management practices not at all conducive of effectiveness.
  - The questions on whether ENISA's location enables it to effectively (i.e. in terms of meeting its objectives) and efficiently conduct its work received mixed feedback. With regard to effectiveness respondents replied: not at all (11.4%); to a limited extent (17.0%); to some extent (27.3%); to high extent (39.8%). ENISA staff was proportionally more positive than the other categories of respondents; for example, 42% of respondents from the Management Board replied "not at all" or "to a limited extent". The same trend was found in the question related to the efficiency of the location: 11,4 % replied "not at all", 23,9% "to a limited extent"; 23,9% "to some extent", 35,2% "to a high extent". Again, ENISA staff was found to reply more positively than the other categories of respondents.
3. ENISA's relationship with stakeholders:
- The vast majority (93%) expressed the views that ENISA to some or high extent has built strong and trustful relationships with its stakeholders when executing its mandate.

- 94% of respondents found that ENISA's activities are coherent with the policies and activities of its stakeholders. Respondents across all categories expressed similar views.

#### **18.4. Results of the workshop on the future contribution of ENISA to EU cybersecurity**

The workshop took place on 22 March 2017 in Brussels at the premises of DG Connect.

The workshop hosted a variety of stakeholders to enable engaging discussions. A group of 48 stakeholders included representatives of the Commission, members of ENISA's Management and Executive Board, as well as members ENISA's permanent stakeholder's group (PSG), representatives from national cybersecurity authorities and CERTs, industry representatives and academia.

The workshop was an opportunity to actively engage with them to discuss, qualify and validate the preliminary findings of the draft interim report on the "Study on the Evaluation of the European Union Agency for Network and Information Security"<sup>23</sup> and to discuss the policy options for the future of ENISA. By discussing key findings with stakeholders, an assessment of findings and additional insights were gained contributing to the data collection and analysis of the study. The group also discussed the perceived needs in Europe in the area of cybersecurity.

#### *Main results:*

- The workshop participants identified the following four high relevance objectives for the work of the Agency:
  - Developing and maintaining a high level of expertise of EU actors.
  - Assisting Member States and the EU institutions in developing policies necessary to meet the regulatory requirements of NIS.
  - Assisting Member States and the Commission in enhancing capacity building throughout the EU.
  - Stimulating cooperation both between EU Member States and between related NIS communities.

- The workshop participants assessed that the ENISA mandate was highly relevant but the actual activities did not fully meet the needs of the community. The main limitations noted were the fixed term ENISA mandate; limited ENISA's in-house expertise; limited ENISA's visibility; and limited resources.
- The workshop participants assessed that ENISA's main added value is the ability to enhance cooperation between Member States and NIS communities.
- A discussion took place on the possible options for the future of ENISA. Four options were presented (Keeping the status quo; Terminating ENISA; Strengthening ENISA with changes to its mandate; Establishing an EU cybersecurity centre). Following the discussion workshop participants indicated the option to strengthen ENISA with changes to its mandate as the favourite one. It was, however, indicated that the option of establishing an EU cybersecurity centre should have been further investigated.

## 19. SUMMARY OF RESULTS FROM THE CONSULTATIONS REGARDING ICT SECURITY CERTIFICATION FRAMEWORK

**19.1.** Results of the public consultation on the contractual public-private partnership on cybersecurity and accompanying measures related to ICT security certification

The public consultation on the contractual Public Private Partnership on cybersecurity took place from 18 December 2015 to 11 March 2016.

Respondents represented a wide variety of organisations, with a good balance between big business (41), SMEs (33), microbusiness (6) as well as other stakeholders e.g. research bodies (20), national public administrations (7) and regulators (1), NGOs (13).

*Main results related to certification:*

1. When answering the question whether national certification schemes are mutually recognised across EU Member States 50,4% (121 out of 240) of respondents stated they "did not know", 25.8% (62 out of 240) replied 'No', while 23.8% (57 out of 240) replied 'Yes'.
2. 37,9% of respondents (91 out of 240) think the **existing certification schemes do not support the needs of Europe's industry**. On the other hand, 17, 5% (42 out of 240) – mainly global companies operating on the European market - expressed the opposite view.

3. 49.6% (119 out of 240) of respondents says that it is not easy to demonstrate equivalence between standards, certification schemes, and labels. 37.9% (91 out of 240) replied 'I do not know'.

In comments to the open question, some respondents emphasize that no reliable certification scheme exists at the moment at the European level, some others point also to the fact that existing national schemes act as barriers to market entry, complaining about the costs of complying with several certification schemes in Europe. Some of the industry associations state that **further fragmenting of the market** with numerous certification schemes **should be avoided**.

At the same time, some industry players emphasize the risk for companies of being overburdened with yet another certification scheme and therefore suggest a cautious approach to any new initiatives in this regard.

With regard to the EU cybersecurity industry, the majority of respondents view the European market as insufficiently competitive. Among the main weaknesses identified are different rules to access public procurement and fragmentation of EU market (in terms of cybersecurity requirements). In particular:

4. More than **44.3%** of respondents (78 out of 176) stated that they **experience barriers** related to market access and export within the EU and/or beyond EU countries, particularly due to the fragmentation of the EU cybersecurity market along EU internal borders.
5. Some respondents also pointed out that the lack of a European certification scheme and the emergence of national schemes, is factor that force them to go through **different costly and complex procedures**.

## **19.2.** Results of the Workshops on 'The development of a European ICT Security Certification Framework'

The series of workshops presented below served as a follow-up on the Commission's commitment to consult stakeholders in the process of developing a proposal for a European ICT security certification framework as stated in Commissions' COM(2016) 410.

### *19.2.1. Workshop 1: October 2016*

The Commission (DG CNECT, JRC) together with ENISA organised a workshop aiming at bringing together representatives from Member States to discuss the development of a possible ICT security certification of products and services. 15 representatives of Member States took part in the workshop. This workshop was a continuation of previous event on the topic of security certification. organised by ENISA in February and March 2016.

#### *Main conclusions:*

- A majority of national delegates welcomed the initiative of the Commission in the area of ICT security certification. In particular, they stressed the need to foster harmonization of security requirements at the European level.
- A roadmap indicating next steps for the development of European security certification framework was to be elaborated.
- A future certification framework should be based on different levels of certification including self-certification.
- It is necessary to harmonize evaluation methodologies across European labs.
- Any certification initiative should build as much as possible on the existing mechanism and international standards.

### *19.2.2. Workshop 2: December 2016*

On 5 December 2016, the Commission and ENISA organised a follow-up workshop aiming at bringing together representatives from Member States to discuss the development of a possible ICT security certification of products and services. This workshop built on the discussion of the previous workshop (October) and saw the participation of 18 representatives from Member States.

A draft Roadmap - previously circulated by email – was further discussed during the workshop. While agreeing on the need to harmonize rules for ICT certification procedures at the European level, Member States called for greater clarity on key issues such as: Definition of scope of the overall initiative (e.g. products vs services, products category, sector)

#### *Main conclusions:*



- It was recommended that the Commission and Member States should: a) identify key sectors or product category; b) define fundamental principles for security certification in Europe; c) consider a pilot project that can help provide the skeleton of a future European certification and labelling Framework, identify initial priorities, estimates, resource allocation and timing.
- The European framework should be based, as much as possible, on existing mechanism and internationally recognised standards. Participants were asked to outline a number of key points that will feed in the upcoming activities leading to the development of the future framework. The following work items – not formally adopted – were identified:
  - Existing initiatives and practises should be identified;
  - Industry’s point of view, through European Cybersecurity Organisation (ECISO), should also be taken into consideration;
  - A master plan of all ongoing activities should be put together;
  - Exceptions, due to high value/high risk should be clearly scoped and considered; and
  - The aspect of liability should also be taken into account.

All participants were given the opportunity to provide a written contribution by the end of December 2016.

### *19.2.3. Workshop 3: April 2017*

On 27 April 2017, the Commission and ENISA organized a workshop attended by 90 participants. This workshop was a follow-up on the Commission's previous workshops (October, December 2016) and saw the participation of representatives from industry as well as Member States.

The workshop consisted of a plenary session in which public and private sector organizations presented their views on the challenges of a European ICT security certification framework. In the afternoon session participants had the opportunity to discuss in small focus groups the four main policy options that were presented such as:

Option 0 - Do nothing: No EU policy initiative or action – baseline scenario

Option 1 - Soft law approach: The Commission to encourage and support national or industry initiatives

Option 2 - Extension of SOGIS agreement: Legislative proposal making MS participation to the SOG-IS agreement mandatory

Option 3 - European certification framework: EU-wide framework with its own scope, functioning and governance rules.

*Main conclusions:*

- Following the group discussion, there was an overwhelming support - from Member States (DE, FR, SE, NL, UK, AT, IT) and industry – for the policy Option that proposes the creation of a European institutional framework for ICT certification that builds on existing ICT certification mechanisms (e.g. SOG-IS Mutual Recognition Agreement);
- However, many underlined the importance to allocate adequate resources in order to ensure an appropriate maintenance of such a Framework;
- For this purpose, it was stressed that an EU body/ Agency (e.g. ENISA) should help carry out secretarial tasks;
- Other Options: it emerged that "no-action option" is not an option. While being more cost-effective, a soft law approach will not tackle the issue of fragmentation caused by emerging national ICT certification schemes popping up across Europe;
- Some Member States (e.g. SE, UK) and industry (e.g., DigitalEurope) called for a European ICT security framework to be built, as much as possible, on internationally recognized standards for cybersecurity certification; and
- As the smart meters industry is exposed to many national ICT certification requirements, the presenter from the trade association (ESMIG) offered to become pilot industry in the context of the development of an EU-wide approach to ICT security certification.

**19.3.** Results of the ENISA Survey on ICT security certification in the EU

This targeted survey took place from 5 until 19 May 2017. It has been broadly publicised within the confined certification community. Total number of participants: 33.

Respondents, who addressed questions related to certification, included national authorities/agencies (14); manufacturer / provider of ICT products and services (9); User / Customer / Consumer of ICT products and services (3); security certification laboratory (1); other (6).

*This survey aimed to consult these stakeholders on the issue of security certification and labelling and seek structured feedback against set policy options such as:*

Option 0 - Do nothing: No EU policy initiative or action – baseline scenario

Option 1 - Soft law approach: The Commission to encourage and support national or industry initiatives

Option 2 - Extension of SOGIS agreement: Legislative proposal making MS participation to the SOG-IS agreement mandatory

Option 3 - European certification framework: EU-wide framework with its own scope, functioning and governance rules.

*Main results:*

- 57%, (19) is aware of multiple existing ICT security certification schemes across EU Member States for the same product or service
- 37%, (12) indicated that they were not aware of multiple ICT security schemes across EU, but they expressed their preparedness to accept one
- the respondents indicated that the main problems they have encountered when dealing with security certification include:
  - 72% (24) Cost
  - 57% (19) Duration of process
  - 51% (17) Lack of mutual recognition of certificates across Member States
  - 45% (15) Lack of a dedicated scheme to cyber -certify a specific product/service
  - 39 (13) Lack of certification support for the lifecycle of the product (e.g., incremental certification for software and hardware changes/updates)
  - 36% (12) Lack of transparency
- 90% (30) agreed that mutual recognition of ICT security certification schemes is desirable at European level.
- 81% (27) agreed also that certification and labelling can be effective tools to increase transparency about the level of security assurances of ICT products/services, and enhance trust across the Digital Single Market.

- However, it has been noted that a ranking of assurance levels with clear information is required as oversimplifying could introduce additional risks. In addition, certification and labelling should denote only baseline security requirements and should not deferment innovation or increase complexity.
- 66% (22) agreed on the need for greater efforts to promote ICT security certification
- 21% (7) stated that ICT security certification is a pure market issue and there is no need for additional support.
- 75% (25) identified the need for ICT security and labelling in the Internet of Things-domain, due to imminent ubiquity of IoT, issues of vulnerabilities and the required interoperability across different platforms.
- 66% (22) identified the need for ICT security certification in the Industrial Control System (ICS)-domain, due to the criticality of processes they support and the level of cyber threats they are exposed to.

### *Policy Options*

- 33% (11) have seen favourably a generic European certification framework, laying down essential rules for mutual recognition of certificates issued.
- 18% (6) favoured the “Soft law approach”, encouraging, supporting and to the extent possible coordinating the adoption and use of certification initiatives at European level
- 12% (4) were in favour of extending the SOG-IS MRA to all Member States and make it mandatory.
- 12% (4) opted for regulating the security of ICT products and services and specify essential security requirements for such products to be placed on the market. T
- The remaining respondents indicated that a mixed approach, from all the aforementioned options, should be the preferred path of action instead. They argued that mutual recognition of existing certification schemes and labelling programs can promote a robust Digital Single Market and support EU digital economy while an entirely new certification framework would not be able to scale with the changing security landscape and consider the state-of-the-art
- 45% (15) were in favour of exploiting the current SOG-IS MRA as the basis to build an EU-wide certification Framework, while 21% (7) stated otherwise and 34% (11) did not answer either positive or negative on the role of SOG-IS MRA.
- 66% (22) agreed that self-certification schemes could be considered a viable option to boost the level of cyber-security for selected product’ domains, especially for low assurance level products and should be considered as an integral part of the future EU certification framework, drawing also experience from existing market driven initiatives. Nevertheless, 24% (8) of the respondents disagree that self-certification should be considered, as it does not provide any assurance, there is no control and it is not sufficient unless there is a third party validating conformance
- 90% (30) indicated that the processes and tools used for security certification should be improved to ensure the required flexibility by allowing different level of assurance.

- 66% (22) were in favour of the introduction of a common label across the EU. Such label will indicate that the products have been certified within a certification scheme in accordance with EU rules and visualize that the characteristics of the products and services comply with specific requirements. Nevertheless, the respondents who were not in favour of a common label (8), proposed a specific sectoral labelling or consider that it could be difficult for complex systems and/or it could also result in a false sense of security
- 78% (26) envisage a role for existing EU Commission's bodies and agencies (e.g. JRC, ENISA, ACER) in a possible future EU certification and labelling security framework. Among the respondents who did not see a role for existing EU Commission's bodies and agencies (4), supporting actions such as determining a minimum level of security per category of technology, issuing voluntary guidelines for both industry and consumers, were envisioned, without identifying the key EU body or agency.

#### **19.4. Results of the SME survey on ICT security certification**

The survey was carried out in June 2017<sup>134</sup>. As of 23 June 2017, 46 respondents have answered the survey. Below are the main preliminary results. Please note that the submission to the Regulatory Scrutiny Board took place on 28 June 2017 while the survey was still ongoing.

##### *Main preliminary results:*

- 40 out of 46 respondents think that ICT security certification is a valuable tool to reduce cyber vulnerabilities of ICT products or services (4 replied "no", 2 replied "I don't know").
- 35 out of 46 respondents believe that the creation of an EU-wide ICT certification framework based on mutual recognition could facilitate SMEs' access to public procurements across Member States (4 replied "no", 7 replied "I don't know").
- 39 out of 46 respondents would be in favour of a common label for certified ICT products (3 replied "no", 4 replied "I don't know").
- 35 out of 46 respondents consider that creating a European certification general framework laying down the essential rules for mutual recognition of certificates is an appropriate action to achieve the objective of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU (multiple answers question).

---

<sup>134</sup> Survey opening dates: 02-30 June 2017. The survey can be found at: <https://ec.europa.eu/eusurvey/runner/ICTCertificationSecurityFramework>.

- 24 out of 46 respondents consider that regulating the security of ICT products and services, specifying essential security requirements for such products to be placed on the market is an appropriate action to achieve the objective of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU (multiple answers question).
- 20 out of 46 respondents see the emergence of multiple national or sectorial certification schemes as a likely scenario in the future, especially in view of the growing cybersecurity risks (8 replied "no", 12 replied "I don't know").
- Two-thirds (30 out of 46) respondents think that a mutual recognition mechanism of certificates across all Member States can be useful to simplify procedures and cut administrative burdens for them (multiple answers question).
- Two-thirds (30 out of 46 respondents) think that a mutual recognition mechanism of certificates across all Member States could be useful to reduce cost of compliance for them (multiple answers question).
- More than half (25 out of 46 respondents) believe that self-certification schemes are NOT a viable option to boost the level of cybersecurity for selected product domains (17 replied "yes", and 4 replied "I don't know").
- 37 out of 46 respondents think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (6 replied "no" and 3 replied "I don't know").
- 34 out of 46 respondents are of the opinion that a labelling scheme underlying the level of security and privacy an IoT device encompasses would help them increase trust in IoT products and services (4 replied "no", 8 replied "I don't know").
- 34 out of 46 respondents identified the cost of current ICT security certification procedures as a problem they encountered (multiple answers question).
- 28 out of 46 respondents identified the duration of the process of current ICT security certification procedures as a problem they encountered (multiple answers question).
- 18 out of 46 respondents believe that the current existence of multiple ICT certification schemes represents a barrier to market entry for them because they are too costly and therefore not affordable for SMEs (most respondents left question 6 blank, 6 replied "lack of reference levels").

- 25 out of 46 respondents said that the main reason that makes them reluctant to buy emerging digital technology products and services is that they are afraid of the cybersecurity risks and consequent damages that may be brought to them (multiple answers question).
- 25 out of 46 respondents feel comfortable installing any software updates needed for the proper functioning of their connected device themselves (multiple answers question).
- 24 out of 46 respondents estimate the cost for certifying an ICT service or product to be between 10,000 and 100,000. 15 out of 46 estimated the cost to be between 100,000 and 1,000,000.
- 18 out of 46 respondents believe ENISA should promote certification schemes and identify the common standards (most didn't reply, 2 replied "ENISA should make sure competition is respected and that the market remains open").

### ANNEX 3:

#### EU Agencies Budget and Staff

The table below provides information on the total EU financial contribution to 32 decentralised EU agencies, as well as their authorised establishment plans (i.e. staff) in 2017. The information derives from the "Draft General Budget of the EU for the financial year 2018 – Working Document Part III – Bodies set up by having legal personality and Public-Private Partnership"<sup>135</sup>, unless otherwise stated.

No.	Agency	Total EU contribution (million EUR)	Authorised establishment plan (staff) <sup>136</sup>
1.	European Agency for the Management of Operational Cooperation at the External Borders – <b>FRONTEX</b>	281.267	352
2.	European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice – <b>EU-LISA</b>	153.334	131
3.	European Police Office – <b>EUROPOL</b>	114.624	550
4.	European Food Safety Authority – <b>EFSA</b>	77.333	323
5.	European Chemicals Agency – <b>ECHA</b> <sup>137</sup>	75.173	460
6.	European Maritime Safety Agency – <b>EMSA</b>	72.359	212
7.	European Asylum Support Office – <b>EASO</b>	69.206	155
8.	European Centre for Disease Prevention and Control – <b>ECDC</b>	56.766	182
9.	The European Union s Judicial Cooperation Unit - <b>EUROJUST</b>	48.379	208
10.	European Environment Agency – <b>EEA</b>	36.309	127
11.	European Aviation Safety Agency – <b>EASA</b>	35.985	678
12.	European Railway Safety Agency – <b>ERA</b>	30	139

<sup>135</sup> COM(2017) 400 – June 2017, available at: <https://myintracomm.ec.europa.eu/budgweb/EN/budgweb/EN/budgweb/proc/adopt/Documents/DB2018-WD03-agencies.pdf>.

<sup>136</sup> This category includes only permanent staff. It does not include contract agents and seconded national experts.

<sup>137</sup> This agency is partially self-financed.



No.	Agency	Total EU contribution (million EUR)	Authorised establishment plan (staff) <sup>136</sup>
13.	European Medicines Agency – <b>EMA</b>	28.892	596
14.	European GNSS Agency – <b>GSA</b> <sup>138</sup>	27.847	116
15.	European Union Agency for Fundamental Rights – <b>FRA</b>	22.567	72
16.	European foundation for improvement of living & working conditions – <b>EUROFOUND</b>	20.371	93
17.	European Training Foundation – <b>ETF</b>	20.144	88
18.	European Centre for the Development of Vocational Training – <b>CEDEFOP</b>	17.434	92
19.	European Fisheries Control Agency – <b>EFCA</b>	17.113	61
20.	European Monitoring Centre for Drugs and Drug Addiction – <b>EMCDDA</b>	15.136	77
21.	European Agency for Safety and Health at Work – <b>EU-OSHA</b>	14.679	40
22.	European Banking Authority – <b>EBA</b> <sup>139</sup>	14.543	134
23.	European Agency for the Cooperation of Energy Regulators – <b>ACER</b>	13.272	68
24.	European Securities and Markets Authority – <b>ESMA</b>	11.02	150
25.	<b>European Network and Information Security Agency – ENISA</b>	<b>10.322</b>	<b>48</b>
26.	European Police College – <b>CEPOL</b>	9.28	31
27.	European Insurance and Occupational Pensions Authority – <b>EIOPA</b>	8.946	101
28.	European Institute for Gender equality – <b>EIGE</b>	7.628	27
29.	Office of the body of European Regulators for Electronic Communications – <b>BEREC</b>	4.246	14
30.	Single Resolution Board – <b>SRB</b> <sup>140</sup>	0	350
31.	Community Plant Variety Office – <b>CPVO</b> <sup>141</sup>	0	44

<sup>138</sup> This excludes the amount delegated to GSA in 2017 and 2018.

<sup>139</sup> This agency is partially co-financed by national public authorities.

<sup>140</sup> This agency is fully self-financed and does not receive EU contribution.

<sup>141</sup> This agency is fully self-financed and does not receive EU contribution.

No.	Agency	Total EU contribution (million EUR)	Authorised establishment plan (staff) <sup>136</sup>
32.	European Union Intellectual Property Office – <b>EUIPO</b> <sup>142</sup>	0	792

\*\*\*

<sup>142</sup> This agency is fully self-financed and does not receive EU contribution.

#### **Annex 4: Preliminary mapping of the EU-level entities that provide cybersecurity content**

The tables below provide a first listing of the EU level entities that provide cybersecurity related information, the type of information, the target audience and the frequency with which they convey such information.

This preliminary mapping was provided by the Commission DG Joint Research Centre (JRC) as part of a technical report on the possible requirements of a European Cybersecurity Information Hub.

Acronym	Description
CERT-EU	After a pilot phase of one year and a successful assessment by its constituency and its peers, the EU institutions have decided to set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies on September 11th 2012. The team is made up of IT security experts from the main EU institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies. <a href="https://cert.europa.eu/cert/filiteadition/en/CERT-LatestNews.html">https://cert.europa.eu/cert/filiteadition/en/CERT-LatestNews.html</a>
ENISA	The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. ENISA is contributing to a high level of network and information security (NIS) within the European Union, by developing and promoting a culture of NIS in society to assist in the proper functioning of the internal market <a href="https://www.enisa.europa.eu/">https://www.enisa.europa.eu/</a>
ERN CIP	European Reference Network for Critical Infrastructure Protection (ERN CIP), aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards and to the creation of a single market for security solutions.
ETSI	<a href="https://ec.europa.eu/ict/en/network-bureau/european-reference-network-critical-infrastructure-protection-ern-cip">https://ec.europa.eu/ict/en/network-bureau/european-reference-network-critical-infrastructure-protection-ern-cip</a> ETSI, the European Telecommunications Standards Institute, produces globally applicable standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. Our standards enable the technologies on which business and society rely. For example, our standards for GSM™, DECT™, Smart Cards and electronic signatures have helped to revolutionize modern life all over the world. <a href="http://www.etsi.org/">http://www.etsi.org/</a>
CENELEC	CENELEC is the European Committee for Electrotechnical Standardization and is responsible for standardization in the electrotechnical engineering field. CENELEC prepares voluntary standards, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market. <a href="https://www.cenelec.eu/Pages/default.aspx">https://www.cenelec.eu/Pages/default.aspx</a>
Eurolex	EuroLex provides free access, in the 24 official EU languages, to: the authentic Official Journal of the European Union EU law (EU treaties, directives, regulations, decisions, consolidated legislation, etc.) preparatory acts (legislative proposals, reports, green and white papers, etc.) EU case-law (judgments, orders, etc.) International agreements EFTA documents summaries of EU legislation, which put legal acts into a policy context, explained in plain language other public documents.
STOA	<a href="http://eur-lex.europa.eu/homepage.html">http://eur-lex.europa.eu/homepage.html</a> European Parliament Science and Technology Options Assessment (STOA) The STOA Panel forms an integral part of the structure of the European Parliament. It is composed of 25 Members of the European Parliament (MEPs) who are nominated by nine permanent Committees of the Parliament: AGRI, CULT, EMPL, ENVI, IMCO, ITRE, JURI, LIBE and TRAN. The EP Vice-President responsible for STOA is a Member of the Panel ex officio. The members of the STOA Panel are appointed for a renewable two-and-a-half-year period.
SAM	<a href="http://www.europarl.europa.eu/stoa/">http://www.europarl.europa.eu/stoa/</a> Scientific Advice Mechanism: Scientific advice in the area of cybersecurity has been requested by Vice President Ansip and Commissioner Oettinger during the SAM High Level Group first meeting on 29 January 2016. The corresponding scoping paper outlines the issues at stake, the EU policy landscape and the potential areas for scientific advice to inform policy-making. <a href="https://ec.europa.eu/research/sam/index.cfm?page=cybersecurity">https://ec.europa.eu/research/sam/index.cfm?page=cybersecurity</a>
ACER	ACER's missions and tasks are defined by the Directives and Regulations of the Third Energy Package, especially Regulation (EC) 713/2009 establishing the Agency, in 2011. ACER received additional tasks under Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT) and in 2013 under Regulation (EU) No 347/2013 on guidelines for trans-European energy infrastructure. The Agency's overall mission, as stated in its founding regulation, is to complement and coordinate the work of national energy regulators at EU level, and to work towards the completion of the single EU energy market for electricity and natural gas. ACER plays a central role in the development of EU-wide network and market rules with a view to enhancing competition. The Agency coordinates regional and cross-regional initiatives, which favour market integration. It monitors the work of European networks of transmission system operators (ENTSOs), and notably, their EU-wide network development plans. Finally, ACER monitors the functioning of gas and electricity markets in general, and of wholesale energy trading in particular. <a href="http://www.acer.europa.eu/">http://www.acer.europa.eu/</a>
EDPS	The European Data Protection Supervisor (EDPS) is the European Union's (EU) independent data protection authority. It's general mission is to: monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals; advise EU institutions, and bodies on all matters relating to the processing of personal information. It is consulted by the EU legislator on proposals for legislation and new policy developments that may affect privacy; monitor new technology that may affect the protection of personal information; intervene before the Court of Justice of the EU to provide expert advice on interpreting data protection law; cooperate with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information. <a href="https://edps.europa.eu/">https://edps.europa.eu/</a>
JRC	As the European Commission's science and knowledge service, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle. Its work has a direct impact on the lives of citizens by contributing with its research outcomes to a healthy and safe environment, secure energy supplies, sustainable mobility and consumer health and safety. <a href="https://ec.europa.eu/jrc/en">https://ec.europa.eu/jrc/en</a>
Europol	Europol assists the 28 EU Member States in their fight against serious international crime and terrorism. Europol also works with many non-EU partner states and international organisations. <a href="https://www.europol.europa.eu/">https://www.europol.europa.eu/</a>
DG-ENER	The Directorate-General for Energy is one of 33 policy-specific departments in the European Commission. It focuses on developing and implementing the EU's energy policy – secure, sustainable, and competitive energy for Europe. The Directorate General develops and implements innovative policies aimed at: i) contributing to setting up an energy market providing citizens and business with affordable energy, competitive prices, and technologically advanced energy production, transport and consumption in line with the EU 2020 targets and with a view to the 2050 decarbonisation objective, ii) enhancing the conditions for safe and secure energy supply in a spirit of solidarity between EU countries ensuring a high degree of protection for European citizen <a href="https://ec.europa.eu/energy/en">https://ec.europa.eu/energy/en</a>
ECSC	The European Cyber Security Organisation (ECSC) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016. ECSC represents an industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). The main objective of ECSC is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity, and in particular to: Foster and protect from cyber threats the growth of the European Digital Single Market; Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position; Develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader. <a href="https://www.ecs-org.eu/">https://www.ecs-org.eu/</a>
IOTA	The Internet of Things Association is an industry forum hosted by Smartex, not an EU body <a href="http://www.smartex.com/IOTA/">http://www.smartex.com/IOTA/</a>
Working Group Art. 29	The Working Party was set up to achieve several primary objectives: To provide expert opinion from member state level to the Commission on questions of data protection; To promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities; To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy; To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community. <a href="http://ec.europa.eu/newsroom/ust/item-detail.cfm?item_id=50083">http://ec.europa.eu/newsroom/ust/item-detail.cfm?item_id=50083</a>

Entity	Type of Content			Domain	Nature	Target Audience	Access Media		
	Knowledge	Services	Software Tools				Web portal	Mobile phone app	Social Media
CERT-EU	White papers/Guidelines, Software vulnerabilities, Web articles	Monitoring of cybersecurity news using European Media Monitor (EEM)		Information Systems	Technical	General	X	X	
ENISA	Best practices & recommendations, Standards and certifications	Training of cyber security specialists, Cyber Exercises and Cyber Security Education, Trust services, Incident Reporting		Cloud and Big Data, Critical Infrastructure and Services, Cyber Crisis Management, IoT and Smart Infrastructures, Data protection, National Cyber Security Strategies, Threat and risk management	Technical	General	X		Twitter, Facebook, LinkedIn, Youtube
ERNCLIP	Requirements and Guidelines	Certification		Critical Infrastructures and Industrial Automation and Control Systems		Industry	X		
ETSI	Standards and White papers			Telecommunication system	Technical	Industry	X		Twitter, Facebook, LinkedIn, Google+, Youtube
CENELEC	Standards and Guidelines			Electrotechnical engineering	Technical	Industry	X		Twitter, Facebook, LinkedIn, YouTube
Eurolex	Directives and Regulation			General purpose	Legislation	General	X		
STOA	Studies			General purpose	Scientific	Government Institutions	X		Twitter, Facebook
SAM	Observations, Recommendations, and Scientific opinions			General purpose in the EU policy landscape	Scientific	Government Institutions	X		
ACER	Recommendations, Guidelines, and Opinions			Energy infrastructure	Technical	Industry and Government Institutions	X		
EDPS	Reference library, Annual Reports, Factsheets, Speeches and Articles, EDPS Strategy			Data protection	Technical	Industry and Government Institutions	X	X	Twitter, LinkedIn, Youtube
JRC	Publications, Technical Reports, Scientific Reports, Patents and Technologies	Science oriented policy support	Scientific Tools and Databases	General purpose in the EU policy landscape	Scientific	General	X		Twitter, Facebook, LinkedIn, Youtube
Europol	Articles, Definitions, Public awareness and prevention guides, Reports	Threat assessments, Early warning notifications		Cybercrime and terrorism	Technical	General	X		Facebook, Twitter, Youtube, LinkedIn
DG-ENER	Studies, Consultations, Reports, Infographics			Energy infrastructure	Technical	Industry and Government Institutions	X		Twitter, Pinterest
ESCO	Reference Documents			Public-Private partnership	Technical	Industry	X		Twitter
IOTA	Guidelines, Letters of members/chair, Opinions			Internet of Things (IoT)	Technical	Industry	X		
Working Group Art. 29				Data protection	Legislation	General	X		



Brussels, 13.9.2017  
SWD(2017) 500 final

PART 2/6

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF  
THE COUNCIL**

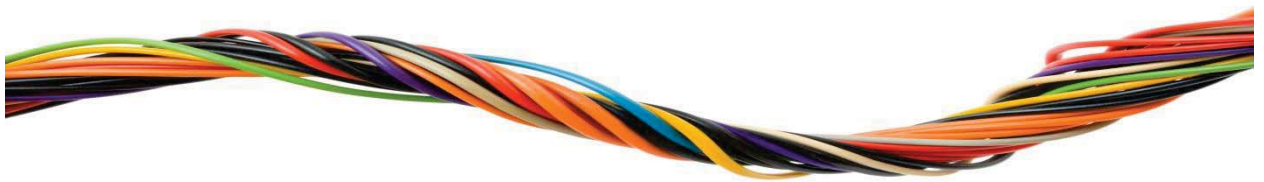
**on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013,  
and on Information and Communication Technology cybersecurity certification  
("Cybersecurity Act")**

{COM(2017) 477 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

# Study on the Evaluation of the European Union Agency for Network and Information Security



## **Final Report**

A study prepared for the European Commission  
DG Communications Networks, Content & Technology  
by:



**This study was carried out for the European Commission by**



Karin Attström, Vanessa Ludden, Franziska Lessmann  
Ramboll



Pär Weström, Johannes Conrads  
Carsa  
Carretera de Asúa, 6  
48930 Getxo  
Vizcaya – Spain  
<http://www.carsa.es>

With contributions from Helena Farrand Carrapico, Aston University; Andrej Savin, Copenhagen Business School; Cristina de la Maza, RedBorder

### **Internal identification**

Contract number: No 30-CE-0815229/00-33 implementing Framework contract No 30-CE-0677656/00-00

SMART number 2016/0077

### **DISCLAIMER**

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN number

doi:number

© European Union, 2014. All rights reserved. Certain parts are licensed under conditions to the EU.

Reproduction is authorised provided the source is acknowledged.



## CONTENTS

<b>ABSTRACT</b>	<b>1</b>
<b>EXECUTIVE SUMMARY</b>	<b>2</b>
<b>1. INTRODUCTION</b>	<b>8</b>
1.1 Structure and content of the report	8
1.2 About ENISA	9
1.2.1 ENISA's mission tasks and activities	9
1.2.2 ENISA's organisational structure	10
1.2.3 ENISA's stakeholders	11
1.2.4 Intervention logic	12
<b>2. METHODOLOGY</b>	<b>14</b>
2.1 Preparatory tasks	14
2.2 Data collection tasks	15
2.2.1 Desk research	15
2.2.2 Consulted stakeholders	15
2.3 Analytical tasks	17
2.4 Developing conclusions and recommendations	19
2.5 Challenges and limitations	19
<b>3. FINDINGS</b>	<b>21</b>
3.1 Key findings	22
3.2 Assessment of ENISA's performance, governance organisational structure and positioning	23
3.2.1 Relevance	23
3.2.2 Effectiveness	35
3.2.3 Efficiency	66
3.2.4 Coherence	79
3.2.5 EU-added value	92
3.3 Assessment of ENISA's strength, weaknesses, opportunities and threats	96
3.3.1 New needs for ENISA's constituency	97
3.3.2 The impact of new policy and regulatory landscape on ENISA's activities	103
3.3.3 Main strengths and weaknesses of ENISA	104
3.3.4 Format of ENISA's mandate	107
3.3.5 Concrete needs and opportunities for practical cooperation with Member States and EU bodies	108
3.3.6 Concrete needs and opportunities for practical cooperation with international bodies	109
3.3.7 ENISA's future mission, tasks, working practices or activities	110
3.3.8 Conclusions on ENISA's SWOTs	111
<b>4. CONCLUSIONS AND RECOMMENDATIONS</b>	<b>114</b>
4.1 Successes of ENISA	114
4.2 Most pressing issues at the strategic / policy level	115
4.3 Most pressing issues at the ENISA level	115
4.4 Options for the future	117
4.5 Costs of the options	127

## FIGURES

Figure 1: Strategic Objectives of ENISA .....	9
Figure 2: Organisational chart of ENISA (2013 to late 2016) .....	11
Figure 3: ENISA's stakeholder map .....	12
Figure 4: Intervention Logic of ENISA as an organisation.....	13
Figure 5: Methodology of the study .....	14
Figure 6: To what extent did ENISA cover CERTs/CSIRTs' needs over the 2013-2016 period? .....	28
Figure 7: Relevance of products/services to respondents' work/activities (n=62).....	32
Figure 8: Respondents willing to pay a fee to obtain additional products/services from ENISA over 2013-2016? (n=22).....	33
Figure 9: Overall assessment of ENISA for the period 2013-2016, (n=65)....	37
Figure 10: Extent to which ENISA has achieved its objectives over 2013-2016, (n=65).....	38
Figure 11: Extent to which ENISA covered CERTs/CSIRTs' needs over the 2013-2016 period .....	41
Figure 12: Importance of ENISA's capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) in 2013-2016 for CERTs/CSIRTs' development .....	42
Figure 13: Frequency of interact with ENISA or usage ENISA's products and services, (n=65).....	43
Figure 14: Reason for using ENISA's products/services, (n=63), multiple choice question.....	44
Figure 15: Extent to which ENISA's products/services over 2013-2016 responded to emerging needs of the cyber-security community in a timely manner, (n=62) .....	47
Figure 16: Extent of agreement or disagreement with the following statement on quality control mechanisms .....	48
Figure 17: Extent of agreement or disagreement with the following statement: To what extent do you agree/disagree with the following statement: The current governance structure, with a Management Board, an Executive Board and the PSG is conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives)? .....	49
Figure 18: Extent of agreement or disagreement with statement regarding ENISA's organisational solutions and procedures .....	50
Figure 19: Extent of agreement or disagreement with the following statement: ENISA's management practices are conducive to creating an effective organisation (i.e. in terms of meeting its objectives)? .....	51
Figure 20: Extent of agreement or disagreement with statement regarding ENISA's recruitment and training procedures .....	51
Figure 21 : Comparison of share of unfilled staff posts for a selection of EU agencies, 2014 and 2015.....	52
Figure 22: Compared share of staff positions filled on an annual basis for ENISA, FRA, and EMCDDA, 2014-2016.....	52
Figure 23: To what extent do you agree/disagree with the statements below regarding ENISA? .....	53
Figure 24: Average distribution over staff categories, 2014-2016.....	54
Figure 25: Percentage change in budget allocations for different staff categories, 2014-2016 .....	54
Figure 26: Extent of agreement or disagreement with statement regarding ENISA's staff composition .....	55
Figure 27: Nationality of staff members (2013-2015).....	55

Figure 28: Extent of agreement or disagreement with statement regarding ENISA's cooperation with stakeholders.....	56
Figure 29: Extent of agreement or disagreement with statement regarding ENISA's cooperation with stakeholders.....	57
Figure 30: Extent of agreement or disagreement with statement regarding ENISA's cooperation with stakeholders.....	57
Figure 31: Extent to which ENISA proactively supported cooperation among CERTs/CSIRTs during the 2013-2016 period .....	58
Figure 32: Extent of agreement or disagreement with the following statement: ENISA's location enables it to effectively conduct its work (i.e. in term of meetings its objectives).....	60
Figure 33: Extent to which ENISA's split location arrangement affected ENISA's ability to conduct its work effectively and efficiently, (n=65) .....	60
Figure 34: Extent of agreement or disagreement with statement regarding ENISA's internal management systems .....	62
Figure 35: Extent of agreement or disagreement with the following statement: The current governance structure with a Management Board, an Executive Board and the PSG is conducive to the efficiency functioning of the Agency (i.e. in terms of value for money) .....	67
Figure 36: Number of Management Board and Executive Board meetings per year for strategic decisions, 2014-2016 .....	68
Figure 37: Extent of agreement or disagreement with the following statement: ENISA's management practices are conducive to creating an efficient organisation (i.e. in terms of value for money)? .....	68
Figure 38: Extent of agreement or disagreement with the following statement on ENISA's working practices .....	69
Figure 39: Extent of agreement or disagreement with the following statement regarding ENISA's internal management systems .....	69
Figure 40: To what extent do you agree/disagree with the statements below regarding ENISA? .....	70
Figure 41: Staff recruitment expenditure compared to overall expenditure, 2015.....	71
Figure 42: Extent of agreement or disagreement with the following statement: ENISA's location enables it to conduct its work efficiently (i.e. in terms of value for money) .....	71
Figure 43: ENISA's budget 2013-2016 .....	73
Figure 44: Comparison of EU agencies based on staff and budget, 2017 .....	75
Figure 45: Distribution of commitment appropriations between staff, administrative and operational expenditure, 2015 .....	76
Figure 46: Staff distribution between operational and administrative staff for ENISA, FRA and EMCDDA, 2015.....	77
Figure 47: Adequacy of the size of the Agency for the work entrusted to it (n=65).....	77
Figure 48: Extent of agreement or disagreement with the following statement on the coherence of ENISA's activities .....	80
Figure 49: Extent to which ENISA's activities towards CERTs/CSIRTs were coherent with and complementary to (i.e. not overlapping or duplicating) what CERTs/CSIRTs were doing.....	82
Figure 50: Extent to which ENISA's activities are coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of respondent's organisation, (n=65) .....	84
Figure 51: Extent to which ENISA's activities are coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of its stakeholders, (n=65) .....	85
Figure 52: Positioning map.....	90

Figure 53: Most urgent needs or gaps in the cybersecurity field in the EU in the next ten years (multiple choice question) .....	98
Figure 54: Adequacy of current instruments & mechanisms at European level to promote and ensure cybersecurity .....	99
Figure 55: Top priorities for EU action from now on in the area of cybersecurity .....	100
Figure 56: Is there a role for an EU-level body in improving cybersecurity across the EU? .....	101
Figure 57: Gaps and needs for which ENISA is perceived to be most able to fulfil a role .....	101
Figure 58: Gaps and needs for which ENISA is perceived to be least able to fulfil a role .....	102
Figure 59: ENISA's main SWOTs .....	113

## TABLES

Table 1: Assessment of ENISA against the evaluation criteria .....	2
Table 2: ENISA's SWOTs .....	5
Table 3: Options for the future of ENISA .....	6
Table 4: Format and purpose of stakeholder consultation tools .....	15
Table 5: Stakeholders reached per data collection tool .....	16
Table 6: Analytical tasks and their purpose .....	17
Table 7: Organisations selected for the benchmarking .....	18
Table 8: Organisations covered under the positioning exercise .....	18
Table 9: Challenges in the evaluation process .....	19
Table 10: Key findings .....	22
Table 11: Evaluation questions covered under the relevance criterion .....	23
Table 12: Key current demands or needs according to the different types of stakeholders .....	30
Table 13: Evaluation questions covered under the effectiveness criterion .....	36
Table 14: Achieved outputs .....	37
Table 15: Overview of Article 14 requests .....	46
Table 16: Staff by category end of year .....	53
Table 17: Overview of ENISA's procurement (operations and non-operations) .....	63
Table 18: Evaluation questions covered under the efficiency criterion .....	66
Table 19: Annual costs for renting and maintaining two offices .....	72
Table 20: Costs for staff based in Heraklion .....	72
Table 21: Budget execution of EU subsidy .....	74
Table 22: Evaluation questions covered under the coherence criterion .....	80
Table 23: Evaluation questions covered under the EU added value criterion .....	92
Table 24: Evaluation questions covered under the assessment of ENISA's SWOTs .....	96
Table 25: Evaluation questions on the options for the future of ENISA .....	117
Table 26: Options for the future – the key issues they will address and expected results .....	117
Table 27: Cost estimations for the options – overview .....	128
Table 28: Cost estimations for the options – detailed including assumptions .....	131
Table 29: Evaluation questions matrix .....	1
Table 30: Overview of positioning analysis framework .....	2

## **APPENDICES**

### **Appendix 1**

Evaluation Question matrix

### **Appendix 2**

Bibliography

### **Appendix 3**

Survey questionnaires

### **Appendix 4**

Positioning exercise

### **Appendix 5**

Comprehensive SWOT table

## LIST OF ACRONYMS

Acronyms	
ANSSI	National Cybersecurity Agency
BEREC	Body of European Regulators for Electronic
BSI	German Federal Office for Information Security
CA	Contract agent
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Teams
CII	Critical information infrastructure
CIIP	Critical Information Infrastructure Protection
COD	Core Operations Department
cPPP	contractual public-private partnership
CSIRT	Computer Security Incident Response Teams
DAE	Digital Agenda for Europe
DG CNECT	DG Communications Networks, Content and Technology
DG DIGIT	DG for Informatics
DG JRC	Commission Joint Research Centre
EC3	European Cybercrime Centre
EDPS	European Data Protection Supervisor
EFCA	European Fisheries Control Agency
eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	European Union Agency for Network and Information Security
EQ	Evaluation question
ETSI	European Telecommunications Standards Institute
FIRST	Forum of Incident Response and Security Teams
FRA	European Union Agency for Fundamental Rights
FTE	Full-time equivalent
ICT	Information and communication technology
INCIBE	Spanish National Institute for Cybersecurity
IoT	Internet of Things
KII	Key impact indicator
KPI	Key performance indicator
MOOC	Massive Open Online Courses
NATO	North Atlantic Treaty Organisation
NCSC	Netherlands National Cyber Security Centre
NIS	Network and Information Security
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
NIST	US National Institute of Standards and Technology
NLO	Network of Liaison Officers
OASIS	Organisation for the Advancement of Structured Information Standards
PSG	Permanent Stakeholders' Group
QMS	Quality Management System
SESIAD	State for the Information Society and Digital Agenda
SMEs	Small and medium enterprises
SNE	Seconded national expert
SWOT	Strengths, weaknesses, opportunities and threats
TA	Temporary agent
UN/ITU	United Nations' International Telecommunication Unit

## ABSTRACT

The European Union Agency for Network and Information Security (ENISA) was established in 2004. The Agency provides advice and recommendations, data analysis, and supports awareness raising and cooperation by the EU bodies and Member States in the field of cybersecurity. ENISA uses its expertise to improve cooperation between Member States, and between actors from the public and private sectors, as well as to support capacity building.

The present study involves the evaluation of ENISA over the 2013-2016 period, assessing the Agency's performance, governance and organisational structure, and positioning with respect to other EU and national bodies. It assesses ENISA's strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It also provides options to modify the mandate of the Agency to better respond to new, emerging needs and assesses their financial implications.

The findings of the evaluation study show that ENISA has made some important achievements towards increasing NIS in the EU. However, a fragmented approach to cybersecurity across the EU and issues internal to the Agency, including limited financial resources, hinder ENISA's ability to respond to the ever growing needs of stakeholders in a context of technological developments and evolving cybersecurity threats.

## EXECUTIVE SUMMARY

This is the executive summary to the “Study on the Evaluation of the European Union Agency for Network and Information Security (ENISA)”.

### Objectives

ENISA is the EU agency for network and information security. It was established in 2004 by Regulation (EC) No 460/2004. Since then, ENISA’s mandate has been reviewed once and the Agency’s mandate has been extended several times. The latest changes were implemented with Regulation (EU) No 526/2013 (hereafter “the Regulation”). Article 32 (1) of the Regulation requires the Commission to “commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency and its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification”.

The study involves the evaluation of ENISA over the 2013-2016 period, assessing the Agency’s performance, governance and organisation structure, and positioning with respect to other EU and national bodies. Furthermore, the study assesses ENISA’s strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It provides options to modify the mandate of the Agency to better respond to the new needs and assesses their financial implications.

### Methodological approach

The evaluation study aims to assess the relevance, effectiveness, efficiency, coherence and complementarity, and EU added value of ENISA. It contains responses to 46 evaluation questions based on the European Commission’s Roadmap for the evaluation of ENISA<sup>1</sup>. The evaluation conclusions are drawn from both primary and secondary data collection and analytical tasks which feed into the development of the answers to the evaluation questions. The evaluation involved extensive data collection, including the consultation of various stakeholder groups (such as ENISA staff and management, ENISA’s Management Board, national Computer Emergency Response Teams and Computer Security Incident Response Teams (CERTs/CSIRTs), EU institutions, private stakeholders). Primary data was collected through different tools: in-depth interviews, two surveys, an open public consultation and a workshop. The evaluation is underpinned by an evaluation matrix, which links the evaluation questions to the data sources, indicators and analytical strategies that were used to answer them, thus making it clear how the conclusions have been reached.

The evaluation was carried out between November 2016 and July 2017 by Ramboll Management Consulting and CARSA, and involved three external experts covering the policy, legal and technical aspects of cybersecurity.

### Findings and conclusions

An assessment of ENISA’s performance, governance and operational structure and positioning for the period 2013-2016 according to the evaluation criteria is presented in the following table. The key findings that have led to this assessment are presented below.

**Table 1: Assessment of ENISA against the evaluation criteria**

Evaluation criterion	Overall assessment
<b>Relevance</b>	Achieved to a large extent
<b>Effectiveness</b>	Partially achieved
<b>Efficiency</b>	Achieved to a large extent
<b>Coherence</b>	Partially achieved
<b>EU-added value</b>	Partially achieved

<sup>1</sup> European Commission (2016): Evaluation Roadmap – Evaluation of the European Union Agency for Network and Information Security (ENISA)



**Relevance:** In the context of technological developments and evolving threats, there is a significant need for increased network and information security (NIS) in the EU. The recent additions to the legislative framework, such as the NIS Directive<sup>2</sup> underline this. Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. Considering this context, the objectives set out in ENISA’s mandate proved to be relevant over the period under evaluation and continue to be of high relevance today.

While the mandate defines the Agency’s objectives in broad terms, leaving room for ENISA’s Management Board to set priorities based on latest developments in order to respond to changing needs and evolving threats, ENISA’s activities do not fully meet the needs of all its stakeholders:

- ENISA’s work programme is dominated by the interests of the Member States, and yet it is necessary to consider the longer-term perspective and the activities of other stakeholders in the cybersecurity area (such as other EU agencies or the private sector) to ensure continued relevance of the Agency
- ENISA’s stakeholders strongly differ in their needs, making it difficult to meet them all. Some Member States (such as Germany, France or Sweden) have significant capacity and resources in the area of cybersecurity and rely on ENISA only for specific services. Other Member States (from Eastern and Southern Europe) are less experienced and rely more strongly on the expertise and capacity of ENISA. The Commission has their own needs and expectations with regard to the services that ENISA can provide to the different DGs. Additionally, industry stakeholders, including a high number of Small and Medium Enterprises (SMEs) are important actors in NIS and could also benefit from ENISA’s activities

**Effectiveness:** In general, ENISA implements its tasks and achieves its set targets. ENISA has made a contribution to increased NIS in Europe through the four tasks presented in the table below, though there is room for improvement in relation to each.

Community building		Capacity building	
Achievements	Areas for improvement	Achievements	Areas for improvement
✓ Important contribution to enhanced cooperation between Member States and related NIS stakeholders, in particular between CERTs/CSIRTs	- Cooperation could be strengthened between ENISA and the Commission and other EU agencies, and with the private sector	✓ Contribution to enhanced capacities in the Member States, most notably in Member States with limited capabilities and resources in the area of cybersecurity  ✓ Important activities include the Cyber Europe Exercises and trainings for CERTs/CSIRTs	- Capacity building with the private sector could be increased

<sup>2</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Expertise provision		Supporting development and implementation of policies	
Achievements	Areas for improvement	Achievements	Areas for improvement
<ul style="list-style-type: none"> <li>✓ Important contribution by supporting CERTs/CSIRTs</li> </ul>	<ul style="list-style-type: none"> <li>- ENISA has not managed to become recognised as a centre of expertise or a reference point for other stakeholders, such as EU institutions or the private sector</li> <li>- High reliance on procurement of external expertise and limited resources available in-house</li> </ul>	<ul style="list-style-type: none"> <li>✓ ENISA has assisted the Member States and the Commission in developing and implementing policies</li> </ul>	<ul style="list-style-type: none"> <li>- ENISA is not consistently being involved by the Commission in all NIS-related activities</li> </ul>

ENISA’s contribution to NIS in Europe is limited by several key factors, including:

- The broad mandate under which a variety of tasks is to be covered, leaving limited scope to work on its own initiative and other than upon request
- The Agency’s difficulties in attracting and retaining cybersecurity experts as staff members, due to various reasons including weak human resources procedures during the period under review
- The limited visibility of ENISA – the Agency is not sufficiently known across the EU and has not been able to establish a brand, unlike other EU agencies

**Efficiency:** ENISA has among the lowest budgets and levels of human resources compared to other EU agencies. In order to complete the various tasks set out in its mandate, ENISA has to be very efficient in the implementation of its budget and carefully consider where resources and working hours can be spent. The Agency develops a high number of publications every year and implements many other activities. Despite its small budget, the Agency has been able to contribute to targeted objectives and impacts, showing efficiency in the use of its budget.

In terms of efficiency, ENISA faces two main challenges:

- A number of administrative requirements set by the Commission which are the same for all EU agencies but weigh more heavily on smaller agencies
- A location split between Athens and Heraklion, requiring additional efforts of coordination and generating additional costs

**Coherence:** ENISA’s activities are generally coherent with the policies and activities of its stakeholders, but there is a need for a more coordinated approach to cybersecurity at EU level. The potential for cooperation between ENISA and the European Commission, as well as other EU bodies, is not fully utilised. For example, the division of responsibilities between ENISA and CERT-EU should be clarified.

ENISA’s activities are largely coherent with the work done at national level in the area of cybersecurity. Coherence is particularly strong between the CERTs/CSIRTs and ENISA. Some overlaps between ENISA’s activities and those of Member States with strong cybersecurity expertise were identified, but Member States with less capacity and resources in the area of cybersecurity still benefit from its activities.

**EU-added value:** ENISA’s added value lies primarily in the Agency’s ability to enhance cooperation, mainly between Member States but also with related NIS communities. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. The added value of ENISA differs between Member States, depending on their cybersecurity capacities and resources. The Agency’s activities of providing expertise and capacity building

represent important added value for Member States with few national resources dedicated to cybersecurity. This is less the case for Member States with more cybersecurity capacities.

Consequently, a discontinuation of ENISA would impact Member States differently. While Member States with strong cybersecurity capacities will be able to replace the services provided by ENISA at least to some extent, this will not be the case for Member States with fewer resources. The latter Member States rely more on ENISA’s services in terms of capacity building, access to expertise and support in the implementation of policy and legislation. Cybersecurity crosses borders, so there is a need to build capacity to avoid weaker links that can impact on cybersecurity in the EU as a whole, as well as a need to provide a cross-EU response. It will not be possible to ensure the same degree of community building and cooperation across the Member States without a decentralised EU agency for cybersecurity; the picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA. Therefore, coordination at EU level is needed.

A potential discontinuation of ENISA would be a lost opportunity for all Member States. Most stakeholders were of the opinion that ENISA could take on a more important role in the EU cybersecurity landscape in the future, ensuring a common response capacity. This potential for the Agency to capitalise on future opportunities would be lost should it be discontinued.

**SWOT analysis:** Based on an analysis of the context – namely the evolution, since the last revision of ENISA's mandate in 2013, of the cybersecurity and digital privacy landscape - the evaluation study provides an assessment of the main strengths and weaknesses of ENISA, and the opportunities and threats in the new cybersecurity and digital privacy landscape. These are presented in the figure below.

**Table 2: ENISA’s SWOTs**

<p><b>Strengths</b></p> <ul style="list-style-type: none"> <li>- Neutral, facilitator, free of political bias or commercial interests</li> <li>- Recognised support to Member States in capacity building &amp; capability development to strengthen resilience to cyber-threats</li> <li>- Acknowledged collaboration &amp; community building reaching wide range of actors, incl. Member States, industry, EU bodies etc.</li> <li>- Horizontal expertise, “landscape overview” of Member States cybersecurity policies</li> </ul>	<p><b>Weaknesses</b></p> <ul style="list-style-type: none"> <li>- Low visibility for various reasons: lack of expertise, weak communication/marketing and limited self-assertion within the EU cybersecurity policy landscape</li> <li>- Lack of a long-term, strategic vision</li> <li>- Recruitment difficulties</li> <li>- Reduced efficiency due to split location</li> <li>- Distance to EU decision makers in Brussels</li> <li>- Lack of financial and human resources to make a difference</li> </ul>
<p><b>Opportunities</b></p> <ul style="list-style-type: none"> <li>- Growing need for synergies between information and communication technology (ICT) operators to ensure concerted and collaborative NIS policy actions</li> <li>- NIS Directive bears the potential to strengthen ENISA’s role in EU cybersecurity policy</li> <li>- There is an acknowledged need and demand of stakeholders to strengthen awareness raising of cybersecurity</li> <li>- Stronger support in the community is evolving for ICT standardisation and certification</li> </ul>	<p><b>Threats</b></p> <ul style="list-style-type: none"> <li>- Policy fragmentation at EU level and diverging policy priorities in EU Member States constrain ENISA’s scope of action</li> <li>- Rapidly evolving and complex threat landscape involving multiple disciplines create new vulnerabilities, e.g. Internet of Things (IoT)</li> <li>- Lack of overall (technical) talent in the field of cybersecurity aggravates ENISA’s recruitment difficulties</li> </ul>

In conclusion, the following **key issues** have been identified as requiring action to improve ENISA’s relevance, effectiveness, efficiency, coherence and added value in the future and ultimately help it contribute to increased NIS in the EU: Weak institutional and legal framework for cybersecurity in the EU – Cybersecurity is primarily seen as an area of national competence, while in reality it is an issue that transcends borders

- *Fragmentation of cybersecurity policy at EU level* – The fragmentation of cybersecurity policy is due to a number of EU-level actors in the area of cybersecurity and insufficient coordination

between them. One important factor here is the division of responsibilities between ENISA and CERT-EU.

- *Limitations for ENISA due to its size* – ENISA has difficulties to make an impact in the vast field of NIS as it has only limited human and financial resources to meet a broad mandate.
- *Limited visibility* – ENISA has not managed to develop a strong brand name and is not seen as a point of reference at European level for cybersecurity.
- *Not perceived as a proactive, visionary Agency* - ENISA's broad mandate makes it reactive to fulfilling the needs of as many stakeholders as possible, but this means that it loses focus. ENISA is not able to use its own knowledge to set work priorities due to the Member State dominance of the work programme.
- *A mandate that is not aligned with cybersecurity needs* – Cybersecurity threats have become a permanent issue in the EU and ENISA has been allocated long-term responsibilities (e.g. under the NIS Directive) which call for a permanent mandate.
- *ENISA does not sufficiently respond to the needs of all its stakeholders* – Under the current governance structure, the needs of the private sector are not sufficiently heard and thus are not adequately reflected in the Agency's work programmes.
- *ENISA should expand its activities to better respond to stakeholder needs* – There is a request by stakeholders (although not unanimous) to ensure a coherent ICT certification and standardisation system in the EU. Member States with fewer resources and expertise require additional support in receiving information on and assessing cybersecurity threats in order to respond to attacks.

Despite these issues, there is significant potential for ENISA, if sufficiently mandated and supported in terms of financial and human resources, to make a contribution to increased NIS in the EU. There is a clear need for cooperation and coordination across different stakeholders and ENISA as a decentralised EU agency is in the position to ensure a coordinated approach to cyber threats in the EU.

### Options for the future of the Agency

Based on the key issues presented above – as derived from the findings and conclusions of the study - four options to review the current mandate of ENISA were developed. They are presented in Table 3 below, highlighting the specific factors for change that could be implemented under each of the options.

**Table 3: Options for the future of ENISA**

Option	Factor for change
<p><b>Option 0: Baseline, maintain the status quo</b></p> <p>This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation<sup>3</sup> and Telecoms Framework Directive<sup>4</sup> would need to be taken into account.</p>	<p><b>Revise ENISA's mandate to make its new tasks as per recent/upcoming legislation more specific:</b></p> <ul style="list-style-type: none"> <li>• Involvement in Cooperation Group as required under the NIS Directive</li> <li>• CSIRT Network Secretariat</li> <li>• Electronic communication code, recital 92 (Telecoms Framework Directive)</li> <li>• eIDAS</li> </ul>
<p><b>Option 1: Expiry of ENISA's mandate (terminating ENISA)</b></p> <p>This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive</p>	N/A

<sup>3</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

<sup>4</sup> Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

<p>and bilateral or regional ties at Member State level.</p>	
<p><b>Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate)</b></p> <p>This option concerns making significant revisions to ENISA’s mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.</p>	<p><b>Strengthen ENISA’s operational role:</b></p> <ul style="list-style-type: none"> <li>• Provide periodic threat intelligence and ad hoc alerts</li> <li>• Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level</li> <li>• Provide emergency cybersecurity response</li> </ul> <p><b>Strengthen ENISA’s role in policy development and implementation:</b></p> <ul style="list-style-type: none"> <li>• Render the consultation of ENISA by the Commission in cybersecurity matters obligatory</li> <li>• Formally involve ENISA in the Connecting Europe Facility</li> <li>• Establish regular meetings between ENISA and other agencies/international organisations</li> </ul> <p><b>Make ENISA’s mandate permanent</b></p> <p><b>Strengthen ENISA’s governance structure:</b></p> <ul style="list-style-type: none"> <li>• Increase the role of the Permanent Stakeholders’ Group (PSG)</li> <li>• Allow ENISA more flexibility in the determination of its work priorities</li> </ul> <p><b>Include a role for ENISA in EU-level standardisation and certification:</b></p> <ul style="list-style-type: none"> <li>• Support the EU ICT Security Certification Framework</li> <li>• Support ICT security standardisation</li> </ul> <p><b>Strengthen ENISA’s position relative to research and innovation:</b></p> <ul style="list-style-type: none"> <li>• Take part in programming implementation</li> <li>• OR Take part in programming in an advisory role</li> <li>• OR Benefit from EU research and development funding</li> </ul> <p><b>Increase ENISA’s visibility:</b></p> <ul style="list-style-type: none"> <li>• Establish a liaison office in Brussels</li> <li>• Create a dedicated communications team within ENISA</li> </ul>
<p><b>Option 3: European Agency with full operational capabilities (Establish a European Centre of Cybersecurity)</b></p> <p>This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.</p>	<p><b>Create an EU cybersecurity umbrella:</b></p> <ul style="list-style-type: none"> <li>• Such an umbrella would encompass ENISA and CERT-EU</li> </ul> <p><b>Create a virtual European CSIRT:</b></p> <ul style="list-style-type: none"> <li>• Coordinate CSIRT Network operations</li> <li>• Produce real time situational awareness and dynamic threat intelligence feeds</li> <li>• Maintain and provide own cybersecurity incident response capacity to public and private sector</li> </ul> <p>All factors related to Option 2 could be fulfilled under Option 3.</p>

# 1. INTRODUCTION

This is the final report for the “Study on the Evaluation of the European Union Agency for Network and Information Security (ENISA)”. The study was implemented between November 2016 and July 2017.

The study aims to support the Commission in evaluating the impact, effectiveness, efficiency, relevance, coherence and value added of ENISA and its working practices, and prepare the ground for a possible revision of the mandate of the Agency. The Commission is evaluating ENISA based on Article 32 (1) of ENISA’s Regulation (Regulation No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004) which requires the Commission to “commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency and its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification.”

As such, the study contains both a summative dimension, looking back at the achievements of the 2013-2016 period, as well as a more formative, forward-looking aspect, as further described below:

- Summative dimension: This aspect of the study assesses the results achieved by the Agency having regard to its objectives, mandate and tasks as set out in the ENISA Regulation.
- Formative dimension: This forward-looking assessment is based on the evaluation of the current positioning of ENISA with respect to other EU and national bodies in meeting the needs of its constituency and the new challenges engendered by the evolving cybersecurity and digital privacy landscape. The study provides recommendations on the possible need to modify the mandate of the Agency and assesses the financial implications of such modifications.

This introductory section presents the structure and content of this report and provides a brief overview about ENISA and the Agency’s work, including its intervention logic.

## 1.1 Structure and content of the report

This report is structured in four main parts. The introduction is followed by information about the methodology applied to implement the study. The third part of the report presents the findings of the study, which are structured according to the evaluation criteria, i.e. relevance, effectiveness, efficiency, coherence and EU-added value, and concludes with an analysis of ENISA’s strength, weaknesses, opportunities and threats, a so-called SWOT analysis. The fourth and final part of the study presents conclusions on ENISA’s key achievements and the most pressing issues at strategic level and at the level of the Agency, before going on to discuss potential options for the future. The specific factors for change of the options are discussed, including an assessment of the costs of their implementation, their added value and coherence.

Part	Heading
1	Introduction
2	Methodology
3	Findings
4	Conclusions and recommendations

The report includes the following appendices:

Appendix	Heading
1	Evaluation question matrix
2	Bibliography
3	Survey questionnaires
4	Positioning exercise
5	Comprehensive SWOT table

## 1.2 About ENISA

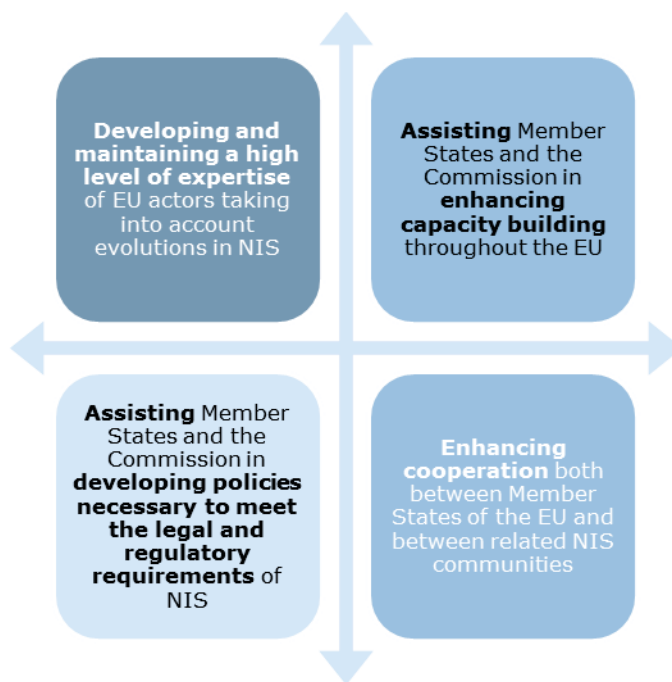
ENISA is the EU agency for network and information security. It was established in 2004 by Regulation (EC) No 460/2004. Since then, ENISA's mandate has been reviewed once and extended several times. The latest changes were implemented with Regulation (EU) No 526/2013 (hereafter "the Regulation"). The Agency is located in Greece with its seat in Heraklion on Crete and an operational office in Athens.

### 1.2.1 ENISA's mission tasks and activities

The Agency's activities consist in providing advice and recommendations, data analysis, as well as supporting awareness raising and cooperation by the EU bodies and Member States. Building on national and Community efforts, the Agency is a centre of expertise in this field. ENISA uses its expertise to improve cooperation between Member States, and between actions from the public and private sectors, as well as to support capacity building.

ENISA's Strategic Objectives (from 2015<sup>5</sup>) are presented in the figure below.

**Figure 1: Strategic Objectives of ENISA**



Source: Ramboll Management Consulting based on ENISA website

In order to achieve its Strategic Objectives, ENISA delivers four key tasks in accordance with the Regulation, namely:

- ✓ Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- ✓ Collecting and analysing data on security incidents in Europe and emerging risks.
- ✓ Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.

<sup>5</sup> There was a shift from work streams to strategic objectives in 2015.

- ✓ Raising awareness and strengthening co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field.

In addition, ENISA undertakes European Network and Information Security (NIS) Good Practice Brokerage activities, which are based on the concept of the exchange of good practices between EU Member States at the area of NIS on a pan-European scale. ENISA acts as a broker in the European NIS 'marketplace' to facilitate the exchange of good practices by:

- supporting co-operative meetings with Member States and other stakeholders;
- assisting in the exchange of experts between Member States;
- supporting the exchange of good practice material;
- contributing with its expertise to co-operative projects.

ENISA mainly conducts the previously mentioned tasks through four activity areas: Computer Emergency Response Teams/ Computer Security Incident Response Teams (CERTs/CSIRTs), Critical Information Infrastructure Protection (CIIP) and Resilience, Identity & Trust and Risk Management.

### 1.2.2 ENISA's organisational structure

The organisational structure of ENISA is laid down in the Regulation which states that the Agency comprises an Executive Director and staff, a Management Board, an Executive Board and a Permanent Stakeholders' Group (PSG). Each of these is described in further detail below.

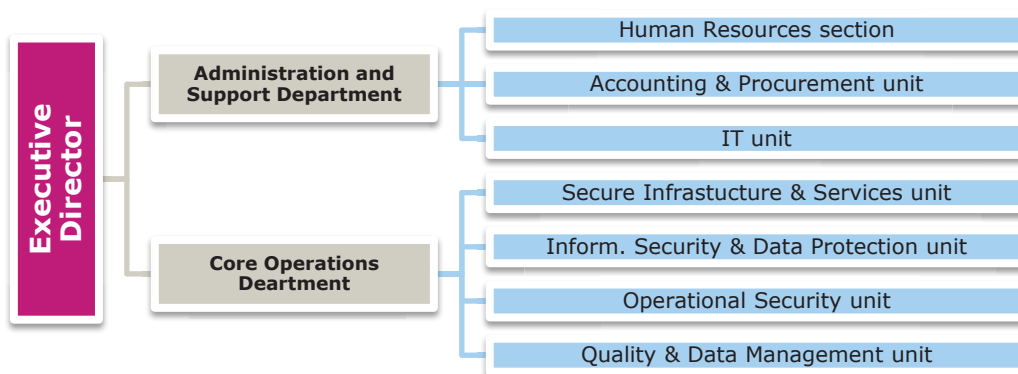
**The Executive Director** is appointed by the Management Board and is responsible for managing the Agency and performs his/her duties independently. He/she also establishes **ad hoc working groups**, in consultation with the PSG, which are composed of experts. The ad hoc working groups are addressing specific technical and scientific matters.

**The Management Board** is composed of representatives of the Member States and the Commission. Tasks of the Management Board include the establishment of the budget, verification of its execution, adoption of the appropriate financial rules, establishment of transparent working procedures for decision-making by the Agency, approval of the Agency's work programme, adoption of its own rules of procedure and Agency's internal rules of operation, appointment and removal of Executive Director. The Management Board will adopt the Agency's internal rules of operation on the basis of a proposal by the Commission. The Management Board ensures that the Agency carries out its tasks under conditions which enable it to serve in accordance with the founding Regulation

**The PSG** is set up by the Management Board, acting on a proposal by the Executive Director, for a term of office of 2.5 years. For the period 2015-2017, the PSG is composed of "nominated members" and of members appointed "ad personam", representing in total 23 members from all over Europe. The 20 members appointed "ad personam" constitute a multidisciplinary group from industry, academia, and consumer organisations and have been selected upon the basis of their own specific expertise and personal merits. Three "nominated members" represent national regulatory authorities, data protection and law enforcement authorities. The role of PSG is to advise the Executive Director on the development of the Agency's work programme, and on ensuring the communication with the relevant stakeholders on all related issues.

In line with the operational and horizontal objectives of the Agency, ENISA's organisational structure was reorganised in December 2013, as depicted in the figure below.



**Figure 2: Organisational chart of ENISA (2013 to late 2016)**

Source: ENISA website, *Structure and Organisation*

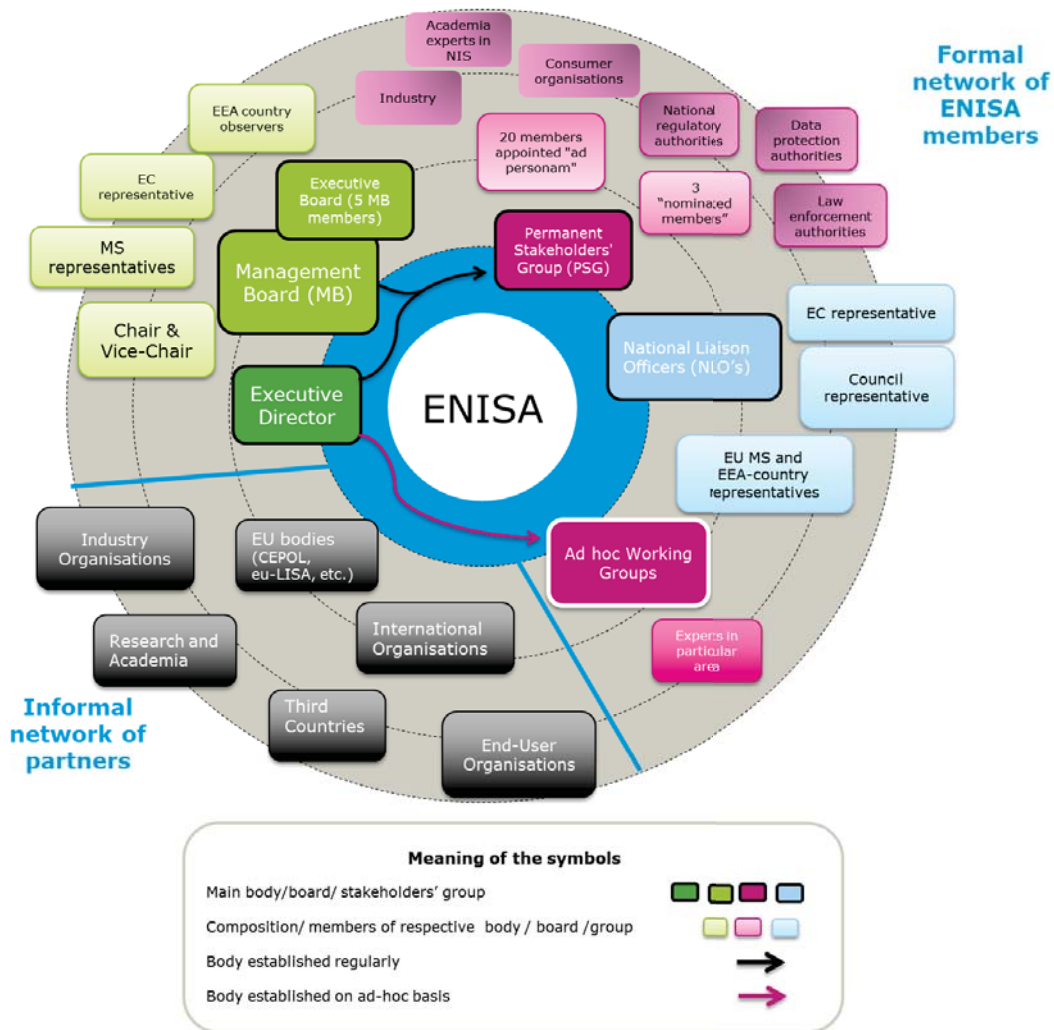
ENISA's organisational structure was changed in late 2016 to include an "Executive Director's Office" and the units within the core operations and administrative departments were reorganised; the split between operations and administration (which from end 2016 also covers "stakeholder relations") was maintained. The previous structure of ENISA has been presented here in line with the scope of this evaluation (2013-2016).

### 1.2.3 ENISA's stakeholders

Engaging with, working with and assisting its stakeholders, is a key factor for ENISA's success and the overall mission of contributing to the security of the EU internal market. Therefore maintaining relationships with these stakeholders through formal and informal channels is one of the main tasks of ENISA. ENISA has importantly set up and continues to maintain a formal group of liaison officers, called **the Network of National Liaison Officers (NLOs)**. This network should be highlighted since, though not formally based on the ENISA Regulation, it is of great value to ENISA as the NLOs serve as ENISA's key points of reference in the Member States on specific issues. ENISA also gains access to a network of national contacts through individual NLOs, reinforcing the activity of the Agency in the Member States and its network consists of (at least) one NLO per Member State. Typically an NLO works in the field of NIS, either in the public sector (ministry), or the IT/telecom sector. In coordination with the Managing Board representative, it may be decided to appoint multiple NLOs for one country – particularly when the country is large or when there are multiple distinct communities (private, public, etc.).

In addition, ENISA has established relations with a wider stakeholder group. These include industry organisations, end user organisations, EU bodies, International Organisations, research and academia, third countries, etc. This open and growing network of stakeholders is essential to the Agency's goals in identifying emerging risks and forging new insights to help Member States and private sector organisations through access to NIS experts. Figure 3 shows a map of ENISA's stakeholders who together strengthen to Agency's capacity to prepare for challenges in a proactive and increasingly professional manner by building novel public and private sector partnerships.

Figure 3: ENISA’s stakeholder map



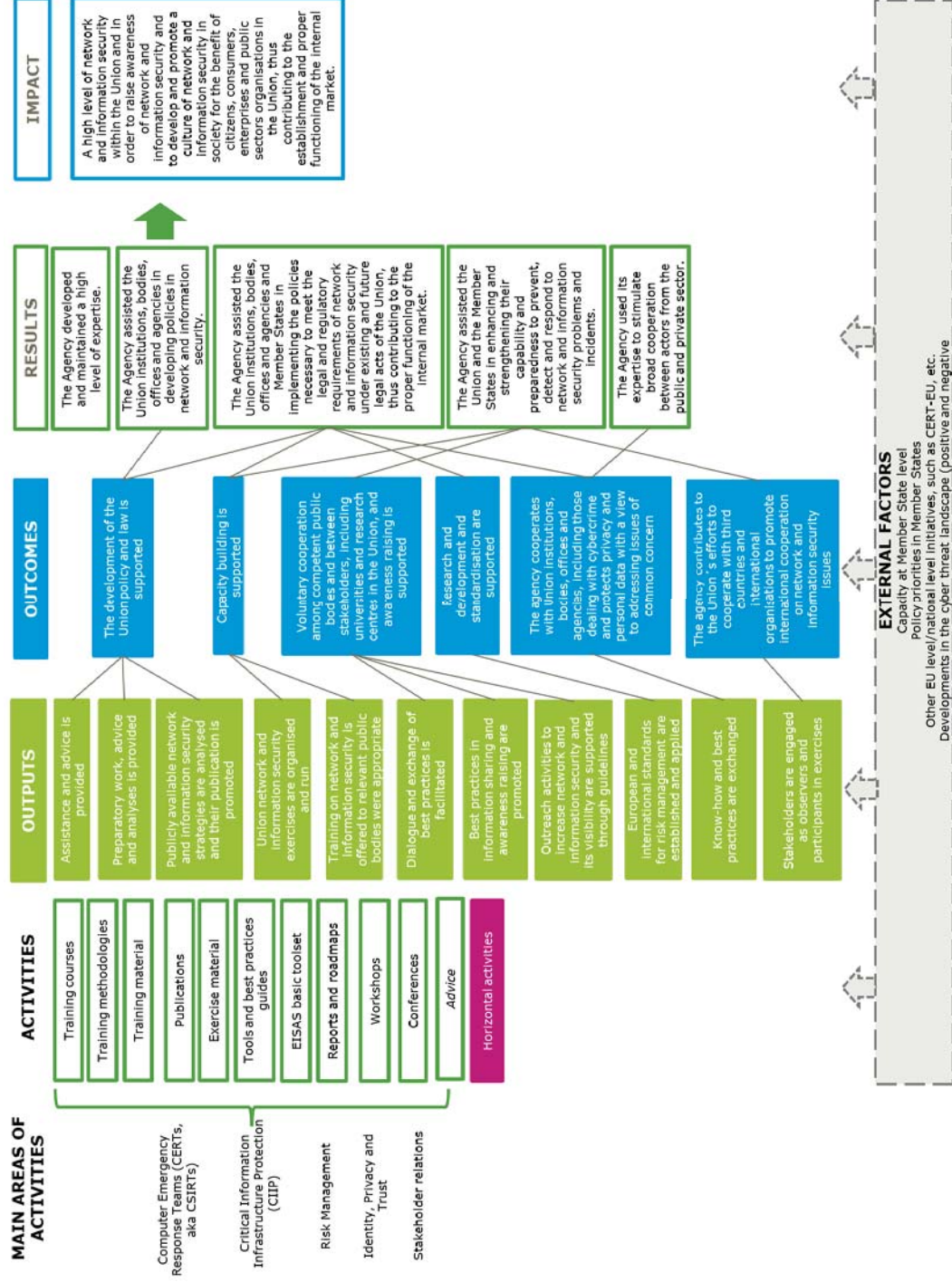
Source: Ramboll Management Consulting based on ENISA website, *Structure and Organisation, Stakeholders Relations*

1.2.4 Intervention logic

The figure below presents the intervention logic for ENISA as an organisation based on the Regulation, which shows how its four key areas of activity are intended to deliver the Agency’s Strategic Objectives and impacts. This intervention logic is a systematic and reasoned description of the casual links between the Agency’s activities, outputs, outcomes, results and impacts, as well as the key external factors affecting the implementation, results and impact of ENISA’s activities. It helps to understand the objectives of the Agency as a whole and its specific tasks.

This study has used the intervention logic as a basis to assess ENISA’s effectiveness in achieving targeted results and impacts based on the implemented activities.

Figure 4: Intervention Logic of ENISA as an organisation



Source: Ramboll Management Consulting based on Regulation (EU) No 526/2013

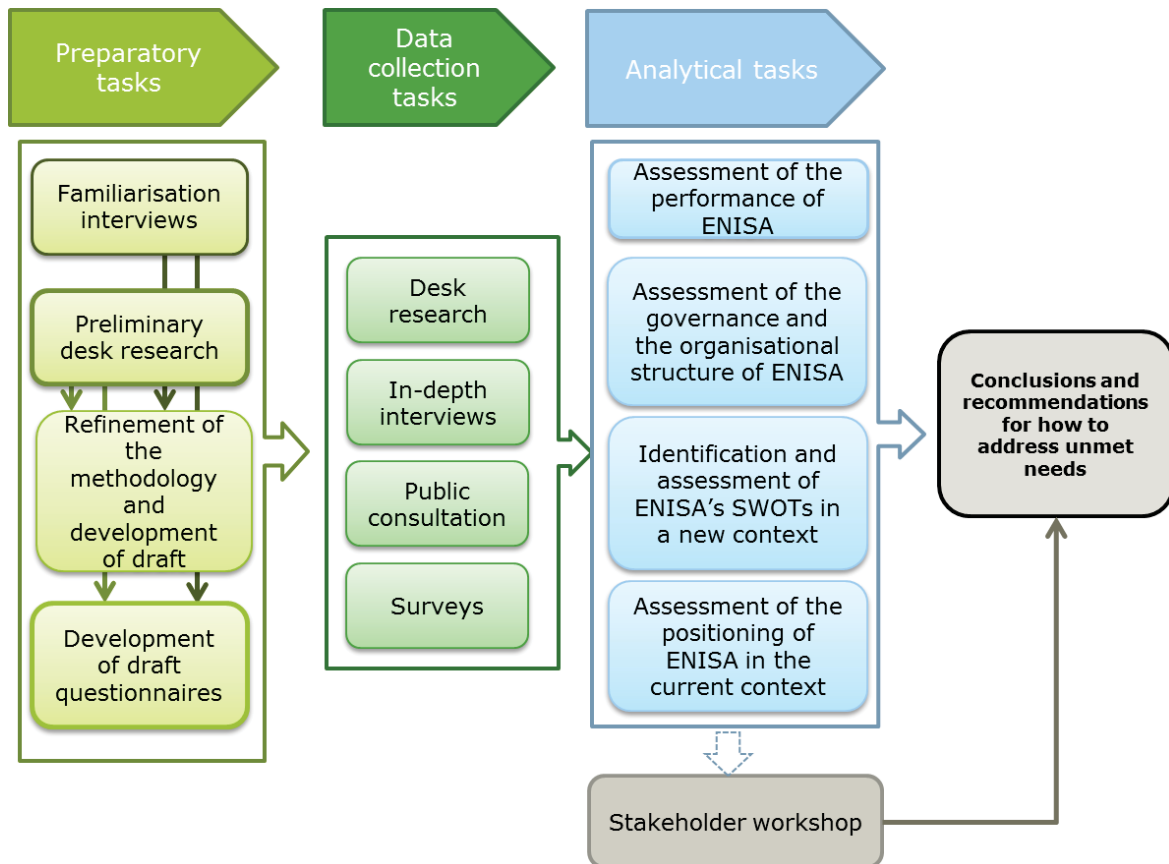
## 2. METHODOLOGY

The purpose of the evaluation study was to support the Commission in evaluating the impact, effectiveness, efficiency, relevance, coherence and value added of ENISA and its working practices, and prepare the ground for a possible revision of the mandate of the Agency. To do so, four different analytical tasks were implemented. As part of the summative (backward-looking) part of the study, the performance of ENISA (i) and its governance and organisational structure (ii) were assessed, and ENISA’s positioning with regard to other EU agencies and bodies and national authorities was also analysed (iii). As part of the formative (forward-looking) dimension of the study, ENISA’s SWOTs in a new context have been identified.

This part of the study presents an overview of the methodology employed for the evaluation of ENISA, by detailing the data collection activities and analytical tasks that have been implemented. The study answers a set of 46 evaluation questions based on the Commission’s evaluation roadmap for ENISA<sup>6</sup>. A complete evaluation question matrix is presented in Appendix 1.

The methods chosen to evaluate ENISA in accordance with the requirements of this study and to respond to the evaluation questions are presented in Figure 5 below.

**Figure 5: Methodology of the study**



Each of the tasks is described in further detail below.

### 2.1 Preparatory tasks

The preparatory tasks were used to set up the methodology and tools for the study and ensure a common understanding of the scope and objective of the evaluation between the European

<sup>6</sup> European Commission (2016): Evaluation Roadmap – Evaluation of the European Union Agency for Network and Information Security (ENISA)

Commission and the study team. For this purpose, five **familiarisation interviews** were conducted with members of the European Commission DG Communications Networks, Content and Technology (DG CNECT) and DG for Informatics (DIGIT), and with the Computer Emergency Response Team for the EU institutions, CERT-EU. **Preliminary desk research** allowed for the identification of the policy, legal and academic documents of relevance to the study. Based on the understanding gained of ENISA and the purpose of the evaluation, the **methodological approach was refined**, including a finalisation of the evaluation question matrix and **data collection tools were developed**.

## 2.2 Data collection tasks

The data collection included a desk review of relevant literature and the consultation of different stakeholders. In-depths interviews with a wide range of ENISA's stakeholders, staff and management were conducted, surveys specifically targeted at ENISA's staff and management and at CERTs/CSIRTs were implemented, and an open public consultation allowed all EU citizens and organisations to contribute to the study. At the end of the data collection and after some analysis, a workshop was held with ENISA's stakeholders in order to validate the findings and preliminary conclusions. Through these various means, a wide range of stakeholders were consulted, ensuring the representativeness of the findings presented in chapter 3.

### 2.2.1 Desk research

The study is based on a variety of secondary sources which fed into all of the analytical tasks. These sources include legal sources on relevant EU legislation, EU strategies and policy documents, reports published by ENISA on programming and reporting, previous evaluations conducted for the Agency and a number of key papers and reports on the issue of cybersecurity in Europe.

A full list of documents is provided in Appendix 2.

### 2.2.2 Consulted stakeholders

The data collection among stakeholders included the following activities: in-depth interviews, an open public consultation, a survey among ENISA's staff and management as well as direct stakeholders (members of the Management and Executive Board of the Agency, NLOs and the PSG), a survey among CERTs/CSIRTs and a stakeholder workshop. Table 4 below presents an overview of the different formats used to involve stakeholders in the study.

**Table 4: Format and purpose of stakeholder consultation tools**

Consultation tool	Format	Purpose
<b>Interviews (49 interviews conducted)</b>	In-depth interviews over the phone or in person	<ul style="list-style-type: none"> <li>Gather information on ENISA's performance (ENISA's staff and management, its direct stakeholders and the European Commission and Parliament)</li> <li>Collect data on ENISA's governance structure (staff and management, direct stakeholders)</li> <li>Gather views on ENISA's SWOTs (all stakeholders)</li> <li>Collect information to understand ENISA's positioning (other EU agencies and bodies)</li> </ul>
<b>Survey to ENISA staff and direct stakeholders (88 participants)</b>	Online survey to ENISA's staff, the Management and Executive Board of the Agency, NLOs and the PSG. Current, as well as former, Management Board members and NLOs were contacted. A total of 199 stakeholders were invited to participate.	<ul style="list-style-type: none"> <li>Gathering views on the effectiveness and efficiency of ENISA's governance, organisational set-up and working practices</li> </ul>
<b>Survey to CERTs/CSIRTs (34 participants)</b>	Online survey sent out to CSIRT Network, including CSIRT representatives from all 28 Member States and CERT-	<ul style="list-style-type: none"> <li>Gathering views on cooperation and coordination between ENISA and the CERTs/CSIRTs</li> <li>Providing input to assess the coherence and complementarity between ENISA's activities and those</li> </ul>

	EU.	of the CERTs/CSIRTs
<b>Open public consultation (90 participants)</b>	Questionnaire available online between 18 January and 12 April 2017	<ul style="list-style-type: none"> <li>Contribution to the assessment of ENISA's performance, the analysis of SWOTs, and to the development of recommendations for the future</li> </ul>
<b>Workshop (43 participants)</b>	Implemented following the analytical tasks. Held on the premises of the Commission in Brussels on the 22nd of March 2017. Presentation of preliminary findings, conclusions and options.	<ul style="list-style-type: none"> <li>Gathering participants' views on the results of the evaluation and to discuss possible options for the future of cybersecurity in Europe</li> <li>Validation of findings</li> </ul>

Through the different data collection tools more than 300 stakeholder contributions were received from across various groups as presented in Table 5 below (individual stakeholders may have contributed to the evaluation through different data collection tools).

**Table 5: Stakeholders reached per data collection tool**

Target group	Type of stakeholder	Number of interviewees	Number of survey respondents	Number of participants to the Open public consultation	Number of workshop participants <sup>7</sup>
<b>Direct stakeholders</b>	Members of ENISA's Management Board and Executive Board	8	19	10	12
	PSG	2	13	3	5
	NLOs	2	12	1	
<b>ENISA's users and advisors</b>	European Commission	6			
	European Parliament	3			
	Other EU agencies and bodies	5			4
	CERTs/CSIRTs	3	34		2
	National cybersecurity authorities	1		9 <sup>8</sup>	5
	Industry representatives (private enterprises or business associations)	4		26 <sup>9</sup>	9
	Civil society organisations or individuals	2		26 <sup>10</sup>	2
	Research or academic institutions			10	2
	Consultants			5	
	Authorities from third countries	1			
<b>ENISA staff and management</b>		12	44		2
<b>Total</b>		<b>49</b>	<b>122</b>	<b>90</b>	<b>43</b>

Across the data collection tools (interviews, open public consultation, workshop), Management Board members of at least 19 Member States were involved in the study.<sup>11</sup> These cover a spectrum of smaller and larger Member States and of different regions.

In addition to the data collection tools presented in the tables above, seven interviews were conducted with national authorities and policy-makers in the latter stage of the evaluation, focussing on the forward looking part of the study and seeking to further operationalise the options under consideration for the future of the Agency. These include Member State representatives and their alternates to ENISA's Management Board, members of ENISA's Executive Board,

<sup>7</sup> Participants from the Commission have not been included in the list of participants and are thus not included below.

<sup>8</sup> Including a position paper received from France

<sup>9</sup> Including one position paper from a UK based business association

<sup>10</sup> This includes 20 respondents who indicated to answer in their personal capacity.

<sup>11</sup> The contributions to the surveys were anonymous. It cannot be verified which Member States were covered.

CERTs/CSIRTs and national cyber security authorities, as well as management staff from ENISA, representatives of DG CNECT and from the private sector.

Further information on the data collection methods can be found in Appendix 3 including the questionnaires used to the two surveys.

### 2.3 Analytical tasks

The study involved four analytical tasks which were used to reach conclusions and recommendations for the revision of ENISA’s mandate and to suggest potential improvements, as presented in Table 6.

**Table 6: Analytical tasks and their purpose**

Analytical task	Purpose
<b>Assessment of ENISA’s performance</b>	<ul style="list-style-type: none"> <li>• Assessment of effectiveness, efficiency, relevance, coherence and EU added value of the work undertaken by ENISA and its working practices over the 2013-2016 period</li> <li>• Review of ENISA’s intervention logic to establish the extent to which ENISA’s activities and outputs have contributed to the expected results and impacts</li> <li>• Assessment of whether ENISA has been able to establish itself as an EU-wide centre of expertise and reference point for stakeholders</li> <li>• Assessment of the degree to which the Agency’s priorities, as set out in its work programmes, are in line with the needs of the time and the degree of the Agency’s flexibility to respond to unforeseen needs</li> </ul>
<b>Assessment of the governance and organisational structure of ENISA</b>	<ul style="list-style-type: none"> <li>• Assessment of how the current, governance, internal organisational structure of ENISA, location and human resources policies and practices contribute to efficiency in and effectiveness of the work of the Agency</li> <li>• Benchmarking exercise comparing ENISA’s governance and organisational structure to that of other EU agencies and organisations</li> </ul>
<b>Assessment of the positioning of ENISA in the current context</b>	<ul style="list-style-type: none"> <li>• Assessment of how ENISA is positioned vis-à-vis a sample of other EU and national bodies working on cybersecurity and digital privacy on the basis of the services offered and the needs expressed by the Agency’s stakeholders</li> <li>• Mapping of the services provided by ENISA and of a selection of other EU and national bodies against identified needs to highlight existing complementarities and potential overlaps between the offered services</li> <li>• Development of a positioning map</li> </ul>
<b>Identification and assessment of ENISA’s SWOTs in a new context</b>	<ul style="list-style-type: none"> <li>• Identification and assessment of ENISA’s strengths, weaknesses, opportunities and threats (i.e. current status / position) in the context of the new and evolving cybersecurity challenges and digital privacy landscape and ENISA’s current mandate</li> <li>• .</li> <li>• Based on all data collection tasks and builds on the analysis conducted as part of the other analytical tasks</li> <li>• Involvement of a panel of cybersecurity experts covering the policy, legal and technical aspects of the area in this task</li> </ul>

The analytical tasks included a benchmarking and a positioning exercise. The sample of EU agencies and bodies selected for these two exercises is presented below.

The EU agencies and bodies covered under the **benchmarking exercise** are presented in Table 7 below. Organisations were selected based on similarities in their work areas and activities with those of ENISA, or in their size to ENISA in terms of number of staff and budget.

**Table 7: Organisations selected for the benchmarking**

Organisation	Reason for selection
<b>Europol – European Cybercrime Centre (EC3)</b>	Similarities in the work areas and activities
<b>European Union Agency for Fundamental Rights (FRA)</b>	Availability of data
<b>Office of the Body of European Regulators for Electronic (BEREC office)</b>	Similarities in the work areas and activities
<b>European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)</b>	Similarity in the activities
<b>European Union Agency for Law Enforcement Training (CEPOL)</b>	Similarity in the activities and similarity in terms of staff number and budget
<b>European Fisheries Control Agency (EFCA)</b>	Similarity in terms of staff number and budget

For the positioning exercise, ENISA's activities were mapped across four tasks: enhancing cooperation, develop and maintain a high level of expertise, enhancing capacity building and developing and implementing policies. Sub-categories of these were developed to understand the more specific tasks that were implemented. The complete mapping of ENISA's services and the full positioning exercise is attached in Appendix 4. The services were then compared to the sample of other EU and national bodies presented in Table 8 below. These organisations were contacted to provide information on their activities. The completeness of the responses received from these organisations varied and in a few cases no responses were received despite numerous follow ups per email and over the phone. As a consequence, parts of the positioning exercise only rely on desk research.

**Table 8: Organisations covered under the positioning exercise**

Organisation	Status
<b>CERT-EU</b>	Input received
<b>Commission Joint Research Centre (DG JRC) Science Hub</b>	Input received
<b>EC3</b>	Assessment made based on desk review
<b>Netherlands National Cyber Security Centre (NCSC)</b>	Input received with no assessments of overlaps or complementarity
<b>French National Cybersecurity Agency (ANSSI)</b>	Assessment made based on desk review
<b>Spanish National Institute for Cybersecurity (INCIBE)</b>	Input received with no assessments of overlaps or complementarity

The aim of the **positioning exercise** was to compare ENISA to organisations implementing similar activities in order to assess ENISA's coherence and identify any potential overlap. Therefore, EU bodies and agencies, and organisations from Member States where the expected potential for overlap was high were selected. Results from the annual evaluations of ENISA in 2014 and 2015 showed that this was the case for Member States' cybersecurity organisation with comparably high human and financial resources and experience in the field of cybersecurity. The selected national organisations were not intended to be representative of all Member States. The needs of Member States with fewer resources and experience in cybersecurity were assessed through different means of data collection and analysis.

As a first step in the **analytical process**, the data gathered through the in-depth interviews, the surveys and open public consultation in relation to the operationalised evaluation questions (see the evaluation matrix in Appendix 1) was analysed, comparing and contrasting the views of different stakeholder types from the same data source.

In a second step, the desk-based analysis was triangulated with the data collected through the different stakeholder consultations, allowing for responses to be drafted in relation to the evaluation questions. On this basis, substantiated conclusions were drawn. The conclusions provide an overall judgement of the effectiveness, efficiency, relevance, coherence, EU added value and impact of ENISA and with regard to the future needs and challenges. The preparation of conclusions and, subsequently, the recommendations is based on four pillars:



- Transparent use of all evidence collected
- Validation of conclusions, notably through the stakeholder workshop and an expert panel
- Recommendations flowing directly from conclusions
- Validation of recommendation and their expected impacts, notably through the stakeholder workshop and an expert panel.

**2.4 Developing conclusions and recommendations**

Against the responses to the evaluation questions reached through the analytical tasks, the most pressing issues at the strategic level and at the level of the Agency were identified and options for the future of ENISA developed. Efforts were made to ensure that a clear and direct link was made between the conclusions and recommendations, enabling the tracking of the reasoning from the analysis carried out in relation to the evaluation questions through to the options for the future. By so doing, it is ensured that the extent to which the recommendations are based on opinion, analysis and objectively verifiable evidence is clear.

An estimation of the costs related to each of the factors for change under a given option derived from the results of the evaluation was developed. The assessment was made on the basis of existing standard costings for the period under review (e.g. for full-time equivalents (FTEs), given activities) and took into account additional start-up costs, where relevant. Furthermore, the EU added value and coherence of the suggested tasks was assessed.

**2.5 Challenges and limitations**

The evaluation study presented a number of challenges, often relating to the availability of data. In the following, the main challenges are outlined, together with an explanation of how they were dealt with in the evaluation process.

**Table 9: Challenges in the evaluation process**

Challenge		Solution / Mitigation strategy
<b>Benchmarking</b>	<p>For the benchmarking exercise other EU agencies and bodies were asked to provide data on their set-up (e.g. numbers of staff, vacancies) and on their outputs (e.g. numbers of publications). The completeness of responses received from the selected bodies varied and in a few cases no responses were received. Consequently, only limited data was available for the benchmarking exercise and not all foreseen comparisons could be made. It has not been possible to compare:</p> <ul style="list-style-type: none"> <li>• percentage of administrative staff and the percentage of operational staff</li> <li>• turnover of the senior management</li> <li>• number of management and executive board meetings (only compared for three agencies)</li> <li>• approach to the use of procurement or external expert groups</li> <li>• budget used for procurement of study</li> <li>• budget allocation to publications</li> <li>• number and costs of publications, trainings, awareness raising events</li> </ul>	<p>In response to the difficulties experienced in collecting the quantitative data originally intended, additional efforts were made to reach out to further agencies and, where possible, additional secondary data sources were employed in order to compare ENISA against. The main sources were the European Commission: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III and Court of Auditors (2016): Summary of results from the Court’s annual audits of the European Agencies and other bodies for the financial year 2015; additionally annual reports of the relevant agencies were used.</p> <p>Despite these efforts, it was not possible to compare ENISA to the other agencies with regard to achieved outputs (such as publications, trainings, events).</p> <p>Moreover, while the scope of the evaluation is 2013-2016, the data which was judged most complete and comparable was used for the analysis. Therefore, there are some variations in the years reported on.</p>
<b>Positioning</b>	<p>These organisations selected for the positioning exercise were contacted to provide information on their activities (through an interview and by completing a data sheet). The completeness of the responses received from these</p>	<p>Data collected through the interviews and desk based research on the activities of the selected national and EU organisations was conducted to respond to the limited data received directly from the organisations covering the concrete points under the positioning exercise.</p>

Challenge	Solution / Mitigation strategy	
<p>organisations varied and in a few cases no responses were received despite numerous follow ups per email and over the phone.</p>	<p>Consequently, some of the assessments presented in the positioning exercise are based on desk research and the interviews but have not been triangulated with input from the organisations themselves in the form of the foreseen data sheet. The concerned organisations were not directly asked about their positioning at the detailed level of the data sheet. Therefore they may have a different understanding of their overlaps and complementarities with ENISA.</p>	
<p><b>Assessing outputs and results</b></p>	<p>For the response to several evaluation questions, the use of the Agency’s key performance indicators (KPIs) and was foreseen (for example for evaluation question 31 (EQ31)). ENISA has not been able to provide the requested data to implement the foreseen assessments.</p> <p>The key impact indicators (KIIs) of the Agency set in the annual work programmes and reported upon in the annual activity reports change from one year to the next. This limited the possibility to implement a comparison of the Agency’s outputs and results over the entire period of 2013-2016.</p>	<p>Without the quantitative data on outputs and results the evaluation relied on the qualitative feedback collected through interviews, surveys and the open public consultation. Where available data from the evaluations of ENISA’s activities in 2014 and 2015 has been introduced to the study.</p>
<p><b>Vested interests of stakeholders</b></p>	<p>As outlined in this section of methodology, the study relied to a large extent on stakeholder contributions. These stakeholders (in particular ENISA’s staff and management and the direct stakeholders) may have vested interests in the future of the Agency. Therefore, a critical assessment of contributions needs to be made.</p>	<p>The analysis included triangulation of the data across different stakeholder groups and across the data collection tools. For example, the surveys and the interviews which primarily covered views from ENISA’s staff, management and direct stakeholders were considered against the open public consultation results and the workshop where a broader scope of stakeholders have been reached.</p>
<p><b>Assessment of the costs related to the options</b></p>	<p>The assessment of the cost of the options identified needed to be based on a number of assumptions.</p>	<p>In order to establish as realistic assumptions as possible, the options were operationalised and a variety of stakeholders were consulted (i.e. Commission, ENISA, industry, Member State representatives) and external sources employed where relevant.</p>

### 3. FINDINGS

This chapter presents the findings of the evaluation study. It presents responses to the evaluation questions listed in Appendix 1. The findings are based on the different data collection tools employed, as described in chapter 2.

The chapter is structured as follows:

- The first section presents an overview of the key findings of the study
- The second section presents the detailed findings and conclusions of the study, including the results of the three of the analytical tasks, namely the assessment of ENISA’s performance; the assessment of ENISA’s governance and organisational structure, and the assessment of ENISA’s positioning.
- Finally, the third section presents the results of the SWOT analysis.

These three sections are structured according to the evaluation questions. In order to assist the (busier) reader, a concluding sentence has been highlighted at the top of each paragraph and the findings that support it are presented below it. Moreover, to allow readers to get a quick understanding of the main conclusions, a box summarising the main conclusions for each question can be found at the end of each subsection. Section 3.2 is structured according to the evaluation criteria: relevance, effectiveness, efficiency, coherence and EU added value. Here conclusions can be found for each of the evaluation criteria, as well as for the evaluation questions at a more detailed level.

The conclusions on each of the evaluation criteria include a short comparison of the assessment made for the 2013-2016 with that of ENISA in 2009 and 2010 based on an evaluation of all EU agencies including ENISA in 2009<sup>12</sup> and an impact assessment of changes to ENISA’s mandate in 2010<sup>13</sup>).

As important stakeholders of ENISA’s work and in the decision making on the future of the Agency, Member States’ opinions have been highlighted throughout the report. It should be noted that, based on the different data collection tools, different types of Member State representatives have been consulted (see also section 2.2.2). In the context of the interviews, “Member States” include the members of ENISA’s Executive and Management Board (8 members were interviewed), as well as one consulted national cybersecurity agency. “Member States” in the survey are 19 members of ENISA’s Management and Executive Boards. In the context of the open public consultation, reference is made to “national authorities” which include members of ENISA’s Management and Executive Boards (10 members), as well as representatives of national cybersecurity authorities (8).

Please note that ENISA’s “direct stakeholders” include ENISA’s Management and Executive Board representatives, members of the PSG and NLOs. The European Parliament, CERTs/CSIRTs, the Commission, other agencies and industry representatives are referred to as “(potential) users and advisors” throughout the report.

The findings of previous evaluations of ENISA’s activities have shown that there is a division between the needs of Member States based on their capacity and resources invested in cybersecurity. Throughout the report, a reference is made to Member States with more experience and resources which mainly include France, Germany, the Netherlands and the UK but also cover

---

<sup>12</sup> Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings



<sup>13</sup> European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

Spain, Italy and the Nordic countries to some extent. Member States with fewer resources include the Eastern and Southern European Member States.

### 3.1 Key findings

A number of key issues emerge from the detailed findings presented below, including:

**Table 10: Key findings**

	<ul style="list-style-type: none"> <li>• ENISA’s objectives are of high relevance in the current context</li> <li>• ENISA’s governance and organisational structure are generally conducive to an effective and efficient Agency.</li> <li>• ENISA has contributed to enhanced cooperation between Member States and NIS stakeholders, community building across Member States, cooperation between CERTs/CSIRTs, and capacity in Member States (notably for Member States with fewer resources for cybersecurity). It has done so through a series of activities, most noteworthy of which are the Cyber Europe Exercises.</li> <li>• ENISA works efficiently, implements a high number of activities and develops a large amount of publications with the resources available.</li> <li>• ENISA’s activities are largely coherent with work at national level, notably that of Member States with fewer capacities and resources in cybersecurity, and complementary to the work of CERTs/CSIRTs.</li> </ul>
	<ul style="list-style-type: none"> <li>• ENISA lacks visibility and has not managed to become recognised as a centre of expertise or a reference point for stakeholders.</li> <li>• Limited resources hamper ENISA’s ability to (1) respond to a wide variety of needs, (2) be effective in all areas covered by its broad mandate as it is forced to prioritise, and (3) to recruit and retain staff.</li> <li>• ENISA’s split location in Athens and Heraklion affects its efficiency through additional travel and coordination costs.</li> <li>• ENISA’s work programme is dominated by the interests of Member States, meaning that it does not sufficiently address the needs of other stakeholder types. Moreover, the differing needs of Member States and lack of a common line lead to work priorities representing the lowest common denominator.</li> <li>• ENISA lacks technical expertise, according to stakeholders, with a high reliance on external expertise over in-house expertise</li> <li>• ENISA had weak human resource procedures leading to difficulties in recruiting and retaining staff.</li> <li>• The approach to cybersecurity in the EU is not sufficiently coordinated, with few formal coordination procedures in place to ensure synergies between ENISA’s activities with the policies and activities of its stakeholders; insufficiently exploited cooperation between the Commission and ENISA; and risks of overlap between ENISA and CERT-EU and between ENISA and Member States with strong cybersecurity expertise in particular.</li> </ul>

### 3.2 Assessment of ENISA’s performance, governance organisational structure and positioning

This section assesses the impact, effectiveness, efficiency, relevance, coherence and EU added value of the work undertaken by ENISA from 2013 to 2016 and of ENISA’s governance and organisational structure. The purpose is to evaluate the implementation of the work programmes and to assess how the whole set of activities run by ENISA (including opinions, guidelines, trainings, recommendations or reports) has contributed to fulfilling its role, as described in Article 1 of the ENISA Regulation. The section presents the extent to which ENISA has become "an EU-wide centre of expertise and a reference point for EU institutions, Members States and the wider stakeholders' community, in providing guidance, advice and assistance on issues related to network and information security". Moreover, the section assesses how effectively the current governance, internal organisational structure of ENISA (Management Board, Executive Board, Executive Director and staff and PSG) and human resources policies and practices contribute to efficiencies and effectiveness in the work of the Agency. The purpose is to provide an assessment of the internal organisational structure including an evaluation of the efficiency and effectiveness of the current arrangements related to the location of ENISA's offices. This part of the evaluation also includes an assessment of how effectively the Agency sets its work priorities, as well as the degree of flexibility it has at its disposal to tackle any upcoming issues. Finally, ENISA’s working relationship with the Commission, other EU institutions and bodies and stakeholders are also analysed, including the extent to which stakeholders are aware of and involved in ENISA's work.

This section relates primarily to the first dimension of this evaluation, namely the retrospective aspects. It responds to the evaluation questions, structured according to the evaluation criteria of relevance, effectiveness, efficiency, coherence and EU added value.

Please note that for each of the evaluation criteria an “overarching” question has been identified and has been responded to in the concluding section for each criterion.

#### 3.2.1 Relevance

The evaluation criterion of relevance looks at the relationship between the needs and problems in society and the objectives of a given intervention, in this case the existence of a European agency of network and internet security.<sup>14</sup> The first sub-section below responds to this question by assessing the relevance of ENISA’s objectives. As the evaluation questions presented in the Evaluation Roadmap focus on the relevance of ENISA’s tasks, the subsequent sub-sections consider the relevance of the activities implemented by ENISA rather than its objectives.

The following evaluation questions are covered in this section:

**Table 11: Evaluation questions covered under the relevance criterion**

Main evaluation question	Other evaluation questions
<b>EQ33: Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework needs?</b> <sup>15</sup>	<p><b>Retrospective</b></p> <p>EQ29: How far are the Agency's tasks and resources aligned with key EU political priorities?</p> <p>EQ4: How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders?</p> <p>EQ30: Which Agency tasks are absolutely essential to deliver on these priorities?</p> <p>EQ31: Which Agency tasks are necessary to continue implementing existing and</p>

<sup>14</sup> Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

<sup>15</sup> For the response to this evaluation question, the use of the Agency’s KPIs related to stakeholder engagement was foreseen. In the end, the data foreseen was not available (This concerns KPIs related to the uptake of the Agencies’ expertise in policy documents or by industry and KPIs related to the Agencies’ contribution to policy development through events).

	<p>evolving obligations under the Treaties and EU legislative framework?</p> <p>EQ32: Are there some Agency tasks that have become redundant / negative priorities? If so, which are they?</p> <p>EQ34: Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?</p>
--	--

### 3.2.1.1 Relevance of the objectives set in ENISA’s mandate

#### **EQ 33: Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework needs?**

The five objectives listed in ENISA’s mandate were over the period 2013-2016 and are still today of continued relevance considering the needs of ENISA’s stakeholders (Member States, including CERTs/CSIRTs, the Commission and other EU institutions and the private sector) and the regulatory and policy context. The development of the cyber threat landscape over the past years shows a continued need for a response at EU level. The objective of ENISA to provide expertise is relevant as it sets the foundation for ENISA to pursue any of the other objectives. Assistance to the development of policies responds to the Commission’s needs to receive sector-specific knowledge, and the assistance to the implementation of policy and legislation responds to the Commission and Member States’ needs in the context of the Directive concerning measures for a high common level of security of network and information systems across the Union (hereafter NIS Directive)<sup>16</sup>. Strengthening Member States’ capabilities and preparedness and stimulating cooperation between Member States and with private stakeholders are objectives of high relevance considering the need for combined efforts to address cyber threats across the EU.

An additional objective that ENISA’s mandate could have covered is the operational support to Member States through more detailed analysis of threats and incidents to provide enhanced advice to these stakeholders.

ENISA’s mandate defines five objectives for the work of the Agency<sup>17</sup>:

- The Agency shall develop and maintain a high level of expertise.
- The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
- The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
- The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
- The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

**A perceived increase in the number and variety of cyber threats over the past years, underlines the continued relevance of all of ENISA’s objectives.** ENISA’s direct stakeholders and the other groups of stakeholders interviewed agree that with the fast pace of technological development and the increase in devices connected to the internet, the variety of cyber threats has been growing in the past years. New technologies enter the market within a few months, leading to new NIS risks. Consequently, all groups of consulted stakeholders see a continued relevance for cybersecurity efforts at EU and Member State level. The evaluations of ENISA’s 2014 and 2015 core operational activities also found a clear need to address cybersecurity challenges in

<sup>16</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

<sup>17</sup> Regulation (EU) No 526/2013, Article 2

the EU and the Member States. Although differences in the needs of ENISA's stakeholders were identified, the objectives of ENISA's work during 2014 and 2015 were found to be relevant to respond to the needs of Member States and stakeholders across the EU.

The objectives listed in ENISA's mandate are broadly defined. To some extent this has allowed the Agency in the past to encompass a variety of activities. Changes in the activities of ENISA based on the annual work programmes show that the way the objectives have been defined allows for flexibility to focus on different needs from one year to another. At the same time, this leads to a discontinuation of activities and limited possibilities to create strong expertise in more specific areas. ENISA's resources do not allow the Agency to fully meet its objectives (as discussed in section 3.2.3.3).

Most interviewees in the present study (including the Member States) considered ENISA's objectives to be of continued relevance. While there are differences in the objectives which are considered to be most relevant, all of them were mentioned to be very important by at least one of the stakeholder groups.

**Developing and maintaining a high level of expertise is a relevant objective that lays the foundation for achieving ENISA's other objectives.** The objective was considered by a majority of interviewees (including some but not all interviewees from the Member States) as a relevant objective. It was seen as the foundation for achieving ENISA's other objectives as expertise is required to understand cybersecurity threats, which is needed to prepare recommendations for the development and implementation of policies, as well as to foster cooperation between the Member States on relevant issues. Both the Member States and the Commission were described as relying on the expertise of ENISA.

In contrast, a few interviewees (including an interviewee from the Member States) noted that ENISA's objective to create and maintain a high level of expertise was not the most important one, as there is considerable expertise at Member State level. This suggests a difference between the needs of Member States depending on their capacity and the financial resources available to them in the area of cybersecurity, showing that those with less focus on this area are more dependent on ENISA's input and therefore expect the Agency to increase its expertise.

**The objective to assist the Union institutions, bodies, offices and agencies in developing policies in NIS continues to be relevant as ENISA can provide added value with technical input.** The objective was found to be important by all types of interviewed stakeholders. They generally saw a need for ENISA to provide technical advice to the Commission to ensure that legislation matches technical needs, for example regarding norms and standards for cybersecurity. This included interviewed Commission staff who considered the expertise that can be provided by an EU cybersecurity agency to be of high relevance to their activities. Under this objective, stakeholders expected ENISA to systematically be involved and assist the Commission when drafting legislation or policies.

**The objective to provide assistance to the Union institutions, bodies, offices and agencies and the Member States in implementing policies and legislation is of particular relevance considering ENISA's role under the NIS Directive.** Under the recent changes to the legislative framework, most importantly the NIS Directive, ENISA is foreseen to fulfil the function of supporting the implementation of legislation. The objective was mentioned comparably less often by interviewed stakeholders as one of their needs. Still, several interviewees (mainly ENISA staff and management but also representatives from other groups including the Member States) considered this objective to be relevant. ENISA's role in the context of the NIS Directive, namely to ensure its implementation, was considered very relevant by these interviewees. Industry representatives and representatives from EU institutions and bodies stated that there is a

need in the Member States for a body that ensures harmonisation and alignment of practices between the countries, as the Commission was not considered to be able to fully ensure this.

**With its objective to assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to NIS problems and incidents, ENISA responds to a clear need in the Member States.** The objective was considered to be of continued relevance by interviewed Member State and Commission representatives. Several Member States saw the enhancing of capabilities as a core objective, noting that there is a need for an agency to help small Member States who do not have the same capacities as larger ones. In the context of increased cyber threats, it was considered very important that the network of CERTs/CSIRTs is able to share relevant information and to consider a coordinated approach. Interviewees underlined that, to achieve this, all members of the network would need to have a certain capacity level. This underlines the relevance of ENISA's objective to enhance and strengthen capabilities and preparedness across Member States and stakeholders.

**The fifth objective of ENISA, to use its expertise to stimulate broad cooperation between actors from the public and private sectors, is of continued relevance as trust needs to be built between stakeholders to ensure their cooperation on threats that often concern more than one of them at a time.** The objective was considered relevant by interviewees from the Member States and the Commission. Also ENISA staff and management considered the need for enhanced cooperation to be significant. Member State respondents specifically underlined their need for cooperation between the countries to build a community with sufficient trust to ensure that exchanges of information are taking place. Members of ENISA's staff noted that the need had further developed over the past years. While initially ENISA had to convince stakeholders, in particular the Member States, that there was a need for more advanced cooperation, the Agency's objective is now to actually implement such cooperation. The need to build trust was also mentioned by respondents from the Commission who considered cooperation between the public and the private sector to be relevant to respond to current cybersecurity threats.

**In summary, all present objectives were found to be of continued relevance but some stakeholders saw a need for additional objectives.** Most mentioned that there was a need for operational support from ENISA. Some of the Member States saw a need to change the Agency's mandate to give it a role as an analytical centre analysing threats and incidents in detail to provide better advice to stakeholders. A few respondents (ENISA staff and Member States) also suggested that there is a need for enhanced cooperation in the field of law enforcement. The Agency could have a role in ensuring that criminal investigations on cybersecurity are more concerted and resources are pooled across the countries. As this is a role already covered by Europol, it can be assessed that changes to ENISA's mandate should be limited to suggesting further cooperation between the two agencies. Another example of an unmet need is support to private stakeholders, including small and medium sized enterprises (SMEs). A few interviewees from the private sector suggested that they could benefit from ENISA's risk assessments capacities and training on how to respond to incidents.

With regard to digital privacy issues, several interviewees noted that ENISA's objectives should remain in the area of cybersecurity as this is where the needs of the Agency's stakeholders are. During the interviews, only two respondents (European Parliament and private sector) suggested that they saw a need for ENISA to cover privacy concerns.

### 3.2.1.2 Alignment of ENISA's tasks and resources with key EU political priorities

**EQ 29: How far are the Agency's tasks [and resources] aligned with key EU political**



**priorities?**

ENISA's mandate and tasks are strongly aligned with key EU political priorities, most importantly the NIS Directive and the new tasks it foresees for the Agency. In general, cybersecurity is considered to be a topic of high importance and a majority of stakeholders across all spectrums considers ENISA's tasks to be well aligned with political priorities and stakeholder needs. However, Member States' needs differ and the Agency is not able to respond to all needs to the same extent.

The adequacy of ENISA's human and financial resources is assessed under EQ16 in section 3.2.3.3.

As presented in section 1.2.1 above and in line with the Agency's objectives, ENISA's tasks can be summarised as covering the following four activities:

- Expertise provision
- Supporting the Commission in policy development
- Supporting Member States in the implementation of legislation
- Community building
- Capacity building.

**ENISA's tasks are aligned with EU priorities in the area of network and information security as presented in relevant EU initiatives.** NIS has been on the agenda for EU policy makers since the 2001 Communication of the European Commission on NIS<sup>18</sup>. The following year – the ePrivacy Directive<sup>19</sup> was adopted, binding providers of electronic communications services to ensure the security of their services and maintain the confidentiality of client information. Back in 2010, when the Europe 2020 strategy was adopted, a Digital Agenda for Europe (DAE) became one of the seven strategic goals for the EU future<sup>20</sup>. The DAE's main objective was to develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe. The third pillar of the DAE is specifically addressing Trust & Security issues<sup>21</sup> and serves as an umbrella for all EU conducted and coordinated activities in the field of NIS. The 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry<sup>22</sup> sets out a strategy for the future of cybersecurity in Europe. Most recently, the NIS Directive was adopted by the European Parliament on 6 July 2016. The Directive entered into force in August 2016, giving ENISA new tasks that were not foreseen as part of its mandate, including assisting the Cooperation Group in the execution of its tasks and taking on the role of the CSIRT Network Secretariat. ENISA's tasks to foster cooperation, develop and maintain expertise in the EU, increase capacities and support the development and implementation of policy, are generally aligned with the EU priorities set out in the initiatives listed above. Moreover, the way in which ENISA's tasks are described is sufficiently broad in scope to allow for the changing EU political context to be taken into account. In particular, the new tasks foreseen for the Agency as part of the NIS Directive fall well within ENISA's current mandate – its role relative to the Cooperation Group involves assisting the Union institutions in the implementation of the policy, while its role as the Secretariat for the CSIRT Network will involve further fostering cooperation among CERTs/CSIRTs.

**NIS continues to be a key political priority of the EU to which ENISA is expected to respond.** In its communication of 5 July 2016<sup>23</sup>, the European Commission encourages Member States to make the most of NIS coordination mechanisms. According to the NIS Directive, ENISA

<sup>18</sup> COM(2001)298, Network and Information Security : proposal for a European Policy approach

<sup>19</sup> Directive 2009/136/EC Of The European Parliament And Of The Council Of 25 November 2009

<sup>20</sup> COM (2010) 2020 final, Communication From The Commission Europe 2020. A strategy for smart, sustainable and inclusive growth; Brussels, 3.3.2010

<sup>21</sup> Digital Agenda for Europe, Pillar III: Trust & Security <<https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security>>

<sup>22</sup> COM (2016)410, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

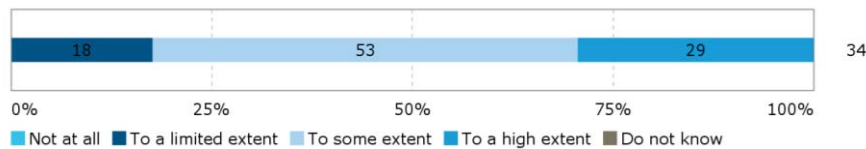
<sup>23</sup> European Commission , *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*, Press release, Brussels, 5 July 2016

will have a stronger role to support this coordination. Stakeholders across all interviewed groups agreed that NIS was one of the key EU political priorities, mainly considering the increasing frequency, variety and intensity of cyber threats and suggested that ENISA should be part of the response to these.

**Overall, ENISA’s tasks are considered to be well aligned with the priorities of its stakeholders.** This was noted by a majority of interview respondents, in particular ENISA’s direct stakeholders. They highlighted ENISA’s work on ensuring interaction and exchange between the Member States, increasing capacity in the Member States and raising awareness of cybersecurity issues. With regard to specific tasks, ENISA’s expected work under the NIS Directive was highlighted as an example of where ENISA’s tasks are particularly well aligned with the political priorities. Exercises and the Threat Landscape reports<sup>24</sup> are examples of where ENISA is meeting the needs of its stakeholders.

Satisfaction with ENISA’s activities can also be seen in the responses to the survey of CERTs and CSIRTs as presented in Figure 6 below. Survey respondents were in most part satisfied with the extent to which ENISA covered the needs of CERTs/CSIRTs over the 2013-2016 period. A large majority of respondents (28 out of 34) thought ENISA covered the needs of CERTs/CSIRTs to a high or to some extent during that period, while six out of 34 thought it did so to a limited extent.

**Figure 6: To what extent did ENISA cover CERTs/CSIRTs’ needs over the 2013-2016 period?**



Source: CERTs/CSIRTs survey

**Stakeholders suggest that ENISA’s tasks respond to the key policy priorities due to the strong influence of the Member States on the mandate.** The 2014<sup>25</sup> and 2015<sup>26</sup> annual evaluations of ENISA showed that ENISA’s activities during these years were clearly linked to the Agency’s legal mandate. There were no cases falling outside the scope of the mandate. Interviewees in the present study (Member States, ENISA staff and EU institutions and bodies) mentioned the delivery of tasks according to its mandate as one of the reasons why ENISA’s work is well aligned with political priorities. As the work programme itself is set by the Commission and the Member States, it is aligned to their intentions and needs. ENISA staff and management suggested that they were well prepared to respond to changing priorities and the needs of the Agency’s constituency.

**There are differences with regard to stakeholders’ needs in the context of the key EU political priorities.** Between the Member States there is disagreement on the extent to which ENISA should cover specific topics, such as certification<sup>27</sup> or whether ENISA should develop operational capacities which could include responsibilities in the area of detection and response to cybersecurity threats. While some Member States would welcome ENISA’s support in this area, others have developed their own capacities. In general, Member States with less capacity and fewer resources in the cybersecurity area (e.g. Eastern and Southern European countries) tend to be in favour of further support by ENISA while Member States with more resources and experience

<sup>24</sup> ENISA publishes every year a report summarising the most prevalent cyber-threats, entitled Threat Landscape

<sup>25</sup> Ramboll Management Consulting (2015) External Evaluation Of ENISA, focussing on ENISA’s 2014 activities.

<sup>26</sup> Ramboll Management Consulting (2016) External Evaluation Of ENISA, focussing on ENISA’s 2015 activities. Ramboll Management Consulting (2015) External Evaluation of ENISA, focussing on ENISA’s 2014 activities.

<sup>27</sup> “Certification” means the implementation of common security certification frameworks for Information and Communication Technologies against harmonized principles a/o standards. Many stakeholders see a role for ENISA in the development of these standards and the application of a certification scheme for the public and/or private sector.

(e.g. Germany, France, the Netherlands and Sweden) do not see the necessity for ENISA to cover these issues.

### 3.2.1.3 Balance between cybersecurity and digital privacy topics

**EQ4: How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders?**

When only considering the identified needs of ENISA’s main stakeholders, the Agency should focus on the cybersecurity area and disregard digital privacy topics. However, the evaluation identified some potential benefits of giving responsibilities to ENISA to ensure greater coordination between the cybersecurity and digital privacy areas.

In the preamble to the Regulation, the objectives linked to cybersecurity and digital privacy topics are presented on an equal footing (“*The Agency should contribute to a high level of network and information security, to better protection of privacy and personal data...*”). However, protection of privacy and personal data are not listed among the objectives listed in the Regulation itself. This leaves room for some discussion on the extent to which ENISA should respond to privacy issues and how these activities should be balanced with the cybersecurity tasks it performs. This fact is also reflected in stakeholders’ feedback on this issue.

**The main needs of ENISA’s stakeholders lie in the area of cybersecurity; digital privacy topics are not considered to be a priority.** A number of interviewees (mainly from EU institutions and bodies) noted that they were not aware of any activities of ENISA in the area of privacy protection but also did not consider this to be a relevant issue in its work. Furthermore, most of ENISA’s direct stakeholders explicitly stated that ENISA should not be covering digital privacy topics, arguing that the Agency should focus its limited resources on cybersecurity topics and that there were other bodies which were better equipped to cover the privacy area such as the European Parliament, DG JRC or the European Data Protection Supervisor (EDPS).

**Stakeholders saw potential benefits for ENISA, its stakeholders and society at large if the Agency were to act as a broker, supporting cooperation across the digital privacy and cybersecurity issues.** Several interviewees from the group of users and advisors pointed to intersections between cybersecurity (e.g. the security of electronic communication) and digital privacy. In these areas ENISA could provide its expertise and share solutions that relate to security and privacy at the same time. One of the interviewees suggested that in the Member States there was a gap between cybersecurity and data protection, suggesting that national representatives working in these two areas would not necessarily be cooperating in all Member States and that ENISA could be the one to start such cooperation.

### 3.2.1.4 Essential tasks to deliver on key EU political priorities

**EQ30: Which Agency tasks are absolutely essential to deliver on these priorities?**

Among the four tasks of ENISA (capacity building, expertise, community building and policy implementation and development), community building stands out as being absolutely essential. ENISA’s stakeholders considered the Agency to be best placed to foster cooperation across the Member States and with other stakeholders.

**Different groups of stakeholders see different priorities for ENISA which makes it difficult to rank ENISA’s tasks according to their relevance.** In particular ENISA’s direct stakeholders and the representatives of national CERTs/CSIRTs consider capacity building to be

essential. They underlined the need to ensure that Member States grow their expertise based on ENISA’s support. Specifically the cyber exercises<sup>28</sup> were mentioned as a highly relevant activity.

Among EU-level institutions and other stakeholders, such as industry, community building and the provision of expertise were considered to be essential. With tasks covering expertise, ENISA is expected to anticipate and support the EU as a whole in facing emerging NIS challenges by making information on cybersecurity available and accessible to the EU. Stock taking of practices and experiences across the EU and best practices disseminated to Member States and the industry were considered to be of high relevance. Several Commission DGs highlighted the capability of ENISA to provide thematic expertise in their relevant sectors.

ENISA’s work to establish and facilitate dialogue between the Member States’ authorities and with industry stakeholders and academics is considered essential. This work of community building is expected to foster collaboration allowing Member States to better respond to cyber threats.

Finally, across the different stakeholder groups, some interviewees suggested that ENISA’s policy work was essential. These stakeholders suggested that ENISA had a key role in supporting policy implementation. Some also mentioned that they expected ENISA to provide input to policy development based on their expertise, but saw a need for the Agency to improve the dissemination of their knowledge and their visibility to take on this role.

The key current demands or needs according to the different types of stakeholders are summarised in Table 12 below.

**Table 12: Key current demands or needs according to the different types of stakeholders**

Stakeholder type	Key demands for ENISA
<b>European Commission</b>	Community building Expertise provision Supporting policy development / implementation
<b>Member States with strong capacities and more resources</b>	Community building Supporting policy development at EU level
<b>Member States with fewer resources and capacities</b>	Capacity building Supporting policy development at EU level Supporting policy implementation at national level Community building Expertise provision
<b>CERTs/CSIRTs</b>	Capacity building
<b>Industry</b>	Community building Expertise provision Supporting policy development / implementation

**Among the four tasks, the one that stands out as most essential is that concerning community building.** When interviewees were asked what the consequences of a discontinuation of ENISA would be (see section 3.2.5.3), respondents across all stakeholder groups saw a huge need for continuation of cooperation across the Member States (in particular between the CERTs/CSIRTs) and also with other stakeholders and considered ENISA as best placed to ensure this.

3.2.1.5 Necessary tasks to implement existing and evolving obligations

**EQ31: Which Agency tasks are necessary to continue implementing existing [and evolving] obligations under the Treaties and EU legislative framework?**  
 The evaluation findings show that different specific activities within ENISA’s four tasks (capacity, expertise, community and policy) are considered necessary to continue responding to the Agency’s

<sup>28</sup> ENISA leads a wide range of activities in the field of cyber exercises. They are related with to activities on increasing capacities in cyber crisis management. Most mentioned were the Cyber Europe Exercises.

existing and evolving obligations. ENISA's obligations under the EU legislative framework can cover a wide array of tasks which respond to stakeholders' current needs. Some suggestions of services that could have been provided by ENISA were made (including the provision of real-time cybersecurity information and further guidelines and benchmarks for the public and the private sector), but stakeholders would not be willing to pay for additional products or services.

Evolving obligations under the Treaties and the EU legislative framework are discussed in sections 3.3.1 and 3.3.2.

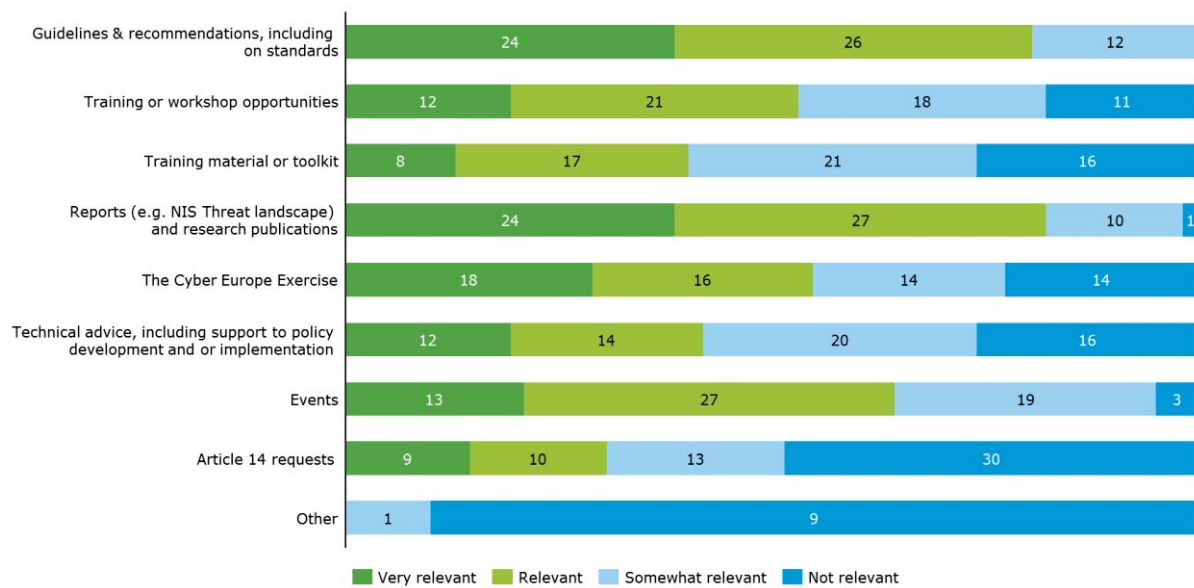
**ENISA's obligations under the Treaties and the EU legislative framework cover a broad area and primarily depend on what the Member States are expecting from ENISA and what is included in the Agency's annual work programmes.** ENISA's direct stakeholders describe the Agency's existing obligations as stemming from its unique position as a neutral player in the field of cybersecurity, serving Member States and the EU institutions. According to these stakeholders, ENISA's obligations include an objective to ensure harmonisation across the Member States to align their cybersecurity capabilities and capacities. Furthermore, they mention specific legislation requiring ENISA's attention, such as the NIS Directive and the General Data Protection Regulation<sup>29</sup>. ENISA's obligations based on Regulation (EU) No 526/2013 are perceived as being broad and rather flexible, requiring the Member States to define what they are expecting from the Agency.

**Across the four main tasks of the Agency, there are a number of specific activities that are considered to be relevant by stakeholders.** Among the respondents to the open public consultation, the products and services most frequently listed as being "relevant" or "very relevant" to respondents' work or activities were reports and research publications (82% or 51 out of 62 respondents), guidelines and recommendations, including publications on standards (81% or 50 respondents) and events (65% or 40 respondents). In contrast, 48% of respondents (30) indicated that Article 14 requests were not at all relevant to their work or activities. These requests can however only be used by Member States and the Commission. Respondents from national authorities considered most often selected guidelines and recommendations (9 out of 15), reports and research publications (6 out of 15), and the Cyber Europe Exercise (8 out of 15) as "very relevant". Article 14 requests were considered to be "not relevant" by five national authority respondents.

---

<sup>29</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

**Figure 7: Relevance of products/services to respondents' work/activities (n=62)**

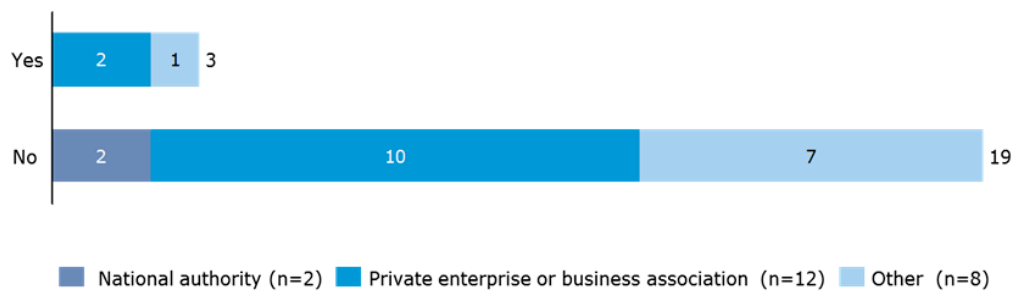


Source: Open public consultation

In the context of the open public consultation, respondents were asked if there were any other products or services they would have liked ENISA to provide the cybersecurity community with over 2013-2016. Out of 62 respondents, 65% (40) answered “no”, while 35% of respondents (22) answered “yes” which were primarily constituted of private enterprise or business association respondents. Only two respondents from national authorities responded “yes” to the question. These respondents were asked to further specify what kind of services they would have liked ENISA to provide. Their responses can be categorised into three broad topic areas, namely: operational capacities, cross-country cooperation (across Member States and with non-EU countries) and the provision of policy advice and guidelines. With regard to products and/or services related to ENISA’s operational capacities, respondents would have liked ENISA to provide near real-time cybersecurity warnings and consider developing a panel of security operation services to address cross-country cyber incidents. With regard to products and/ or services related to cooperation across Member States, respondents would have liked ENISA to encourage information sharing to support the adoption of new regulations and incident handling procedures as well as supporting cybersecurity capacity building. Respondents would have also liked ENISA to make visible the kind of expertise and knowledge available in Member States. With regard to products and/or services related to cooperation with stakeholders outside the EU, respondents would have liked ENISA to work together with the public and private sector to act as a contact point for cybersecurity organisations from outside the EU allowing it to also promote European security technology in foreign markets and provide cybersecurity capacity building in third countries. Finally, with regard to products and/or services related to policy and guidelines, respondents would have liked ENISA to provide benchmarks and best practices to help establish the framework for an EU cybersecurity strategy. These could cover for example, cybersecurity priorities for research and development and securing critical infrastructure. It was also suggested that ENISA could contribute by creating horizontal policy documents and guidelines across for exchange across EU bodies.

Open public consultation respondents were further asked whether they would be willing to pay for additional services if they were provided by ENISA. Only 14% of respondents (3) who would have liked ENISA to provide further services over the 2013-2016 period indicated they would be willing to pay a fee in the future for the additional products or services they would have liked ENISA to offer during 2013-2016.

**Figure 8: Respondents willing to pay a fee to obtain additional products/services from ENISA over 2013-2016? (n=22)**



Source: Open public consultation

### 3.2.1.6 Tasks that potentially have become redundant

**EQ32: Are there some Agency tasks that have become redundant / negative priorities? If so, which are they?**

The evaluation has not identified any redundant tasks implemented by ENISA. The assessment of the relevance of ENISA's tasks strongly depends on stakeholders' differing needs. The Management Board seems to set the right priorities, though some stakeholders would like ENISA to be able to act more on their own initiative.

**Based on the stakeholder consultation, no tasks of ENISA have been identified as being redundant or a negative priority.** Interviewees across all groups stated that there was no redundant work done by ENISA. In particular in the context of a very restricted budget, ENISA would ensure that only relevant tasks were being implemented. The Management Board was mentioned as an important mechanism to ensure the relevance of all of ENISA's tasks. Similarly, from the open public consultation, no task or activity of ENISA emerged as being potentially redundant.

The only activity that was mentioned by more than one interviewee as something ENISA should not focus on was the work in the area of privacy which two interviewed stakeholders considered to be outside the Agency's key competences. Other responses to the question on redundant tasks, on the one hand, showed that needs differ between the Member States based on their national capacity and resources. Interviewees mainly referred to tasks that could be made more relevant by implementing some improvements rather than suggesting that these tasks be completely abandoned. Although no redundant tasks were identified, some interviewees suggested that ENISA should be able to act more on its own initiative and could intervene more strongly to set priorities when the members of the Management Board have opposing opinions or when suggested tasks only respond to Member States' needs and leave out those of other stakeholders.

### 3.2.1.7 Non-core activities becoming part of the core-business

**EQ34: Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?**

There are activities which have moved from non-core to the core-business of the Agency, such as specific training activities or the topic of critical infrastructures. These changes can be assigned to technological developments and changes in the needs of the Member States based on legislation, their capacities and preferences.

**Over time, some of ENISA's activities have moved from non-core to being part of the core-business, but the development can also be noted in the opposite direction.** ENISA's direct stakeholders and ENISA staff mentioned examples of changes in ENISA's core activities,

such as in the area of capacity building and training. These were initially key tasks of the Agency which became less of a focus with growing levels of expertise in certain Member States, but more recently have become a priority once again with the implementation of the NIS Directive. Another example provided relates to critical infrastructures which Member States with strong cybersecurity expertise initially preferred covering themselves, but more recently they have welcomed ENISA's support in this area. According to ENISA staff, awareness raising has been less prioritised over the years, mostly as Member States have taken on part of the activities themselves, for example in the planning and implementation of the Cybersecurity Month.

**The priorities set among the Agency's tasks depend on the demand from the Member States and the technological evolution.** With ENISA's broad mandate it is possible to change priorities with regard to specific tasks from one year to another. The priorities set depend on the one hand on technical developments which require ENISA to set their focus on a specific area, such as with the evolution of the Internet of Things (IoT). On the other hand, the Member States can, through their position in the Management Board, decide what ENISA should be focussing on (see section 3.2.2.5 for more information of ENISA's effectiveness at setting its work priorities). Where ENISA helps them to put in place a specific initiative, the Member States might be able to implement the work themselves after some time. With changing legislation, the Member States might require support from ENISA in a new area.

#### 3.2.1.8 Conclusion on relevance

##### **Conclusion – Relevance**

*The baseline situation (established based on an evaluation of all EU agencies including ENISA in 2009<sup>30</sup> and an impact assessment of changes to ENISA's mandate in 2010<sup>31</sup>) shows an increasing dependence on NIS across ENISA's stakeholders and increasing expectations on what the Agency should be delivering. The impact assessment of 2010 concluded that the tasks listed in the Regulation on ENISA were insufficient to provide the Agency with the necessary flexibility and adaptability to respond to the continuously evolving NIS environment.*

The assessment of ENISA's relevance over the period 2013-2016 concludes on the continued relevance of NIS. It points to the fact that ENISA has a broad mandate which allows it to take on new topics as they emerge. However, at the same time, the Agency has difficulties meeting all of its objectives resulting from its broad mandate due to limited resources; it is often forced to prioritise (see section 3.2.2).

In the context of technological developments and evolving threats, over the period 2013-2016 there was a significant need for increased NIS in the EU. This continues to be the case today. The recent additions to the legislative framework, such as the NIS Directive and the Commission's communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry<sup>32</sup> underline this. Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. Based on its mandate, ENISA is intended to respond to these needs.

Considering this context, the objectives set out in ENISA's mandate continue to be of high

<sup>30</sup> Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

<sup>31</sup> European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

<sup>32</sup> European Commission: Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry COM(2016) 410 final



relevance today.

These objectives also leave room for ENISA’s Management Board to set priorities based on latest developments in order to respond to changing needs and evolving threats.

While ENISA’s mandate remains relevant, its activities do not fully meet the needs of all t stakeholders for two main reasons:

- ENISA relies on its the Member States and the European Commission to provide clear guidance via the Management Board on where its contribution is most needed. Its work programme is dominated by the interests of Member States, and yet it is necessary to consider the longer-term perspective and the activities of other stakeholders in the cybersecurity area (such as other EU agencies) to ensure continued relevance of the Agency.
- ENISA’s stakeholders strongly differ in their needs, making it difficult to meet them all. Some Member States (such as Germany, France or Sweden) have significant capacity and resources in the area of cybersecurity and rely on ENISA only for specific services. Other Member States (from Eastern and Southern Europe) are less experienced and rely more strongly on the expertise and capacity of ENISA. The Commission has their own needs and expectations with regard to the services that ENISA can provide the different DGs with. Additionally, industry stakeholders, including a high number of SMEs are important actors in NIS and could also benefit from ENISA’s activities.

ENISA could respond better to stakeholders’ needs by providing operational support to Member States through analysis of threats and incidents to provide enhanced advice to these stakeholders and support response cooperation.

Among ENISA’s direct stakeholders, cybersecurity needs prevail over digital privacy needs.

### 3.2.2 Effectiveness

This section covers the evaluation criteria effectiveness. The effectiveness analysis considers how successful EU action, in this case the activities of ENISA, have been in achieving or progressing towards its objectives<sup>33</sup>. It also includes an assessment of the effectiveness of ENISA’s governance and internal organisational structure.

The following evaluation questions are covered in this section:

---

<sup>33</sup> Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

**Table 13: Evaluation questions covered under the effectiveness criterion**

Main evaluation question	Other evaluation questions
<p><b>EQ1 To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate?</b></p>	<p><b>Retrospective</b></p> <p>EQ2: What have been the benefits of acting at agency level both from the operational and strategic perspective?</p> <p>EQ3: To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe? What more could be done?</p> <p>EQ5: To what extent has ENISA become an EU-wide centre of expertise and a reference point for stakeholders<sup>34</sup> in providing guidance, advice and assistance on issues related to network and information security?</p> <p>EQ6: How effectively has the Agency managed to set its work priorities?</p> <p>EQ7: How effectively does the Agency tackle important upcoming, unplanned issues deriving by demands of its constituencies and/or EU policy priorities?</p> <p>EQ8: Does the Agency consistently perform the same tasks with the same quality level over time?</p> <p>EQ11: How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to effectiveness in the work of the agency?</p> <p>EQ12: How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate?</p> <p>EQ13: What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives?</p> <p>EQ19: To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc.)?</p> <p>EQ20: To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?</p>

3.2.2.1 Implementation of tasks and achievement of objectives

**EQ1 To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate?**

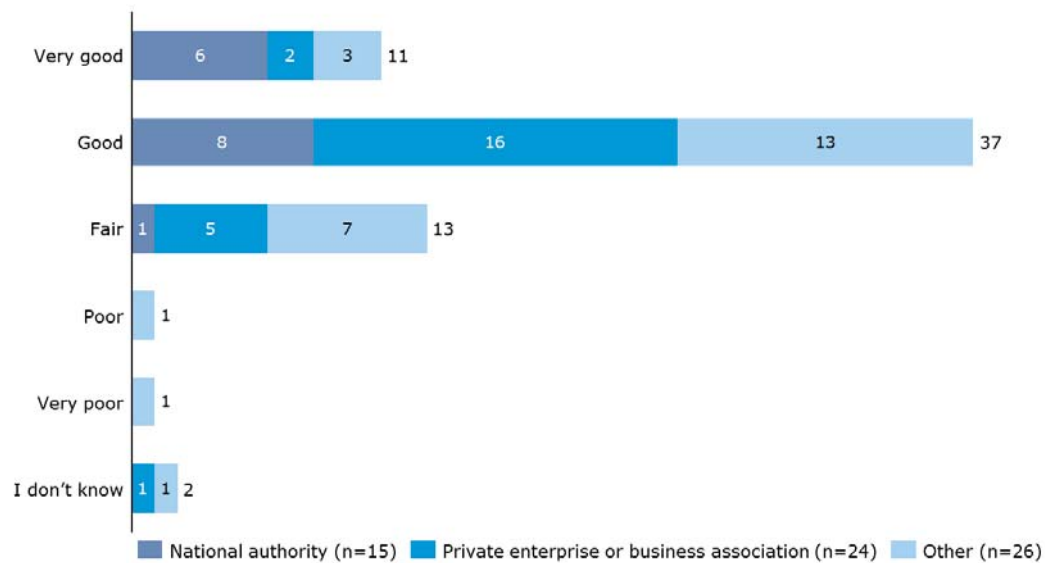
ENISA successfully implements the tasks set by its annual work programmes and achieves targeted KIIs. However, ENISA has difficulties covering the entire spectrum of the broad mandate in each of the work programmes due to limited resources. Consequently, ENISA makes a more significant contribution to some of its objectives, in particular enhancing cooperation and ensuring capacity building in the Member States. The objectives to develop and maintain expertise and to support the development and implementation of policy are attained to a smaller extent. The activities of the Agency that benefit the private sector directly are limited. The Cyber Europe Exercises, support to CERTs/CSIRTs, its publications and the Cybersecurity month are some of ENISA’s main achievements.

**There is a generally positive, but not excellent, perception of ENISA’s work over the period 2013-2016.** Respondents to the open public consultation were asked to give an overall assessment of ENISA for the period. Overall, 74% of respondents to the open public consultation (48 out of 65) had a positive (very good or good) view of ENISA. The overall assessment of ENISA

<sup>34</sup> The stakeholders include EU institutions, Members States and the wider stakeholders community

was more positive among national authorities, while respondents from the private sector were more likely to indicate their overall assessment as being “fair”.

**Figure 9: Overall assessment of ENISA for the period 2013-2016, (n=65)**



Source: Open public consultation

**ENISA attempts to implement all its tasks. For some of the activities, there is mixed feedback on their degree of quality.** Based on its mandate and the annual work programmes, ENISA implements the tasks assigned to it. The main outputs of the Agency’s activities are publications as presented in Table 14 below. Reports are available for download on ENISA’s website and statistics of downloads show that downloads of publications have been consistently high over the four years under review.<sup>35</sup>

**Table 14: Achieved outputs<sup>36</sup>**

	2013	2014	2015	2016
<b>Number of publications</b>	54	45	52	64
<b>Number of downloads</b>	856,017	766,385	808,923	901,464
<b>Number of training sessions</b>	not available	11	10	11
<b>Number of participants per training</b>	not available	190	170	150
<b>Number of exercises</b>	1	1	1	2
<b>Number of participants per exercise</b>	30-50	600-800	40-50	900-1100

Source: information provided by ENISA

ENISA’s training sessions are targeted at CERTs/CSIRTs. In 2015, CERTs/CSIRTs from seven Member States received training, involving various private and public organisations.<sup>37</sup>

Feedback on the quality of the Agency’s outputs is varied. A number of interviewees from all stakeholder groups suggested that the degree of usefulness and quality of ENISA’s reports/publications was not always satisfactory. Feedback on trainings from CERTs/CSIRTs

<sup>35</sup> An assessment of further outputs has not been made as output indicators change from one year to the next and thus do not allow to make comparisons over the years.

<sup>36</sup> This data was provided by ENISA.

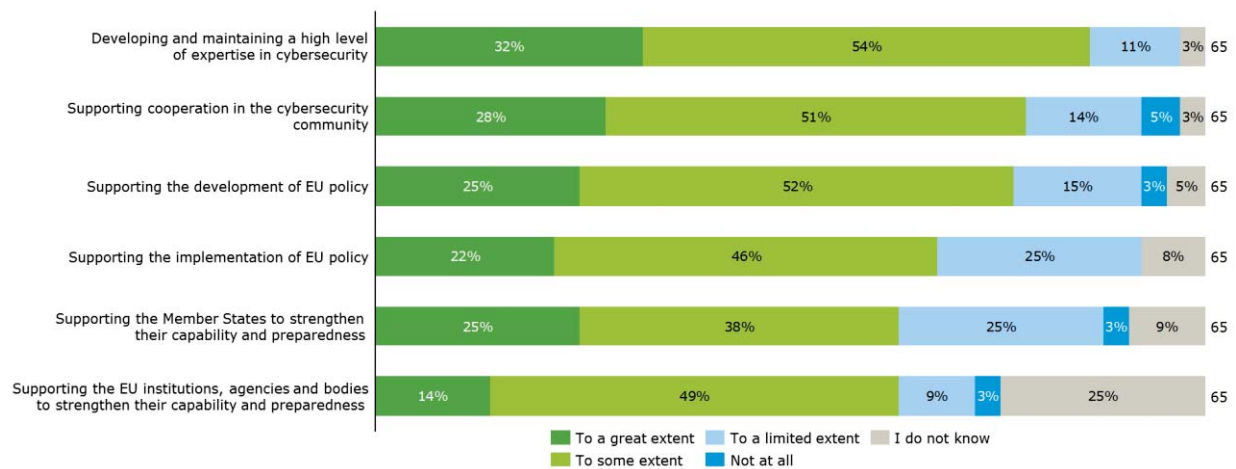
<sup>37</sup> ENISA (2016): Activity report 2015

received during interviews and the workshop was generally positive, while the views on the Cyber Europe exercises were more mixed. Some stakeholders considered their participation in the exercises to be beneficial, whereas others were concerned about the high number of participants making the exercises more complex and slower. The quality of ENISA’s outputs is further discussed in section 3.2.2.7.

**ENISA generally achieves short term KIIs but it is more difficult to establish its contribution to long term objectives.** ENISA sets KIIs for the monitoring of the implementation of the work programmes. In general, these have been achieved according to the annual reports in 2013, 2014 and 2015. Only for a few long term targets set for 2015 the annual report of that year noted that it was too early to judge the degree of achievement. The annual evaluation of 2015 stated that there is a clear pattern in terms of progress, where targets under ENISA’s control (such a high quality, community building, good practice dissemination) are largely achieved. The progress towards more long term objectives looks more uncertain (preparedness to respond to crisis, increase in capacity etc.), as this is highly dependent on contextual factors as well as public and private stakeholders’ engagement and investment. Still, ENISA does achieve some of its targeted objectives and the large majority of stakeholders agree that ENISA makes a contribution to increased NIS across Europe.

**ENISA achieves its objectives but to varying degrees across the different activities.** All respondents to the open public consultation indicated that ENISA had achieved at least some of its targeted objectives to some extent or to a great extent. Respondents were asked to evaluate the extent to which they felt ENISA had achieved the objectives set out in its mandate during the period of 2013-2016. The assessment made by 65 respondents is presented in Figure 10 below. The objective of “developing and maintaining a high level of expertise in cybersecurity” was selected as being achieved to a great extent or to some extent by the highest number of respondents (86% or 56 respondents), followed by “supporting cooperation in the cybersecurity community, e.g. through public-private cooperation, information sharing, enhancing community building, coordinating the Cyber Europe Exercise” (79% or 51 respondents). “Supporting the implementation of EU policy” was selected by all of the respondents from national authorities as being achieved either to some or to a high extent. National authorities generally indicated that ENISA had achieved all its objectives “to some” or “to a large extent” with few respondents selecting “to a limited extent” (3 out of 15 for “supporting the development of EU policy” and 4 out of 15 for “supporting Member states to strengthen their capacity and preparedness”).

Figure 10: Extent to which ENISA has achieved its objectives over 2013-2016, (n=65)



Source: Open public consultation

All respondents to the open public consultation were asked to list what they thought were the main achievements of ENISA over the 2013-2016 period. In total, 55 responses were received. The following points were mentioned by several respondents:

- The coordination of the Cyber Europe Exercise
- The provision of support to CERTs/CSIRTs through training and workshops fostering coordination and exchange.
- ENISA's publications (guidelines and recommendations, threat landscape reports, strategies for incident reporting and crisis management etc.) that were considered as useful to create and update national security frameworks, as well as for reference to policy makers and cyber practitioners.
- Assisting with the promotion of the NIS Directive
- Efforts to increase awareness on cybersecurity via the cybersecurity month.

National authority respondents believed another main achievement was the support ENISA provided to Member States in particular fostering cooperation by sharing of expertise among Member States, information sharing on Art. 13, and support for the implementation of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)<sup>38</sup>. Private enterprises and business associations also commended ENISA's work in fostering public-private cooperation and increasing better cross-sector engagement, providing a degree of "coordination and harmonisation that might have otherwise been missing". They also felt that another main achievement was that ENISA had established itself as a "relevant, neutral reference point of cyber expertise in Europe with demonstrated EU added value". As well as being a source of knowledge that is easily accessible and easy to use covering a wide range of cybersecurity topics.

As concluded in the evaluations of the Agency's activities, ENISA's 2014 and 2015 activities have made important contributions to enhancing cooperation both between Member States of the EU and between related NIS stakeholders. The assessment was made based on survey findings which pointed to the fact that the support from ENISA has contributed to a great extent to enhancing community building in Europe and beyond, increased cooperation of operational communities and improved workflow and communication among stakeholders. Interview results supported these findings, with stakeholders stressing the positive role that ENISA has in bringing people together to discuss and cooperate.<sup>39</sup> In extension of this finding, it is assessed that ENISA has contributed to a great extent to enhancing community building in Europe and beyond.

ENISA's activities contributed to some extent to capacity building, and to varying degrees depending on the stakeholder type. In this regard, the evaluation of ENISA's 2015 activities finds that ENISA's support has allowed for the development of sound and implementable strategies to ensure preparedness, response and recovery in the Member States and contributed to developing capacities in prevention, detection, analysis and response at national level. The findings further suggest that ENISA has assisted in enhancing the capacity of Member States (most notably Member States with fewer resources and capacities) in particular through: the pivotal role it plays in bringing different actors together and building networks; the dissemination of good practices; and the organisation of training sessions (e.g. for CERTs/CSIRTs) on a technical level. The evaluation concluded that the support provided by ENISA was perceived as complementary to that of other public interventions, clearly pointing to a role for ENISA in relation to capacity building.<sup>40</sup> The contribution to capacities of the private sector of ENISA's activities is more uncertain according to the annual evaluations and the interviews conducted in the context of the present evaluation. The 2015 evaluation of ENISA's activities concluded that there was still a long road

<sup>38</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

<sup>39</sup> Ramboll (2016): External evaluation of ENISA – 2015, Final report

<sup>40</sup> Ramboll (2016): External evaluation of ENISA – 2015, Final report

ahead before an EU-level crisis management process was put in place in the cybersecurity area mainly due to a lack of trust among stakeholders, weaknesses and differences in national capabilities and insufficient exchanges of information in “real life”. This conclusion was also reflected in the interviews for the present evaluation.

ENISA’s contribution to the development and maintenance of a high level of expertise of EU actors is limited. On the one hand, evidence from the previous evaluations and the interviews confirm that ENISA’s activities do provide some stakeholders (e.g. critical information infrastructures (CIIs), CERTs/CSIRTs) with advice and assistance. On the other hand, evidence suggests that these activities have not contributed as significantly as intended towards the adoption of methods towards new technologies and enabling the exploitation of the opportunities in emerging technologies.

The contribution towards implementing and developing policies was considered to be the least achieved objective by the interviewed stakeholders. While efforts have been made to prepare for the implementation of the NIS Directive, the Agency is not consistently being involved in all NIS related activities of the Commission. Interviewees from the different Commission DGs indicated that ENISA could be more involved in their process of developing policies. In turn, ENISA’s staff and management noted that they were not always fully aware of all Commission activities related to cybersecurity, most notably considering initiatives of DGs other than DG CNECT.

**Obstacles to achieving the targeted objectives stem from a broad mandate.** When assessing the achievements of the Agency, it becomes clear that a lot of efforts are being made but they are spread over a wide field of responsibility. The fact that cybersecurity is such a broad topic and that ENISA’s stakeholder community is so diverse compounds the issue.

Within the NIS community there is a wide spectrum of expectations towards ENISA across the various stakeholders but with the limited resources at its disposal, ENISA has to set priorities. This means that the Agency is not able to implement all tasks set out in the mandate to the same extent. In the development of the annual work programmes some tasks are prioritised over others. Generally, ENISA implements all the tasks set out in the annual work programmes.

### 3.2.2.2 Benefits of acting at agency level

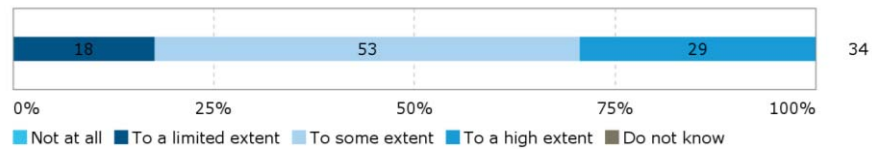
#### **EQ2: What have been the benefits of acting at agency level both from the operational and strategic perspective?**

ENISA has filled a gap by acting as a neutral, independent broker at EU level. It has helped to bring stakeholders of various types and from various sectors together and acted as a bridge between the strategic and operational worlds, thereby contributing to its ultimate goal of increasing network and information security in Europe. That being said, its work programme is heavily influenced by Member State interests and there is scope to increase the Agency’s impact.

**Acting at agency level provides for independence and neutrality.** A number of interviewees across all groups stressed the neutral position of ENISA as an Agency as one of its key strengths – it was seen as providing advice that is not influenced by industry or political interests. This was particularly appreciated by respondents to the open public consultation from private enterprises and business associations, noting that having established itself as a “relevant, neutral point of cyber expertise in Europe” was one of ENISA’s main achievements. The findings of the 2015 evaluation also supported this with the case studies conducted confirming that ENISA’s activities in 2015 were generally relevant to both the public and private sector on national level, in particular since ENISA is an important neutral source of information, in a field where many reports would be written, for example, by providers themselves wanting to sell their own solutions.

**ENISA has acted as a bridge between the strategic and operational worlds.** From an operational perspective, ENISA managed to cover the needs of national CERTs/CSIRTs. A large majority of respondents to the CERT/CSIRT survey (28 out of 34) thought that ENISA covered the needs of CERTs/CSIRTs to a high or to some extent during the 2013-2016 period.

**Figure 11: Extent to which ENISA covered CERTs/CSIRTs' needs over the 2013-2016 period**



Source: CERT/CSIRT survey

From a strategic perspective, ENISA is considered important in its ability to bridge the policy/operational divide through the provision of policy support and the creation of a network of stakeholders from various organisations and sectors. Interviewees from different stakeholder groups perceived the NIS Directive as an opportunity for ENISA to expand this role.

**As an Agency governed by a Management Board made up primarily of Member States, ENISA's work priorities are heavily influenced by the interests of Member States.** Interviewees from the group "users and advisors" and ENISA staff pointed to the fact that Member States were key in determining ENISA's work priorities, sometimes at the expense of the needs and interests of e.g. industry, certain types of Member States (see section 3.2.2.5).

### 3.2.2.3 Contribution to increasing network and information security in Europe

#### **EQ3: To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe? What more could be done?**

The evaluation finds that ENISA has clearly contributed to increasing network and information security in Europe through its various activities and their outputs and results. However, the Agency is limited in its contribution to this goal due to its mandate, its resources and a lack of visibility. A number of suggestions were made on how ENISA could further contribute to NIS in Europe, however these rely on additional resources being at its disposal.

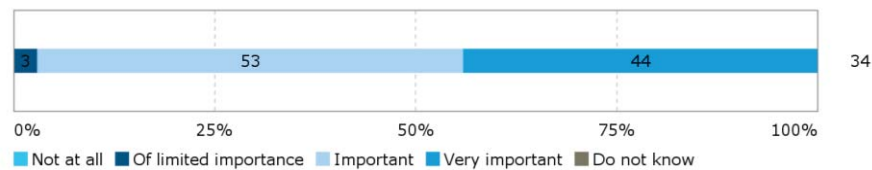
According to the intervention logic (presented in Appendix 1) based on Regulation (EU) No 526/2013, ENISA's work is intended to contribute to a high level of network and information security. The Regulation understands network and information security as "*the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems*" (Article 1.3).

**ENISA has made a clear contribution to the overall goal of increasing network and information security in Europe.** As presented in section 3.2.2.1, ENISA has generally been successful in the implementation of its tasks and the achievement of the KIIs set by the Management Board. The two previous evaluations showed that ENISA clearly contributes to ensuring a high level of NIS in the EU (including by sharing good practices in NIS, as shown in the stakeholder survey carried out by the 2015 evaluation), which should be seen as a strong achievement. A survey conducted among members of ENISA's Management Board, NLOs, the PSG and a small sample of industry stakeholders in the context of the 2014 evaluation, found that 74% of respondents (42 out of 58) agreed or strongly agreed that ENISA contributed to ensuring a high level of NIS within the EU. A strong majority of interviewees in the present study also agreed that ENISA contributed to this overall goal. A number of activities were mentioned through which this

contribution was made, including ENISA’s work on developing networks, the exercises and training activities, awareness raising activities and the provision of the Agency’s expertise.

A more concrete example of the impact of ENISA’s work can be found in the survey of CERTs/CSIRTs, in which respondents were asked about the importance of ENISA’s capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) in 2013-2016. Respondents were very positive as to its importance for CERTs/CSIRTs’ development. As can be seen in Figure 12 below, almost all respondents (33 out of 34) thought that such capacity building activities were either very important or important.

**Figure 12: Importance of ENISA’s capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) in 2013-2016 for CERTs/CSIRTs’ development**



Source: CERT/CSIRT survey

### **There are limits to what ENISA can achieve with regard to increasing NIS in Europe.**

Stakeholders mentioned limitations to the Agency’s effectiveness. These include a lack of visibility, making it difficult to reach the targeted stakeholders with their publications and expertise, and a general underestimation of the relevance of cybersecurity issues by different stakeholders across the EU.

A number of interviewees from the group of “users and advisors” noted that they would not be able to respond to questions regarding ENISA’s impact. This suggests that there is limited visibility of ENISA’s successes.

#### 3.2.2.4 EU-wide centre of expertise and reference point for stakeholders

##### **EQ5: To what extent has ENISA become an EU-wide centre of expertise and a reference point for stakeholders in providing guidance, advice and assistance on issues related to network and information security?**

With the exception of very few stakeholders, ENISA was not described as a centre of expertise or as a reference point for stakeholders in the NIS area. The Agency is more considered as a valuable partner for ensuring coordination across the EU. Its guidelines and reports are used by many stakeholders, but are appreciated for their availability and for coming from an EU Agency rather than purely for the presented expertise. ENISA’s low visibility and perceived limited technical expertise were named as the reasons for this.

### **There is little evidence to suggest that ENISA is being considered as a reference point by its various stakeholders and is recognised for its expertise across the EU.**

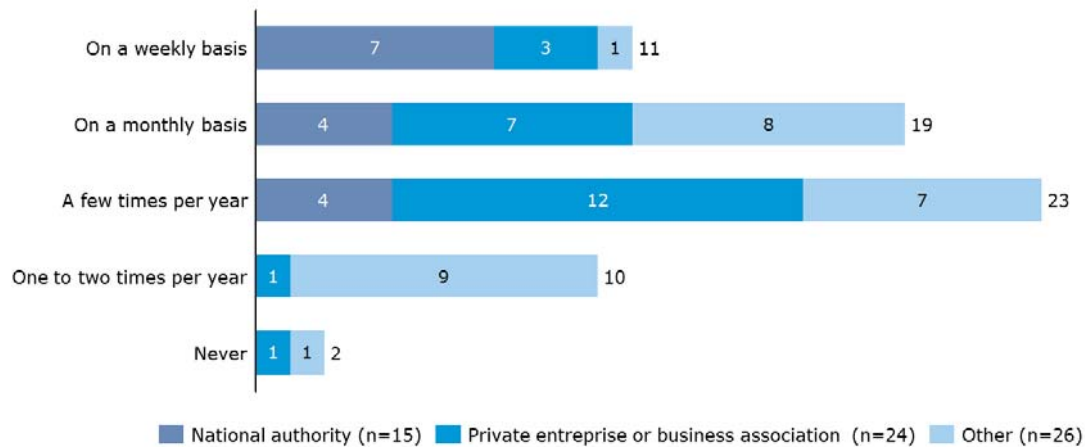
In the interviews only a few stakeholders said that they would consider ENISA to be a centre of expertise. However, Member States and representatives from the EU institutions mostly saw ENISA as a valuable partner at EU level supporting coordination and capacity building. They did not consider ENISA as a source of expert knowledge. Among private sector stakeholders, ENISA has limited visibility and has not become known as a reference point for advice or assistance, as shown by the evaluations of ENISA’s activities in 2014 and 2015, as well as confirmed by the interviews.

Moreover, among the respondents to the open public consultation, the regularity of interaction with ENISA and use of the Agency’s products and services varies between the stakeholders. While 51% (33 out of 65) interacted with ENISA’s products and services a few or only two times per year, 46% of respondents (30) interacted with ENISA on a weekly or a monthly basis. A



comparison across the three groups of respondents shows that national authorities interact with ENISA or use its products and services more regularly than respondents from the group of private enterprises and business associations or other respondents (see Figure 16). Among national authority respondents, 47% interact on a weekly basis, while the largest proportion (50%) of private enterprise and business association respondents do so a few times per year and 35 % of other respondents interact one to two times per year.

**Figure 13: Frequency of interact with ENISA or usage ENISA’s products and services, (n=65)**

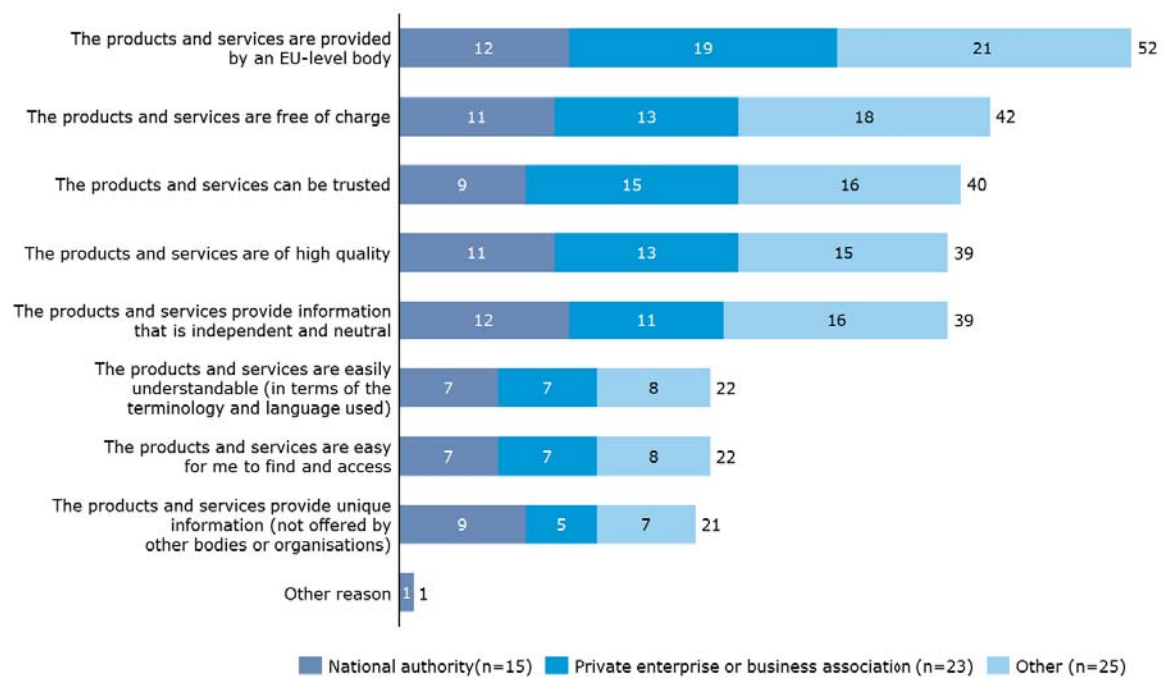


Source: Open public consultation

From a list of eight of ENISA’s products and services, the most frequently mentioned as having been used by respondents to the open public consultation in the period 2013-2016 were ENISA’s “Guidelines & recommendations, including on standards” (90% or 56 respondents) and the “Reports (e.g. NIS Threat Landscape) & Research Publications” (86% or 53 respondents). This reflects some interest by the stakeholders in the publications of ENISA. Responses were very similar across the three respondent groups: national authorities, private enterprises and business associations and other. Products and services less frequently mentioned as being used were “Article 14 requests” (which are only available to Member States and the EU institutions), “training material or toolkit” (in particular rarely indicated by private enterprises or business associations as being used) and “training or workshop opportunities” were least indicated as being used by ‘other’ respondents.

The most frequently given reasons for using ENISA’s products were “The products and services are provided by an EU-level body” (83% or 52 respondents), “The products and services are free of charge” (67% or 42 respondents) and “The products and services can be trusted” (63% or 40 respondents). Respondents were asked to select out of a list of eight options. This suggests that the expertise presented in ENISA’s publications and services is recognised, but is a secondary consideration relative to their availability and the trustworthiness which seem to stem from the fact that it is an EU level body.

**Figure 14: Reason for using ENISA’s products/services, (n=63), multiple choice question**



Source: Open public consultation

**Little visibility and lack of expertise impede ENISA becoming a centre of expertise and a reference point for stakeholders.** Most importantly, compared to other EU agencies, ENISA has little visibility and most stakeholders doubted that ENISA had been able to develop its own brand as compared to Frontex or Europol (EC3). Without being sufficiently known across the EU, it will not be possible for ENISA to be considered as a central source of guidance, advice and assistance. The 2015 evaluation of ENISA’s activities found that the Agency could improve its effectiveness by ensuring better dissemination of events and publications in order to reach a larger audience and increase its visibility. Interviewees also criticised the Agency for its limited expertise, in particular in the technical fields. The findings also show that ENISA struggles to hire experts which can be explained by a combination of factors: there are general difficulties across the public sector to compete with the private cybersecurity sector when trying to hire experts; ENISA’s human resource policies over the period 2013-2016 did not function well (see section 3.2.2.8.) and, for some experts, Greece as a location seems to be less attractive, e.g. in terms of spouses being able to find work (see section 3.2.2.10).

3.2.2.5 Effectiveness at setting its work priorities

**EQ6: How effectively has the Agency managed to set its work priorities?**  
 ENISA sets its annual work programme one year ahead – the work priorities are determined by the Management Board with input from ENISA’s management and to a limited extent the PSG. As a result, the work priorities primarily reflect the interests and needs of Member States (as ENISA’s main clients) over those of other stakeholders, e.g. industry, the Commission and the EU more widely. Due to divergences in priorities at national level, the work programme often reflects what is least controversial to Member States and risks representing the lowest common denominator.

Changes in the work programmes from one year to the next, linked to ENISA’s broad mandate, mean that there is a lack of continuity in many of ENISA’s activities from one year to the next, namely due to the annual (rather than multi-annual) nature of its programming.

**ENISA’s work priorities primarily reflect the interests of Member States and not necessarily the needs of all relevant stakeholders; they are set by the Management Board in an annual work programme with input from ENISA.** ENISA’s work is based on annual planning. The work programmes are set up in consultation with the Management Board which is primarily made up of Member States, but also representatives of the Commission and observers; Member States provide comments on the programme that is initially set out in draft form by ENISA. PSG members have a lesser say than in the past – their views are expressed through the ad hoc group of certain Member State representatives and PSG members.<sup>41</sup> The work programme’s structure underwent changes in 2015 – in 2013 and 2014 the work was divided across three work streams that changed on an annual basis with given activities being planned within these, while from 2015 onwards strategic objectives were set out that remain the same year-on-year. Additionally, Horizontal Operational Activities are conducted. KIIs are set by the Management Board for the work plan activities - they are followed up on through the annual activity reports. The process was judged by a few interviewees as being long, tedious, time consuming and burdensome, occupying much of ENISA managements’ time when it is being set.

When commenting on the effectiveness of the process, ENISA staff and users and advisors, as well as some PSG members pointed to the fact that Member States were key in determining ENISA’s work priorities, sometimes at the expense of the needs and interests of other stakeholders, e.g. industry, the Commission and the EU more broadly. Moreover, it was felt that due to competing interests among larger, more experienced Member States and smaller, less resource-rich Member States, ENISA’s work programme risked representing the lowest common denominator and being diluted. Standardisation and certification were referred to as two areas where Member States had their own national plans and resist ENISA getting involved. Some areas that ENISA should be focussing on more as priority areas than is currently the case, according to industry stakeholders in particular, included the Internet of Things, the move to big data and machine intelligence, certification, becoming more active in the educational field, e.g. by supporting the creation of Massive Open Online Courses (MOOC) in the field of cybersecurity.

It was suggested that more room could be integrated into ENISA’s work programme to allow for it to respond to the ad hoc needs of the Commission and to unforeseeable events/needs. A few interviewees from ENISA staff and ENISA’s users and advisors suggested that ENISA itself could be given the possibility to determine part of the work programme.

**ENISA’s work programme covers a wide range of activities and sectors, and there is a lack of continuity in many of its activities from one year to the next.** The Cyber Europe Exercises and the threat landscape were cited as the two main activities that are repeated regularly; others change on an annual basis, leading to a lack of continuity and the inability for ENISA staff to develop in-depth expertise in given areas. This is also a reflection of the annual (rather than multi-annual) nature of the way ENISA sets its work priorities. The 2015 evaluation supported these findings with the broad mandate of the Agency and the variety of tasks it seeks to fulfil being perceived by stakeholders as a limiting factor to its effectiveness. In the open public consultation, stakeholders suggested that ENISA should keep a clearer focus on priorities and avoid taking on additional tasks that represent a burden for the staff members.

#### 3.2.2.6 Tackling upcoming, unplanned issues

**EQ7: How effectively does the Agency tackle important upcoming, unplanned issues derived from the demands of its constituencies and/or EU policy priorities?**

<sup>41</sup> The PSG representatives are not formal members of the Management Board and primarily have an advisory role vis-à-vis the Executive Director.

ENISA is able to respond to upcoming, unplanned issues based on stakeholder demands or EU policy priorities through Article 14 requests and amendments to its work programme. These options are considered to be effective, though there is room for more flexibility in order to further consider the needs of stakeholders other than Member States, in particular those of the CERT/CSIRT community, and resource constraints mean it has to prioritise.

**Article 14 of ENISA’s Regulation allows it to respond to the upcoming needs of its key stakeholders to a degree** Based on Article 14, the European Parliament, the Council, the European Commission and a competent body appointed by a Member State can submit a request for advice or assistance falling within the Agency’s objectives and tasks. These requests have to be addressed to the Executive Director who then informs the Management Board and the Executive Board to take a decision whether the requested advice or assistance can be provided. Requests can be within the scope of what ENISA already does (e.g. the provision of a specific training course) or cover new areas as long as they are within the remit of the Agency’s mandate. The stakeholders concerned expressed satisfaction with the provision. However, ENISA staff and management noted that it was not possible to respond to all requests within the limits of the Agency’s budget and human resources. Therefore, requests had to be carefully considered and some requests were not responded to.

Between 2013 and 2016, ENISA responded to a total of 63 requests submitted under Article 14. Over the years 2014 and 2015, requests were received from 17 different Member States, the Commission, the Council of the European Union, the European External Action Service, CEPOL and a third country. Member States’ requests primarily concerned training for CERTs/CSIRTs or other public bodies. Requests also concerned the implementation of topical workshops, support with developing a cybersecurity strategy for an entire Member State or on specific topics.<sup>42</sup> Among the respondents to the open public consultation, “Article 14 requests” were one of the services that were less frequently mentioned as being used. Only five out of 15 responding national authorities reported that they had used Article 14 requests over the period 2013-2016. However, the actual number of different Member States having used the services shows that in fact, the requests are used more often. On average, the response to one request costs EUR 15,000. There is however no clear relation between the number of requests responded to per year and the total costs.

**Table 15: Overview of Article 14 requests**

	2013	2014	2015	2016
<b>Number of new Article 14 requests</b>	13	12	23	15
<b>Total cost of Article 14 requests</b>	€ 200,000	€ 317,637	€ 210,957	€ 229,107

The presented data shows that Article 14 requests are employed to receive support from ENISA and the Agency is able to use them as a means to respond to needs that were not foreseen at the moment the work programme was set up.

**ENISA’s work programme and activities can be amended to allow the Agency to react to upcoming, unplanned events.** Although adopted well in advance, ENISA’s work programmes tend to evolve during their year of implementation. A structured process is in place allowing the Management Board to modify the work programme and reallocate financial and human resources when needed. This flexibility was positively viewed by a variety of stakeholders. However, there is room for more flexibility in order to further consider the needs of stakeholders other than Member States. The fact that the work programme needs to be drafted one year in advance, and does not allow for greater flexibility to respond to ad hoc requests, was perceived by a number of

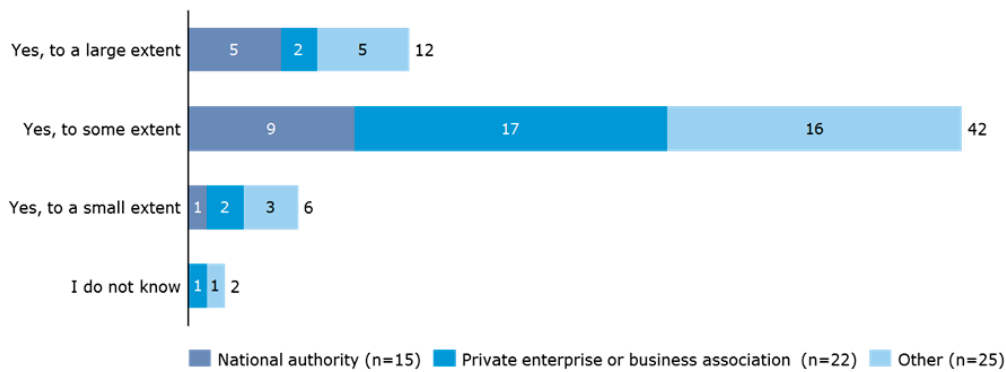
<sup>42</sup> ENISA (2016) Activity Report 2015 and ENISA (2015): Activity Report 2014.

interviewees as a limiting factor to the Agency’s effectiveness and ability to respond in such a fast paced area as NIS with changing political priorities at EU level. A few survey respondents pointed to this rigidity in their comments on ENISA’s organisational set-up, stating that it blocked resources and did not allow the Agency to contribute to emerging issues. It was suggested that part of ENISA’s budget should be set aside to allow it to respond to emerging challenges.

However, additional activities (which fall outside the work programme) undertaken by ENISA’s staff reflect its ability to tackle unplanned issues. This includes the preparation of Info Notes or ENISA internally deciding to produce papers in response to policy discussions as part of its role as an advisor to the EU institutions. As these activities are not foreseen in the Agency’s work programmes, they rely on the motivation of ENISA’s staff to take on additional tasks.

Moreover, among the respondents to the open public consultation, 87% (54 respondents) agreed that ENISA’s products and services over 2013-2016 had to a large or to some extent responded to the emerging needs of the cybersecurity community in a timely manner. As Figure 15 below shows, this was a consistent assessment across all respondent categories.

**Figure 15: Extent to which ENISA’s products/services over 2013-2016 responded to emerging needs of the cyber-security community in a timely manner, (n=62)**



Source: Open public consultation

**Limitations in ENISA’s flexibility to respond to unforeseen issues stem from the Agency’s limited resources.** With generally scarce resources, ENISA’s management needs to carefully consider whether and to what extent Article 14 requests can be covered. According to interviewees, this can lead to situations where there is competition between the completion of the work programme as agreed with the Member States and any ad hoc request submitted by an EU institution. In fact, the CERT/CSIRT community expressed little satisfaction with ENISA’s ability to react to unplanned issues. Interviewees from the Member States and EU institutions and bodies suggested that they would seek support within their own community in case of unplanned, short-term requests rather than address these to ENISA. Due to its limited resources, it was judged that the Agency would respond to ad hoc requests with significant delay or not at all. In particular, in the context of ENISA’s new responsibilities under the NIS Directive, an important amount of the Agency’s budget will be fixed and cannot be moved to respond to unplanned issues.

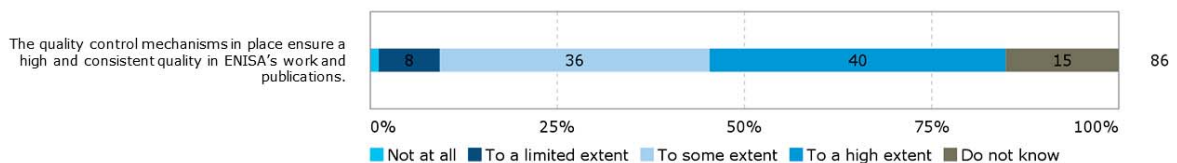
3.2.2.7 Quality level of tasks over time

**EQ8: Does the Agency consistently perform the same tasks with the same quality level over time?**  
 Overall, the tasks performed by ENISA meet minimum quality expectations, though mixed feedback was provided on the quality and utility of its reports. Moreover, the evaluation identified a varying degree of utility of the Agency’s outputs depending on the needs of the different stakeholder groups.

**ENISA’s performance generally meets quality standards but does not seem to exceed these.** Interviewed stakeholders provided mixed feedback on the quality level of the Agency’s work, notably of its reports. A number of interviewees – across all stakeholder groups - suggested that the degree of usefulness and quality of ENISA’s reports/publications varied and that they did not necessarily “bring a unique selling point”. While a few Member State interviewees considered the reports which summarise information from several Member States and provide an independent EU perspective to be very useful, others suggested that the utility varied depending on what was available at national level. Among the open public consultation respondents, 62% (39 out of 63) indicated that they used ENISA’s products and services because they were of high quality. Among national authorities, 73% (11 out of 15) indicated to use products and services due to their high quality. This was not among the most selected reasons by respondents, but national authorities in particular selected this response. It was suggested by one interviewee that to improve the quality of reports, ENISA could draw more on the expertise of national cybersecurity experts from national authorities, academics and the private sector to assist them in developing reports/publications in-house through a peer review process; such a practice would allow it to draw on a wider net of expertise to produce more tailored outputs. Another interviewee suggested that there could be a more structured approach to the selection of expert contributors to publications, thereby ensuring that this is a more European undertaking representing the cybersecurity point of view of Europe. Respondents to the open public consultation also suggested that ENISA could increase the quality of publications by covering less topics but more in-depth. In general, stakeholders showed to be very understanding when it came to smaller issues such as difficulties at the start of a cyber exercise.

As can be seen in Figure 16 below, the quality control mechanisms in place were seen by 76% of respondents to the survey of ENISA’s staff and direct stakeholders (65 out of 86) as ensuring a high and consistent quality in ENISA’s work and publications “to some” or “to a high extent”. They were seen as doing so only “to a limited extent” or “not at all” by 9% of respondents (8 out of 86). ENISA staff were slightly more critical than the average in considering the quality control mechanisms as only ensuring such quality “to a limited extent” or “not at all” (14%).

**Figure 16: Extent of agreement or disagreement with the following statement on quality control mechanisms**



Source: Survey of ENISA staff and direct stakeholders

Seven survey respondents provided additional comments, all of them referring to low or non-existent quality control mechanisms.

3.2.2.8 ENISA’s effectiveness considering its governance structure, organisational structure and HR policies

**EQ11: How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to effectiveness in the work of the agency?**

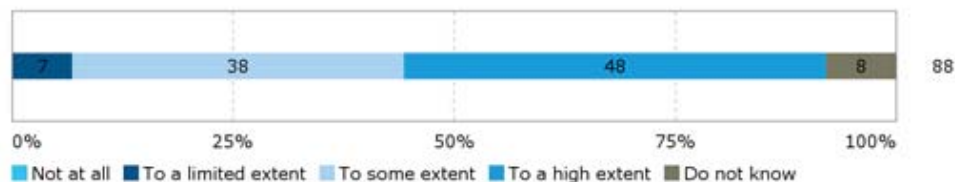
**ENISA’s governance structure**, with a Management Board, an Executive Board and the PSG, is conducive to the effectiveness of its work, though there is room to increase its representativeness and effectiveness by, for example, giving the PSG a more formal role, delegating power within the Management Board to smaller groups, allowing the Executive Board to take on a more pro-active role, and formalising the role of the NLO network.

Its **internal organisational structure** contributes to the effectiveness of its work through its management practices, small size which leads to a lack of complexity, separation along thematic lines and relatively flat structure. That being said, reorganisations, while necessary to ensure renewal, risk posing a limit to its effectiveness when too frequent; here a balance is necessary.

The **human resource (HR) policies and practices** of ENISA are a key limiter to effectiveness in that ENISA had weak HR policies and practices in place over the 2013-2016 period, with a formal HR department only being set up in late 2016. ENISA also suffers from difficulty recruiting and retaining staff due to both internal (i.e. slow recruitment procedures in a fast-paced, competitive environment; a lack of career progression prospects) and external factors (i.e. constraining staff management rules (e.g. number of contract agents (CAs) versus temporary agents (TAs)); an expertise shortfall in the sector; a lack of competitive salaries in an area that is dominated by demand from the private sector).

**ENISA’s governance structure is conducive to the effectiveness of its work.** The current governance structure, with a Management Board, an Executive Board and the PSG Group (see section 1.2.2 for a description of the governance structure), was seen as conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives) by the large majority of ENISA’s direct stakeholders (85% or 75 out of 88 survey respondents) (see Figure 17 below). The interviews with staff and direct stakeholders supported this finding, suggesting that the structure “worked well”, “was reasonable”, “was adequate”, and represented well the views of different stakeholders.

**Figure 17: Extent of agreement or disagreement with the following statement: To what extent do you agree/disagree with the following statement: The current governance structure, with a Management Board, an Executive Board and the PSG is conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives)?**



Source: Survey of ENISA staff and direct stakeholders

Key areas for improvement referred to by interviewed stakeholders concerned increasing the representativeness/effectiveness of the governance structure by:

- **Giving the PSG a more formal role:** While it was acknowledged that Member States were ENISA’s main client and it therefore made sense for them to be the key players in the governance structure, it was also stated that “as [ENISA is] an internal market agency, the role of Member States versus the rest [e.g. industry] could be slightly more balanced”. To ensure this balance, a few interviewees from ENISA staff and among the direct stakeholders suggested giving the PSG (industry) a more formal role and having it feed more into the Management Board’s plenary meetings<sup>43</sup>.
- **Delegating power within the Management Board to smaller groups:** The Management Board functions in a traditional manner, giving one place and one vote per Member State in plenary meetings. There are different levels of engagement and agendas among the Member States, and ENISA could consider doing like in other agencies and create sub-sets of the

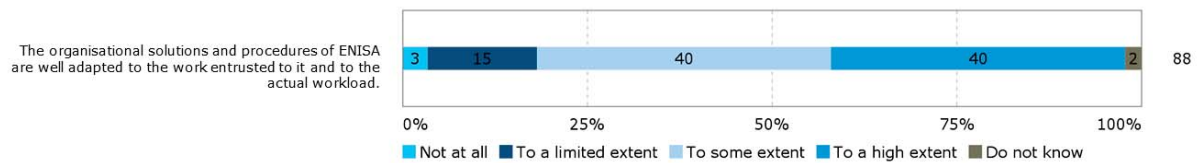
<sup>43</sup> Until 2013 (i.e. ENISA’s mandate revision) there were three Management Board members representing consumers, industry and academia - they had no voting rights but had a voice; this was no longer the case at the time of writing. Through a non-formal approach, there is an attempt for three rapporteurs from the PSG to attend the Management Board meetings to have a voice. The PSG has an advisory role relative to the Executive Board and the Management Board listened to/exchanged views with them through an ad hoc group of Member States and PSG representatives.

Management Board to discuss given topics according to needs and the level of interest before discussing it in plenary form to make the process more streamlined and effective. This has been done with the Executive Board to a certain extent, but it can only prepare advice and assist the Management Board so it is confined to administrative, not policy matters.

- **Providing a more pro-active role to the Executive Board:** The addition of an Executive Board was seen as a positive development, though one interviewee suggested that the structure could be streamlined so that the Executive Board could react to a certain need when it arose and be used in more areas to ensure further flexibility.
- **Formalising the role of the NLO network:** The NLO network was also viewed as a positive element of the governance structure, but it was felt that its role needed to be more formalised<sup>44</sup>. The findings of the 2015 evaluation point to the fact that different NLOs view their role differently and are more or less active at, e.g. disseminating ENISA’s publications to national stakeholders.

**ENISA’s internal organisational structure was overall perceived as contributing to the effectiveness of its work, though frequent reorganisations limited its effectiveness.** A high proportion of respondents to the survey (80% - 70 out of 88) saw ENISA’s organisational solutions and procedures as adequate to some or to a high extent (see Figure 18 below). However, ENISA staff (including management) was more critical of the organisational solutions and procedures relative to the direct stakeholders - a quarter (25%) considered them to be only adequate to a limited extent or not adequate at all. Frequent internal reorganisations, limited professional development opportunities and an unclear evidence base being used for decisions related to the allocation of work to given individuals were cited as some of the problems faced.

**Figure 18: Extent of agreement or disagreement with statement regarding ENISA’s organisational solutions and procedures**



Source: Survey of ENISA staff and direct stakeholders

The interviews with staff and Executive and Management Board members supported these findings with the internal organisational structure being qualified as “adequate for a small organisation”, “rather flat and with an open atmosphere”, “not very hierarchical”, “not too complex because of the small size of the teams”, “the separation along thematic lines working well”, and the ability to avoid overlap by working together. Should the Agency grow in size, it was suggested that a further clustering of the operational department may be necessary along the lines of national agencies like ANSSI, the German Federal Office for Information Security (BSI) etc. Moreover, reference was made to organisational reorganisations leading to a lack of continuity in activities and dissatisfaction among staff. However, views were also expressed as to the necessity of reorganisation for renewal, e.g. the end 2016 reorganisation involved bringing in a “stakeholder relations” aspect to ENISA’s architecture to support less technical aspect to their work/communications.

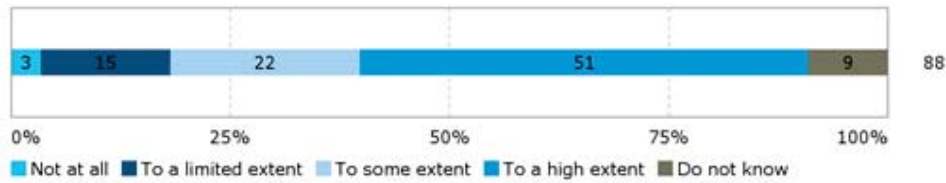
Moreover, a majority of survey respondents (73% or 64 out of 88 respondents) saw ENISA’s management practices as conducive to creating an effective organisation (i.e. in terms of meeting its objectives) to some or to a high extent. Management Board members were generally more positive than the other stakeholders, with 63% indicating that ENISA’s management practices are conducive to creating an effective organisation “to a high extent”. Some concerns were expressed by respondents who rated these practices more negatively, citing unjustified decisions, the

<sup>44</sup> The NLO network is not defined in the ENISA Regulation.



expression of personal agendas and ENISA staff not being allowed to express themselves fully and freely as reasons for this assessment.

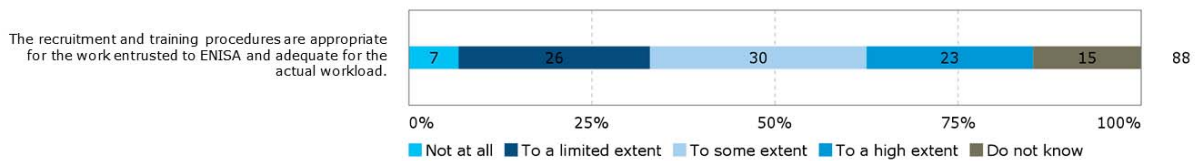
**Figure 19: Extent of agreement or disagreement with the following statement: ENISA’s management practices are conducive to creating an effective organisation (i.e. in terms of meeting its objectives)?**



Source: Survey of ENISA staff and direct stakeholders

**ENISA had limited formal HR policies and practices over the 2013-2016 period.** While the recruitment and training procedures were seen as appropriate to some or to a high extent by 52% of respondents to the survey to ENISA staff and direct stakeholders (46 out of 88), they were seen by 33% of respondents (29 out of 88) as not being appropriate or only being appropriate to a limited extent for ENISA’s workload (see Figure 20 below). ENISA staff (including management) were more critical than the direct stakeholders vis-à-vis the recruitment and training procedures, with more than half of them (52%) regarding them as only adequate to a limited extent or not at all. Problems linked to the recruitment process were mentioned by 13 respondents. They criticized the process for being too slow and therefore not being adapted to the cybersecurity domain. It was stated that technical experts were being sought out heavily in this area and could not wait so long for a positive answer or a confirmation from ENISA. The lack of training that the staff experienced over the past five years due to the Agency not having an HR office was the second most mentioned issue, with 12 respondents providing comments on this topic. In the field of cybersecurity, which evolves fast, a lack of training was perceived as very detrimental as it did not allow ENISA staff to stay up to date with the most recent developments. In contrast to these findings, the 2013 and 2014 annual reports state that the Agency complies with the three assessment criteria for the internal control system, where the first criteria is “staff that have the requisite knowledge and skills”.<sup>45</sup>

**Figure 20: Extent of agreement or disagreement with statement regarding ENISA’s recruitment and training procedures**



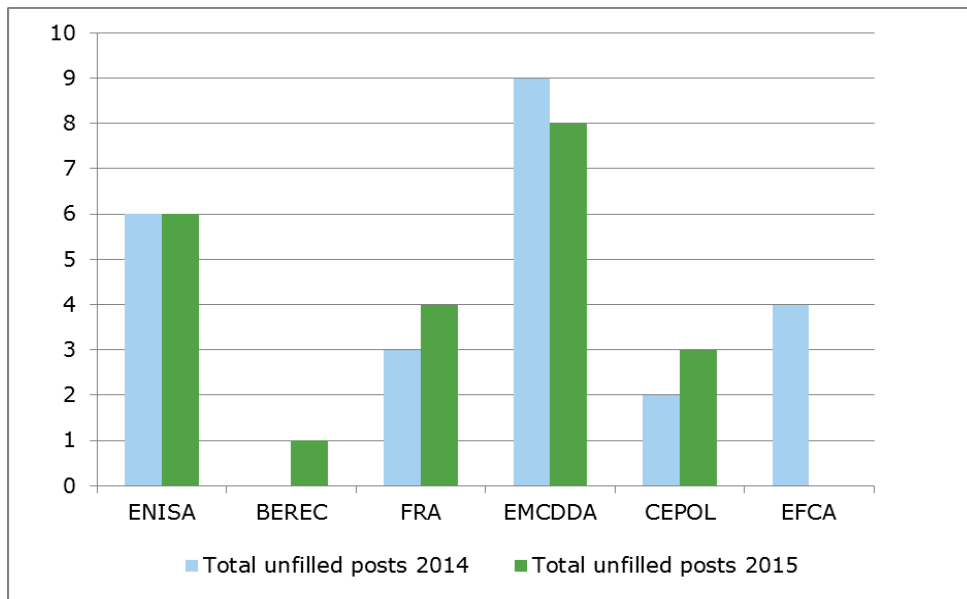
Source: Survey of ENISA staff and direct stakeholders

The interviews with ENISA staff and management revealed that ENISA has weak HR policies and practices in place, with a formal HR department only being set up in late 2016. The appointment of a formal HR manager was very positively viewed and hopes were expressed by many interviewees that HR practices and processes would be prioritised further in the future.

**ENISA has difficulty recruiting and retaining staff.** The recruitment issues that ENISA faces are more significant than in most of the other EU agencies and bodies that ENISA was compared to as part of the benchmarking exercise. The data presented below, which compares the share of unfilled staff posts of 2014 and 2015 across a selection of EU agencies and bodies, points to the fact that ENISA has been unable to fill the same number of posts over the two year period and is the agency with the second highest number of unfilled positions.

<sup>45</sup> Annual activity report 2013, p.40; Annual activity report 2014, p.59

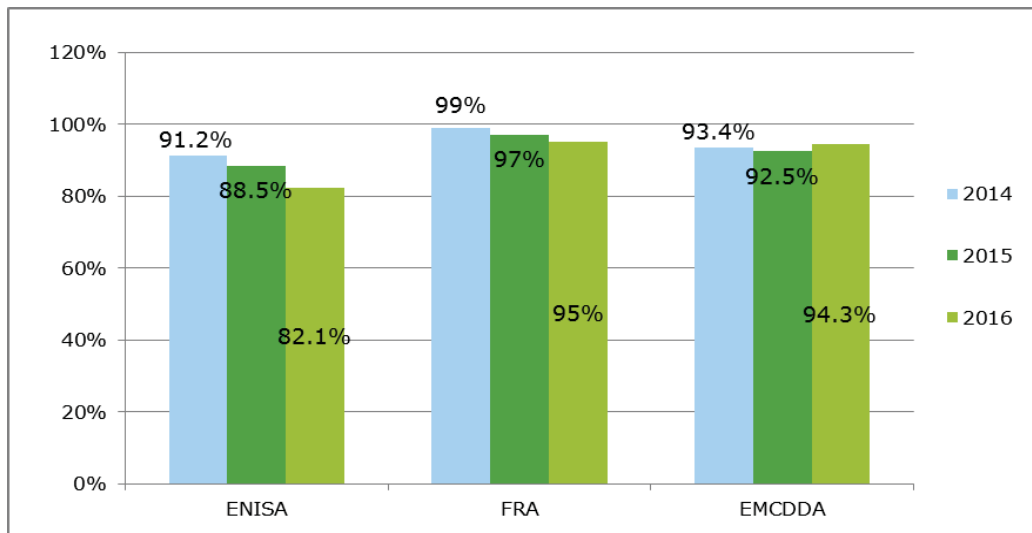
**Figure 21 : Comparison of share of unfilled staff posts for a selection of EU agencies, 2014 and 2015**



Source: Source of data: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III Bodies set up by the EU and having legal personality and Public-Private Partnership.

The same development is also visible in Figure 22. ENISA’s share of filled staff positions has gradually decreased in comparison to FRA and EMCDDA who were able to maintain a fairly consistent percentage of filled positions across 2014-2016.

**Figure 22: Compared share of staff positions filled on an annual basis for ENISA, FRA, and EMCDDA, 2014-2016**



Source: Data gathered through secondary sources and received by ENISA, FRA and EMCDDA.

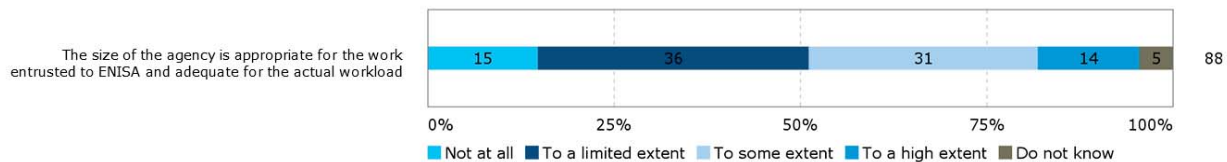
**A number of factors have been identified that lead to ENISA’s issues in recruitment and retaining staff.** The interviews with ENISA staff and management pointed to the fact that ENISA has difficulty recruiting and retaining staff due to a number of factors including:

- constraining staff management rules (e.g. number of CAs versus TAs);
- an expertise shortfall in the sector;
- a lack of competitive salaries and attractive contract conditions in an area that is dominated by demand from the private sector;
- slow recruitment procedures in a fast-paced, competitive environment;

- a lack of career progression prospects due to the size of the Agency and limited turnover at the Head of Unit level;
- perceived barriers to integration for experts from outside Greece, including difficulties for spouses to find work (due to the language barrier, the economic crisis), and insufficient schooling options

It was further mentioned that in other public sector organisations a more flexible structure has been created to keep people (e.g. legislation has been introduced to pay people more in a number of Member States, being more adaptable in the work arrangements offered like teleworking, offering a train package, or packages for the children of staff), but doing this within the confines of the EU institutions and legislation proves a challenge. This was also confirmed by ENISA’s annual activity reports, where the main reasons for difficulties in recruiting and retention are attributed to the types of post that are being offered (CA posts), the low coefficient factor which applies to salaries of ENISA employees in Greece (AAR:2015:50), and the absence of international schooling for the children of Agency staff (AAR:2014: 31, AAR:2015:50).<sup>46</sup> The survey also supported this finding when respondents were asked about the size of the Agency, which was the element of ENISA’s organisational setup that was judged the most strongly by survey respondents (Figure 23 below).

**Figure 23: To what extent do you agree/disagree with the statements below regarding ENISA?**



Source: Survey of ENISA staff and direct stakeholders

ENISA staff (including management) was much more pessimistic about the size of the Agency being adequate than other respondent types, with 61% of them regarding it as adequate only to a limited extent or not at all. A large number of those respondents (35) that were more negative in their assessment referred to the need to have more staff (this was mentioned by a variety of respondent types, including six Management and Executive Board members, 21 ENISA staff members, two NLOs and five PSG members). They called for the need for “more operational experts” and expressed their concern related to hiring being frozen. They explained in detail the difficulties faced in recruiting staff willing to work in Greece and the negative impact on hiring of the lack of facilities for international families in Heraklion and Athens.

The table below presents an overview of ENISA’s staff composition. A significant increase can be noted between 2014 and 2015 in the number of CA.

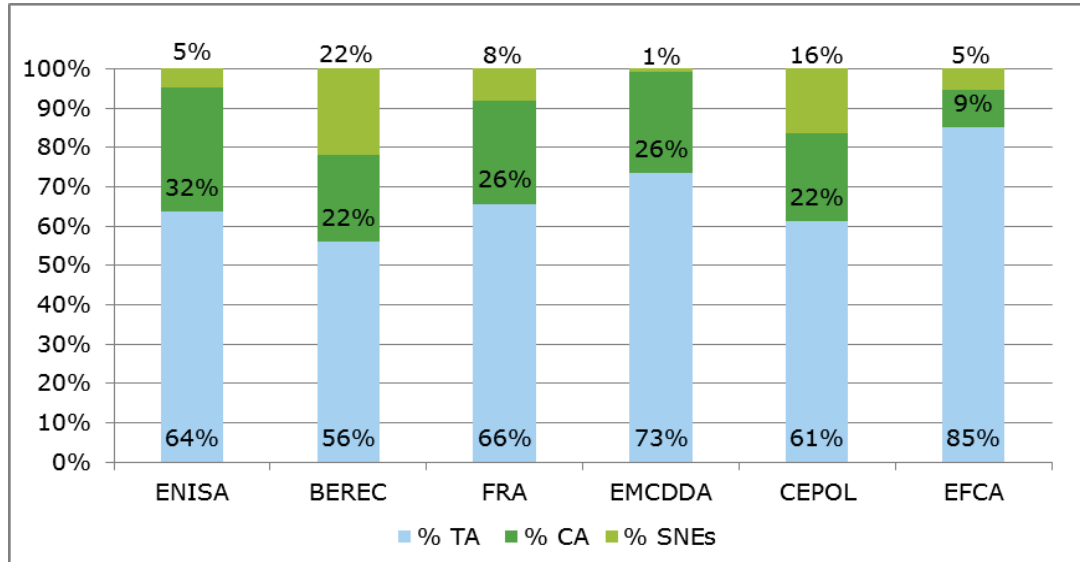
**Table 16: Staff by category end of year**

Staff category	2011	2012	2013	2014	2015
<b>Administrators</b>	26	27	27	34	32
<b>Assistants</b>	15	15	16	14	16
<b>Contract agents</b>	13	12	13	15	24
<b>Seconded national experts</b>	4	4	3	5	3
<b>Total</b>	<b>58</b>	<b>58</b>	<b>59</b>	<b>68</b>	<b>75</b>

<sup>46</sup> These issues are not raised in the 2013 annual activity report, except for a reference to a shortage of staff in connection with the Internal Control Coordinator role. Furthermore, this report states that “adequate measures” are in place to ensure business continuity, also in relation to staff (sick-leave, holidays, etc.) (AAR:2013:38).

**A comparison with other EU agencies and bodies also shows the increasing reliance within ENISA on CAs and a low number of seconded national experts (SNEs).** As presented in Figure 24, ENISA has the highest share of CAs among the agencies and bodies considered as part of the benchmarking exercise conducted for this study. In addition, ENISA employs comparably few SNEs. In interviews, a need was expressed to ensure better exchange between ENISA and the Member States. An increase in the number of SNEs up to the level of other agencies could be a response to this request.

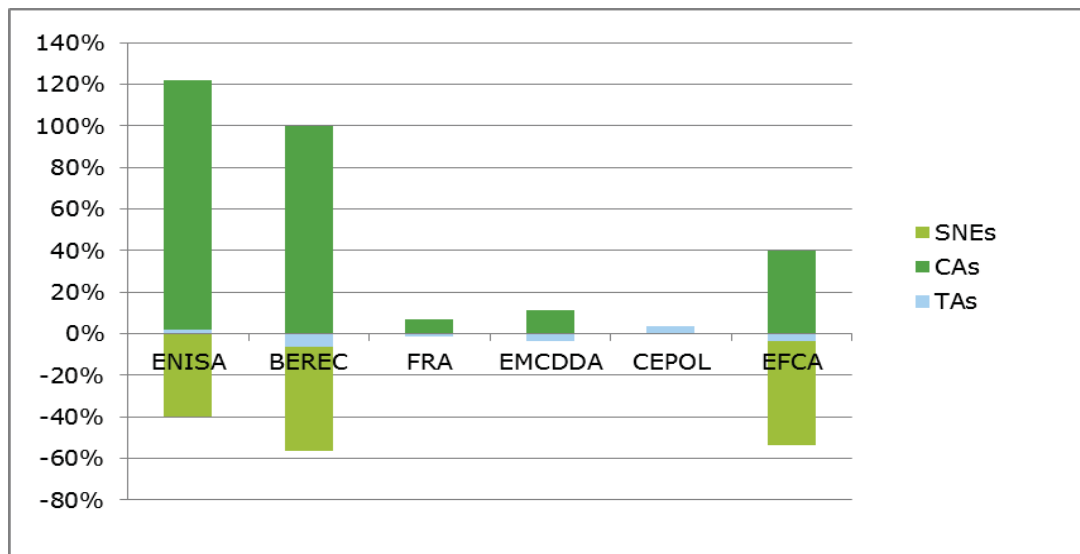
**Figure 24: Average distribution over staff categories, 2014-2016**



Source: presentation by Ramboll, data from European Commission: Draft General Budget of the European Union for the financial year 2017 - Working Document Part III

Over the period 2014-2016, ENISA had the highest percentage increase of CAs compared to the other agencies, reflecting the efforts to reduce staff expenditure. The share increased by 120% for ENISA. As presented in Figure 25 below, BEREC and the EFCA went through a very similar development between 2014 and 2016 in which some of the SNE positions were replaced with CAs.

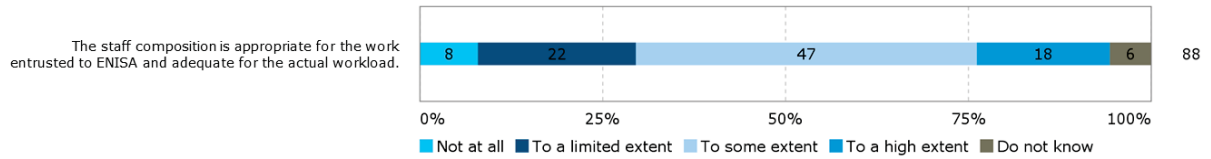
**Figure 25: Percentage change in budget allocations for different staff categories, 2014-2016**



Source: presentation by Ramboll, data from European Commission: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III

Nevertheless, 65% of respondents to the survey to ENISA staff and direct stakeholders (57 out of 88) saw staff composition as adequate for ENISA’s work to some or to a high extent and 30% of respondents (26 out of 88) saw it as only adequate to some extent or not at all (see Figure 26 below). ENISA staff (including management) were more likely to express a more negative view than the direct stakeholders. A number of respondents felt that there was a need to develop internal expertise through the hiring of more senior staff. The balance between administrative staff and operational staff was also seen as an issue by seven respondents, who said that there was a clear need for more technical staff hires. Finally, one respondent expressed the importance for ENISA staff being more geographically representative of the EU; this view was also supported in the interviews.

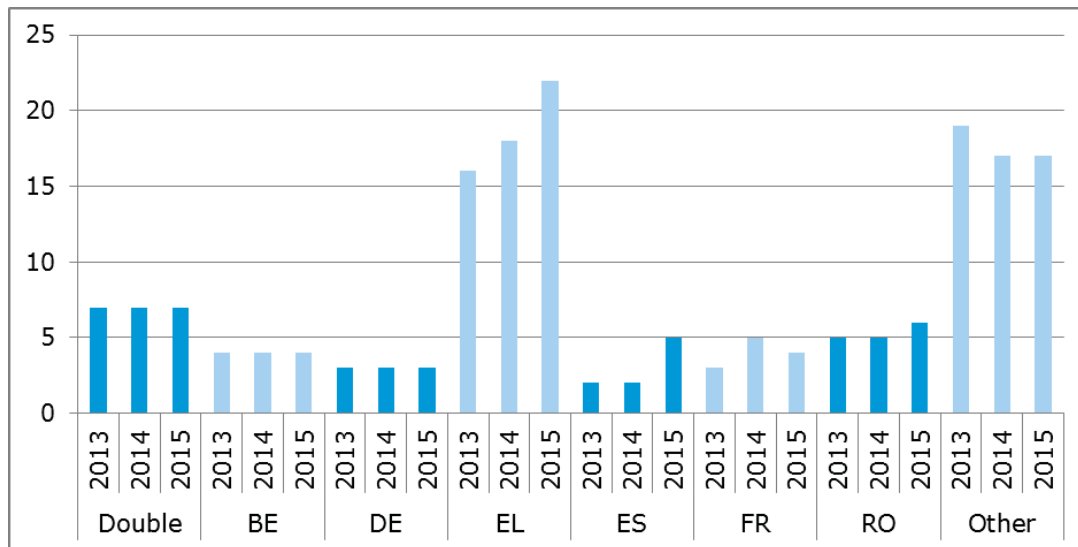
**Figure 26: Extent of agreement or disagreement with statement regarding ENISA’s staff composition**



Source: Survey of ENISA staff and direct stakeholders

Vacancies are difficult to fill with the current salary level (basic level for the functional area concerned is 2,476.74 EUR according to vacancy announcements) and limited benefits or allowances. As a consequence, most applicants are either Greek nationals and/or from other parts of Southern Europe, with very few applicants from northern Europe. This is reflected in the staff composition of the Agency (presented in Figure 27 below), with approximately 32% of staff being Greek nationals in 2015.

**Figure 27: Nationality of staff members (2013-2015)**



Source: Ramboll Management Consulting based on data from ENISA annual reports

As one interviewee put it: “To compete better, we need to put the HR department at a higher level; vacancy notices should be quicker; we could provide better topics (could be more interesting in our job offers); and in general we should provide a more competitive package in terms of medical scheme and other various things”. Another suggested that staff rotations between the EU agencies and with the Commission to make the work more attractive and to bring in new people qualified to work at a higher career level would be a plus.

**The findings of the evaluations of ENISA’s 2014 and 2015 core operational activities supported these findings.** While stakeholders assessed that ENISA’s organisational set-up,

procedures and processes were conducive to the achievement of its objectives, a number of limiting factors to its effectiveness were identified, including:

- The limited resources that ENISA disposes of (2014 and 2015 evaluation);
- The broad mandate and the variety of tasks it seeks to fulfil;
- Difficulties with recruiting staff/talent with the needed competence, due to the salaries ENISA can offer and its geographical location.

3.2.2.9 Relationship with its stakeholders

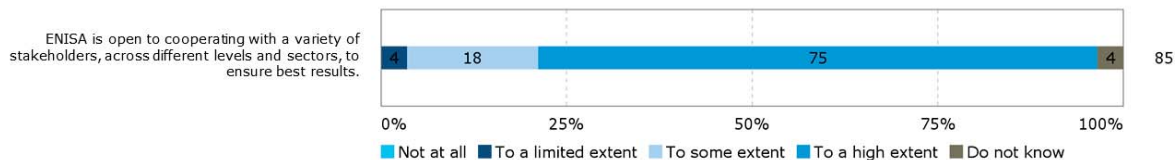
**EQ12: How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate?**

The evidence shows that ENISA has created strong and trustful relationships with some of its stakeholders, most importantly with the Member States and in particular the CERT/CSIRT community. The evidence suggests that ENISA could further improve the exchange of information between CERTs/CSIRTs by providing an oversight of available knowledge and good practices and by enhancing the coordination of CERTs/CSIRTs at the policy level.

The cooperation and coordination with the Commission’s DGs and some of the EU Agencies could be improved to reduce risks of overlap and create synergies. ENISA could also improve cooperation with the industry.

**ENISA’s direct stakeholders and ENISA staff agree that ENISA ensures successful cooperation with its stakeholders.** As can be seen in Figure 28, almost all respondents to the survey of ENISA staff and direct stakeholders (93%) thought that ENISA is open to cooperating with a variety of stakeholders to some or to a high extent, across different levels and sectors, to ensure better results. Two respondents from the Management and Executive Boards and one respondent from the PSG thought that the Agency was only open to such cooperation to a limited extent.

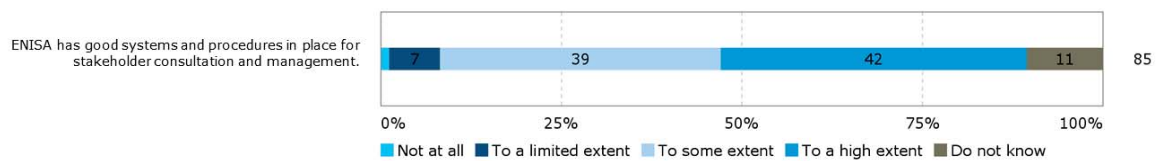
**Figure 28: Extent of agreement or disagreement with statement regarding ENISA’s cooperation with stakeholders**



Source: Survey of ENISA staff and direct stakeholders

A majority of respondents to the survey of ENISA staff and direct stakeholders (81%) considered that to some or to a high extent, ENISA has good systems and procedures in place for stakeholder consultation and management, as shown in Figure 29 below. A minority (8%) thought that it only had such good systems in place to a limited extent or not at all. ENISA staff were slightly more critical of these systems than the average, with 12% of them considering that ENISA only had such good systems in place to a limited extent or not at all. The Management and Executive Board members as well as the PSG members were mostly positive (respectively 84% and 92%), saying that ENISA had good systems in place to some or to a high extent or did not know.

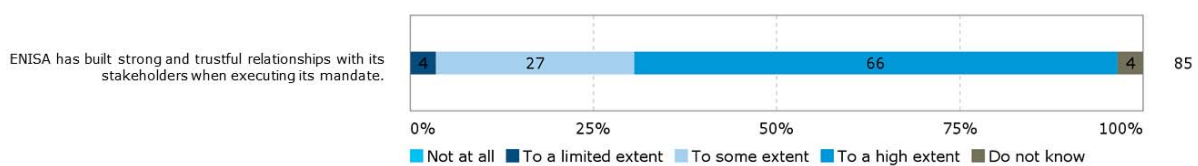
**Figure 29: Extent of agreement or disagreement with statement regarding ENISA’s cooperation with stakeholders**



Source: Survey of ENISA staff and direct stakeholders

Almost all respondents (93%) to the survey of ENISA staff and direct stakeholders thought that ENISA had built strong and trustful relationships with its stakeholders when executing its mandate to some or to a high extent (see Figure 30 below). Responses across the different stakeholder groups were very similar.

**Figure 30: Extent of agreement or disagreement with statement regarding ENISA’s cooperation with stakeholders**



Source: Survey of ENISA staff and direct stakeholders

Open public consultation respondents from national authorities believed that one of the main achievements of ENISA was the support ENISA provided to Member States in particular by fostering cooperation via the share of expertise among Member States. However, it was also suggested that ENISA could do more to share information on which expertise and practices are available in the Member States and can be of benefit to others.

**General suggestions were made to improve ENISA’s cooperation with its stakeholders.**

These were found in the surveys, the open public consultation, as well as the interviews and provided by a variety of the different stakeholder groups:

- ENISA should develop more internal expertise to provide better services to its stakeholders. Stakeholders did not refer to specific areas but rather indicated that in general ENISA should have more technical, in-depth expertise, ideally in all the thematic areas covered by the Agency.
- ENISA tends to be very structured in their approach to stakeholders, following the work programme very closely. This limits the possibility for informal interaction or ad hoc cooperation.
- It was recommended that ENISA ensures greater engagement with the PSG and generally ensures a better connection with the industry, for example through public private partnerships.

**Cooperation with the EU institutions is in place but there is a lot of room for improvement.**

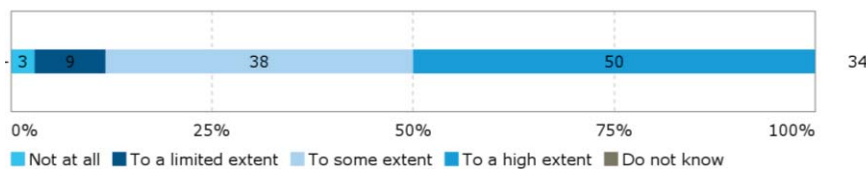
In the interviews, stakeholders from the different Commission DGs and other EU institutions explained how they worked together with ENISA and highlighted some positive achievements of this cooperation. Nevertheless, the collected evidence also shows that ENISA’s relationships with EU institutions are not sufficiently strong. On the one hand, there is a perception that the Commission DGs do not systematically involve ENISA when they work on matters relating to cybersecurity or data protection. There seems to be some doubt about ENISA’s expertise in some areas and a lack of structural cooperation between ENISA and the DGs. On the other hand, ENISA seems to lack resources to take ownership on some of the tasks when sharing responsibilities with the Commission.

The interviews show that ENISA has positive relationships with most of the EU agencies. A topic of raised by many interviewees is the degree of cooperation between ENISA and CERT-EU, which is described in section 3.2.4.1. In general, there is a need for a clearer mandate and delimitation of the role of different EU agencies and bodies active in the area of cybersecurity, including ENISA, CERT-EU, Europol’s EC3, but also of the Commission’s DG JRC. There seems to be untapped potential for cooperation and exchange of information.

**ENISA has developed strong relationships with the Member States.** Member States are present in ENISA’s Management Board allowing for the involvement in the development of the annual work programmes. ENISA cooperates with the Member States through the NLO network which is intended to serve ENISA as a point of reference into the Member States on specific issues. As shown in the survey results above, the participating members of ENISA’s Management Board and the NLOs show a high satisfaction with and trust in the cooperation with ENISA. There are various formats in which ENISA cooperates with the Member States, including exercises, trainings, meetings and the CERT/CSIRT community. A few of the interviewees of ENISA’s staff and direct stakeholders considered the complex structures of responsibility for cybersecurity issues in the Member States as a challenge for ENISA, in particular in the context of the upcoming implementation of the NIS Directive, under which ENISA will have to build up relationships with several new groups of authorities in the Member States.

**ENISA fosters the cooperation among CERTs/CSIRTs across the EU.** ENISA is heavily involved in fostering cooperation between CERTs/CSIRTs, as well as capacity building for CERTs/CSIRTs. In the CERT/CSIRT survey, participants were asked to what extent they thought ENISA proactively supported cooperation among CERTs/CSIRTs during the 2013-2016 period. As can be seen in Figure 31 below, the answers were in large part positive, with 83% of respondents (28 out of 34) thinking it did so to a high or to some extent and 12% (4 out of 34) thinking that it did so to a limited extent or not at all.

**Figure 31: Extent to which ENISA proactively supported cooperation among CERTs/CSIRTs during the 2013-2016 period**



Source: CERT/CSIRT survey

In the survey but also during the interviews, CERTs/CSIRTs provided suggestions how cooperation could be even further improved. It was suggested that ENISA should work on improving how CERTs/CSIRTs exchange information. This could be done by providing an oversight of what expertise and knowledge exist in the CERT/CSIRT community and helping to share good practices and lessons learned from one country to another. Respondents also stressed the importance of “liaising with CERTs/CSIRTs members on the technical level” so as to make ENISA management better equipped to address the needs of the CERT/CSIRT community. At the same time, they suggested that there was a need to reach out to the decision making level of the CERTs/CSIRTs in the Member States and not only focus on the technical level.

**ENISA’s relationship with further stakeholders, including industry and academia is limited.** Among industry and academia stakeholders ENISA is not widely known. Although ENISA publishes reports targeting the industry, for example SMEs, the Agency does not have sufficient outreach to these stakeholders. This was concluded in the evaluations of ENISA’s activities in 2014 and 2015 and confirmed during the interviews for the present evaluation. With the PSG there is a formal approach to involving these stakeholders in the planning and decision making processes of the Agency. ENISA’s management as well as other stakeholders noted, however, that the role of



the PSG was not sufficiently formalised. Within the Management Board, Member States have the main voice and consequently most of ENISA's activities are targeted towards them (see section 3.2.2.8 for further findings relating to ENISA's governance structure). Respondents from private enterprises and business associations to the open public consultation suggested that ENISA could foster private-public cooperation in the area of cybersecurity.

#### 3.2.2.10 ENISA's effectiveness considering its location

##### **EQ13: What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives?**

ENISA's effectiveness has overall been positively impacted by the move in 2013 of its operations teams to Athens from Heraklion, thereby facilitating access to the Agency from elsewhere and by Agency staff to Brussels. However, its location limits its effectiveness in achieving its policy objectives to a degree as it is more difficult for ENISA's management and staff to organise (ad hoc / informal) exchanges with the EU institutions, thereby affecting the degree of influence it can have on cybersecurity policy at the EU level and its impact in this area. Moreover, the difficulties experienced in recruiting and retaining qualified/expert staff which are partially linked to the Agency's location (see section 3.2.2.8 for further findings relating to ENISA's human resources) limit its ability to recruit and maintain the necessary staff to meet its objective of providing expertise through collating, analysing and making available information and expertise on key NIS issues.

The decision of the seat of EU agencies is a political one, determined by a common agreement between the representatives of the Member States meeting at Head of state or government level or by the Council. An attempt has been made to spread the agencies across all Member States. While in some cases the location decisions taken specify in which city a given agency will be located, in the case of ENISA, only Greece was defined as the location, leaving the decision on the city to the Greek government.<sup>47</sup> ENISA was established in Heraklion. In March 2013, a decision was made to move the operations of the Agency to Athens.

**The move of operations to Athens in March 2013 has increased the Agency's effectiveness, though the split between Athens and Heraklion was seen as a limiting factor to its effectiveness.** ENISA staff generally saw ENISA's location as less of a hindrance to its effectiveness than other stakeholder types; the move to Athens was overwhelmingly perceived as positive. The main benefit mentioned was that ENISA had become more easily accessible for those visiting the Agency and for staff it had become less time-consuming and expensive to travel across the EU. However, a few ENISA staff (including management) respondents were critical of the fact that the Agency is divided in two (between Heraklion and Athens), which it was perceived hampered internal communication and cohesion.

##### **ENISA's location is limiting its effectiveness in achieving its policy<sup>48</sup> related objectives.**

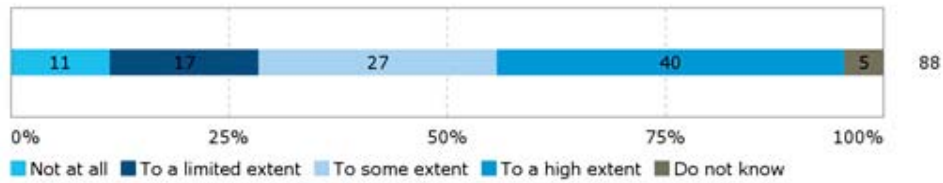
ENISA's location was judged by 67% of respondents to the survey of ENISA staff and direct stakeholders (59 out of 88) as enabling ENISA to effectively conduct its work (i.e. in terms of meeting its objectives) to some or to a high extent. It was reviewed as not enabling such effectiveness or only doing so to a limited extent by 28% of respondents (25 out of 88). ENISA's direct stakeholders were more critical than ENISA's staff and management of its location, with the NLOs, the Management and Executive Boards and the PSG members seeing the location as enabling the effectiveness of the Agency to a limited extent or not at all (with 58%, 42% and 39% respectively being of this opinion). By contrast, the large majority of ENISA staff including

<sup>47</sup> European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No3 – Agencies' seat and role of the host country. Available at: [http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche\\_3\\_sent\\_to\\_ep\\_cons\\_2010-12-15\\_en.pdf](http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_3_sent_to_ep_cons_2010-12-15_en.pdf)

<sup>48</sup> Policy objective: Promote network and information security as an EU policy priority, by assisting the European Union institutions and Member States in developing and implementing EU policies and law related to NIS.

management (84%) assessed the location as conducive to the effectiveness of ENISA’s work to some or to a high extent.

**Figure 32: Extent of agreement or disagreement with the following statement: ENISA’s location enables it to effectively conduct its work (i.e. in term of meetings its objectives)**

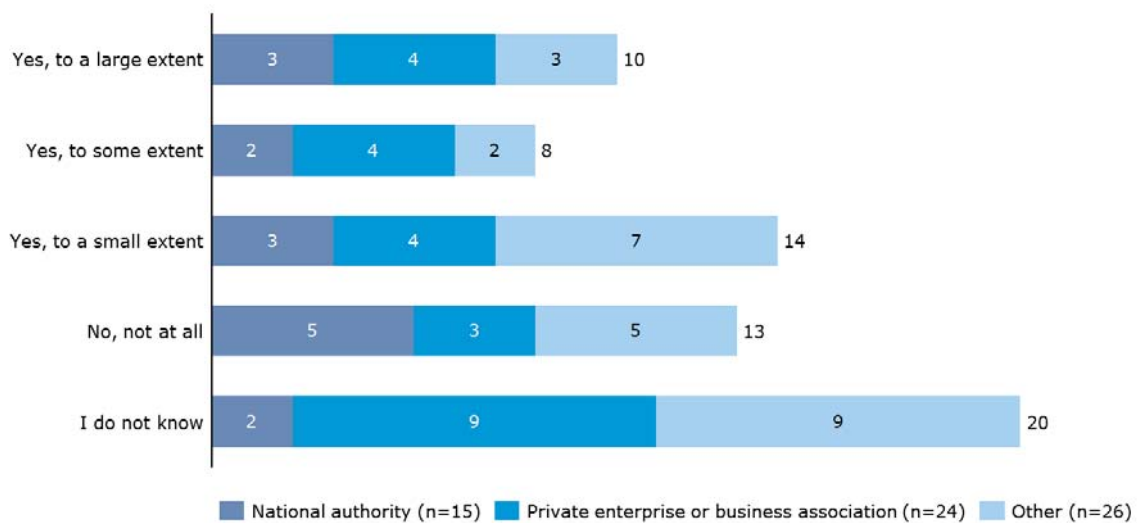


Source: Survey of ENISA staff and direct stakeholders

It was primarily felt by the more critical stakeholders referred to above that ENISA was situated too far from Brussels, making (ad hoc / informal) exchanges between the Agency and the EU institutions more difficult and thereby affecting the degree of influence ENISA can have on cybersecurity policy at the EU level and its impact in this area. The location of ENISA was cited as one source for a lack of coordination with ENISA by several members of the Commission. A number of interviewees across all stakeholder groups were of the opinion that its location limited ENISA’s ability to keep its finger on the pulse. It was suggested that the location helped explain why CERT-EU, which is situated in Brussels and can be called upon more easily, is taking on tasks that are could arguably also fall within the mandate of ENISA. Some suggestions for improvement included having a more decentralized office structure though care would need to be taken not to create too much of a fragmented Agency, flexible arrangements with smaller offices where needed, for projects etc., or having a liaison office in Brussels.

In the open public consultation, respondents were asked about the impact of ENISA’s split location on the Agency’s ability to conduct its work effectively and efficiently. As presented in Figure 33 below, there were very mixed views on this question with 28% (18) judging that the split location affected ENISA’s ability to conduct its work effectively and efficiently to some or to a large extent, while 20%(13) felt it did not do so at all. The views were divided among all respondent stakeholder groups.

**Figure 33: Extent to which ENISA’s split location arrangement affected ENISA’s ability to conduct its work effectively and efficiently, (n=65)**



Source: Open public consultation

Respondents were invited to provide a further explanation of their assessment. Respondents who felt more positive about ENISA’s current arrangement said that being decentralised from Brussels

provided the Agency an advantage to be perceived as a neutral source of information. Considering that ENISA has still been successful in operating outside its offices and maintained presence and cooperation in relevant events, the location of its offices was not perceived to have affected ENISA's ability to work effectively and efficiently. Respondents who felt less positive about ENISA's current location arrangements said the split location was not optimal for efficiency. Reasons for this included the increase of travel costs as well as costs spent on maintaining both offices. The split location was thought to present a challenge to people management.

**ENISA's location limits its effectiveness in terms of its objective to provide expertise<sup>49</sup>.**

There are several factors influencing ENISA's ability to hire and retain staff but as described in section 3.2.2.8 difficulties for spouses to find work in Greece and the lack of a European school in Athens contribute to the Agency's human resources issues and thus lead to difficulties to provide its stakeholders with the sought after expertise.

3.2.2.11 ENISA's internal mechanisms for programming, monitoring, reporting and evaluating

**EQ19: To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc.)?**

The programming, monitoring, reporting and evaluating mechanisms implemented by ENISA are adequate to ensure accountability and an appropriate assessment of performance. However, these mechanisms lead to a degree of administrative burden as they are not adapted to the size of the Agency and there is room for improvement in terms of the establishment of a monitoring system that enables the tracking of performance over time against pre-determined KIIs.

**ENISA has a series of internal mechanisms for ensuring accountability and the assessment of performance.** ENISA's work is based on annual planning and KIIs are set for all activities to evaluate performance. These KIIs are followed up on in ENISA's annual activity reports (section 3.2.2.1 considers ENISA's KIIs to assess effectiveness). The quality assurance of projects is done with a Quality Management System (QMS); the Agency reviewed the QMS in 2015 and 2016. A range of instruments are available to ensure quality such as manuals and guidelines laying down standard operating procedures. Activities follow the Deming Cycle (plan, do, check, act). ENISA has been integrating tools such as electronic signatures, electronic workflows and enterprise resource management. Finally, ENISA has a number of activity-specific tools that it uses to monitor performance, including surveys of participants in the Cyber Europe Exercises and of participants in training sessions. The evaluation of ENISA's 2015 core operational activities (undertaken in the first half of 2016) pointed to some areas for improvement in this regard and assisted ENISA by designing tools for the monitoring of publications via a brief pop up questionnaire, and of the initial and follow-up monitoring of training activities.

**ENISA's internal mechanisms for programming, monitoring, reporting and evaluating ensure accountability and an appropriate assessment of the overall performance of the Agency.** ENISA carefully follows requirements imposed by the Commission rules and according to reports from the Court of Auditors, the Agency has shown strong compliance and raised no concern with regard to its accountability.<sup>50</sup> ENISA's direct stakeholders, most importantly the Management Board, showed satisfaction with the developed procedures. Also internally (by ENISA

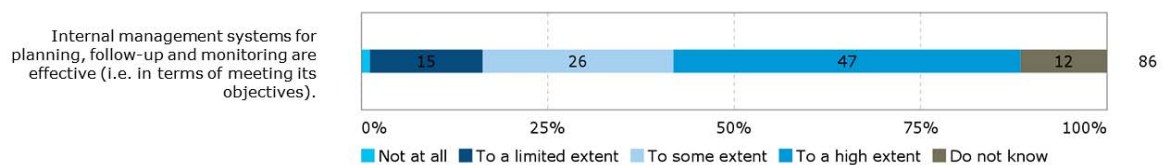
<sup>49</sup> Expertise objective: Anticipate and support Europe in facing emerging NIS challenges, by collating, analysing and making available information and expertise on key NIS issues (potentially impacting the EU taking into account the evolutions of the digital environment.)

<sup>50</sup> Court of Auditors (2015): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2014 together with the Agency's reply, and Court of Auditors (2016): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2015 together with the Agency's reply

staff and management), the effectiveness of project planning, project tracking and budget management was considered to be high.

The survey results further confirmed this finding. As can be seen in Figure 34 below, the majority of respondents to the survey of ENISA staff and direct stakeholders (73%) thought that the internal management systems were conducive to effectiveness (i.e. in terms of meeting ENISA's objectives) to some or to a high extent. This effectiveness was viewed as existing only to a limited extent or not at all by 16% of respondents (14 out of 86). Specifically, the members of the Agency's Management and Executive Board were overall satisfied with the effectiveness of these systems, with 84% of them ranking them as leading to effectiveness to some or to a high extent.

**Figure 34: Extent of agreement or disagreement with statement regarding ENISA's internal management systems**



Source: Survey of ENISA staff and direct stakeholders

**Requirements to ensure accountability and a review of performance are burdensome for ENISA, in particular considering the small size of the Agency.** As an EU Agency, ENISA has to follow the rules and obligations imposed by the Commission. In particular, ENISA's staff and management reported that these requirements represented an important burden as they were not adapted to the small size of the Agency. A quarter of ENSIA staff (25%) indicated in the survey question above that the internal management systems were only to a limited extent or not at all conducive to effectiveness. For example, the Agency works with a high number of rather small projects. Not each of these projects requires the same detailed planning and follow-up as some larger Commission projects would need. Interviewees noted that with limited administrative resources in the Agency it was burdensome to meet all the requirements.

**Specific suggestions were made to improve the mechanisms for programming, monitoring, reporting and evaluating:**

- Reporting tools should be better integrated with one another and automated to alleviate the burden of administrative tasks. This includes the planning and reporting tools for travel of staff
- The follow up on the use of created reports could be improved. Currently, a focus is set on monitoring the number of downloads of reports. Interviewees suggested that it would be more informative to collect actual feedback from users of reports and to identify how information from reports is being used. Such follow up should take place over several years.
- Members of the Management Board saw artificial constraints created by the requirement to provide an early draft of the work programme by January for the following year. It was reported to be difficult to make specific plans so early in advance and the Work Programme risks to be outdated quickly because the cybersecurity environment is changing rapidly.

The 2015 evaluation also made some conclusions and recommendations in relation to the setting of KIIs which are worthy of note here: **For ENISA, measuring impact is highly challenging and to a large extent dependent on contextual factors, so setting up a monitoring system that works over the long term is essential.** This is true in particular for policy agencies like ENISA, since the impact can only take place in the larger community by stakeholders applying and/or using ENISA's outputs. Moreover, impact can often only really be judged on the longer term through an annual monitoring process. In this respect, ENISA's annual KIIs are an essential data source when it comes to monitoring the Agency's impact over time. In comparison to 2014, some of the KIIs for 2015 were more ambitious and provided a better starting point to

measure ENISA’s contribution to reaching the impacts foreseen. However, it should be noted that the actual data needed to measure the KIIs was not available at the time of the evaluation. The reporting on some of the more ambitious KIIs which seek to ascertain “use” is more operational, focussing more on outputs (e.g. the organisation of and number of participants in a workshop) rather than on the actual contribution to an impact (e.g. using ENISA’s recommendations). This is likely to be in part the result of it being too early to judge the true impact of given activities, but also due to a lack of follow-up on a yearly basis in relation to the KIIs set in a given year. On this basis, it was recommended that ENISA set up a monitoring system which seeks to measure performance against pre-defined KIIs set in a given year, allowing for the measurement of impact over a more extended period of time than a year (as is currently the case). Monitoring and reporting in relation to such KIIs would therefore need to be ensured on an annual basis for, e.g. five years. It was further recommended that ENISA ensure that the KIIs capture impact rather than output, and that the collection of data in relation to these is improved.

### 3.2.2.12 In-house capacity and use of external service providers

**EQ20: To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?**

The findings are contradictory on whether ENISA has succeeded in building up in-house capacity. Stakeholders strongly differ in their assessment. While the Agency has been able to hire some experts over the last years, ENISA highly depends on external expertise for the implementation of its activities. Decisions to outsource work are made on an individual basis and are only to some extent guided by efficiency criteria.

**ENISA strongly relies on external expertise for its activities.** From 2014 to 2016, around 80% of the Agency’s operational budget was used for procurement of studies. As indicated by ENISA in the benchmarking exercise, in 2016, procurement of study amounted to EUR 1.597.087 of a total operational budget of EUR 2.000.000. Compared to other EU Agencies, ENISA relies a lot more on external expertise. For example, the ratio of operational budget used by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) for procurement of study was reported by the EMCDDA to represent less than 5% in 2013 but has increased to reach slightly over 15% in 2016.<sup>51</sup> Table 17 below provides a detailed overview of ENISA’s procurement activities between 2013 and 2016.

**Table 17: Overview of ENISA’s procurement (operations and non-operations)**

	2013	2014	2015	2016
<b>Contracts signed</b>				
Service contracts	18	25	11	12
Specific contracts awarded under re-opening of competition	8	15	20	25
Framework contracts	7	18	19	14
Total number of procurement related contracts	33	58	50	51
<b>Purchase orders</b>				
Issued under a framework contract	78	119	143	127
Not issued under a framework contract	84	115	158	193
Total number of purchase orders	162	234	301	320
<b>Procurement procedures</b>				

<sup>51</sup> Information provided by ENISA and EMCDDA for the benchmarking exercise. The agencies were asked to provide the ratio of budget used for procurement of study over the overall operational budget. It has not been possible to verify this information based on other sources.

Open procedures	15	10	9	8
Other procedures	4	20	38	27
<b>Total number of tender procedures</b>	<b>19</b>	<b>30</b>	<b>47</b>	<b>35</b>

*Source: Based on Annual Reports, completed and verified by ENISA*

From its outset, ENISA is an agency that uses procurement for a lot of its work. With limited human and financial resources, ENISA has to find external capacities to cover the very specific and complex topics of the cybersecurity field as needed by its stakeholders. Often research and data collection is done by external experts, while ENISA staff maintains the responsibility to analyse and report on the collected data. However, some specific tasks are being done internally, such as the cyber exercises, Article 14 requests and the preparation of the implementation of the NIS Directive. A few stakeholders suggested that these tasks would become even more important in the future.

**Stakeholders disagree on whether ENISA has successfully built up internal expertise to cover the various tasks assigned to the Agency.** While some interviewees (direct stakeholders and representatives from the EU institutions) think that ENISA has managed to hire staff with specific expertise over the past years and see ENISA as being very capable to respond to their needs, other interviewees (of the same group) think that the Agency is significantly hindered to attract the needed expertise as explained in section 3.2.2.8 concerning the effectiveness of ENISA’s human resources policies.

**The disagreement also concerns the question whether the use of procurement is advisable at all.** Some members of ENISA’s Management Board said they would like to see ENISA get more work done internally because procurement processes made the Agency slow and dependent on external stakeholders. Others said that ENISA should use its network of experts even more systematically and also involve them in project management roles. This way, staff resources could be freed up for other tasks.

**The findings suggest that the "make or buy" choices are made on a case by case basis with no institutionalised consideration of efficiency criteria.** According to ENISA staff and management the decision whether an activity is carried out in-house or requires procurement of external services depends on the task and the topic covered. Reasons for outsourcing are to involve sector experts to provide a different perspective or for quality assurance, for specific data collection (e.g. through surveys) and to take over services developed by the Agency that have become too big to handle in-house. In this sense, it can be said that efficiency plays a role when outsourcing decisions are made: work that is faster or cheaper if implemented by an external service provider is considered for outsourcing. However, ENISA staff and management also noted that the Agency received a specific budget from the Commission for procurement and that decisions are made in a way to ensure full use of this budget.

## 3.2.2.13 Conclusion on effectiveness

**Conclusion – Effectiveness**

The *baseline situation* (established based on an evaluation of all EU agencies including ENISA in 2009<sup>52</sup> and an impact assessment of changes to ENISA's mandate in 2010<sup>53</sup>) shows concerns about ENISA's ability to achieve targeted impacts. The main reasons provided were ENISA's limited financial resources and the small size of the Agency. These concerns continued to be relevant in the period 2013-2016, as presented below.

The annual evaluations of ENISA show that the Agency implements its tasks and achieves its set targets. Through this work, ENISA has made a contribution to increased NIS in Europe. However, this contribution is limited by several factors:

- the broad mandate under which a variety of tasks is to be covered,
- the strong influence of Member States when it comes to setting the work programmes,
- the Agency's difficulties in attracting and retaining cybersecurity experts as staff members,
- and the limited visibility of ENISA.

ENISA's activities have made an important contribution to **enhanced cooperation** between Member States and related NIS stakeholders. Community building has been enhanced across Member States and in particular the cooperation between CERTs/CSIRTs has increased. However, the cooperation and exchange between ENISA and the Commission and other EU agencies could still be improved. Furthermore, cooperation with industry stakeholders should be strengthened.

ENISA has contributed to **enhanced capacities** in Member States, most notably in Member States with more limited capabilities and resources in the area of cybersecurity. Important activities have been developed and implemented, such as the Cyber Europe Exercises and trainings for CERTs/CSIRTs. Similarly to its contribution to enhance cooperation, ENISA is not reaching all stakeholders with its capacity building activities. Industry stakeholders could be better involved.

ENISA is limited in the **expertise** it can provide. It makes an important contribution to the CERTs/CSIRTs. Other stakeholders from the Member States, but also the EU institutions and industry representatives, are less convinced by ENISA's expertise. ENISA has not managed to become recognised as a centre of expertise or a reference point for stakeholders. The high reliance on the procurement of external expertise in the implementation of tasks is a consequence of the limited in-house expertise but also the limited resources available.

ENISA has assisted the Member States and the Commission in developing and implementing the **policies** necessary to meet the legal and regulatory requirements of NIS, though the Agency is not consistently being involved by the Commission in all NIS-related activities.

Overall, ENISA has difficulties meeting its objectives. This is linked to the Agency's broad mandate which is not matched by sufficient financial resources. A lot of efforts are being made but they are spread over a wide field of responsibility, therefore ENISA can only have a limited impact on cybersecurity.

<sup>52</sup> Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

<sup>53</sup> European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

### 3.2.3 Efficiency

Efficiency considers the relationship between the resources consumed by an intervention and the changes generated by it (which may be positive or negative).<sup>54</sup> The assessment of the efficiency of ENISA considers the relationship between the resources used by the Agency and the changes generated by its activities. The section also covers the efficiency of ENISA’s governance and internal organisational structure. The benchmarking of ENISA with other EU agencies and bodies has been integrated in this section.

The following evaluation questions are covered in the present section:

**Table 18: Evaluation questions covered under the efficiency criterion**

Main evaluation question	Other evaluation questions
<p><b>EQ14: To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation? To assess this question, elements relating to internal structure, operation, programming of activities and resources, accountability and controls, etc. will be analysed.</b></p>	<p><b>Retrospective</b></p> <p>EQ15: Were the annual budgets of the Agency implemented in an efficient way considering the results achieved?</p> <p>EQ16: Have the resources allocated to the Agency been sufficient for the pursuit of its tasks (input/output analysis)?</p> <p>EQ17: To what extent are the organisational solutions and procedures of ENISA adapted to the work entrusted to it and to the actual workload? Is the planning cycle of the agency (work programme and budget) in line with the objective of achieving efficient results?</p> <p>EQ18: To what extent have ENISA's governance, organisational structure, locations and operations as set in its Regulation and the arrangements related to the location of its offices been conducive to efficiency and to achieving economies of scale?</p> <p>EQ21: To what extent and how have external factors influenced the efficiency of ENISA?</p>

#### 3.2.3.1 ENISA’s efficiency considering its governance, organisational structure, procedures, budget and location

**EQ14: To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation? To assess this question, elements relating to internal structure, operation, programming of activities and resources, accountability and controls, etc. will be analysed.**

**EQ17: To what extent are the organisational solutions and procedures of ENISA adapted to the work entrusted to it and to the actual workload? Is the planning cycle of the agency (work programme and budget) in line with the objective of achieving efficient results?**

**EQ18: To what extent have ENISA's governance, organisational structure, locations and operations as set in its Regulation and the arrangements related to the location of its offices been conducive to efficiency and to achieving economies of scale?**

While ENISA’s governance structure (with an Executive Board, Management Board and the PSG), management practices and dedicated staff are conducive to the efficient functioning of the Agency, there are a number of areas where further efficiency gains could be made. These relate to the relatively rigid and inflexible planning cycle; the split location between Athens and Heraklion which incurs additional travel costs and costs in terms of ensuring cohesion; its working practices relating to its objective of delivering “expertise” through reports and publications which through a more

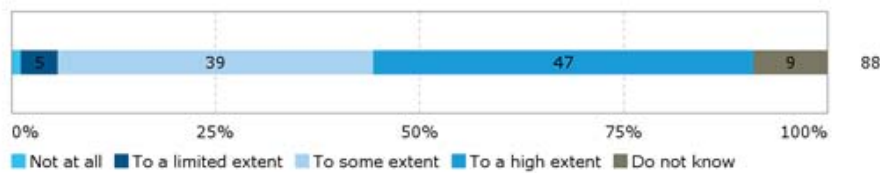
<sup>54</sup> Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final



efficient process of, for example, peer review could be improved in terms of their quality; the need to further modernise and automate given administrative processes; and the need for HR processes to be further formalised to ensure a smoother, quicker process.

**ENISA’s governance structure is conducive to the efficient functioning of the Agency.** The current governance structure was seen as conducive to the efficient functioning of the Agency (i.e. in terms of value for money) by most of the respondents to the survey on ENISA’s governance, organisational set-up and working practices (86% or 76 out of 88 respondents) and was judged conducive to this efficiency to a limited or to no extent by only 6% of respondents (5 out of 88). Members of the Management and Executive Boards provided more positive answers than the other groups of respondents: 63% considered the governance structure to be conducive to efficiency “to a high extent”. The interviews with staff and ENISA’s direct stakeholders also pointed to the fact that ENISA’s organisational set-up was adapted to the work it carries out and its workload, enabling it to achieve its objectives in an efficient manner.

**Figure 35: Extent of agreement or disagreement with the following statement: The current governance structure with a Management Board, an Executive Board and the PSG is conducive to the efficiency functioning of the Agency (i.e. in terms of value for money)**

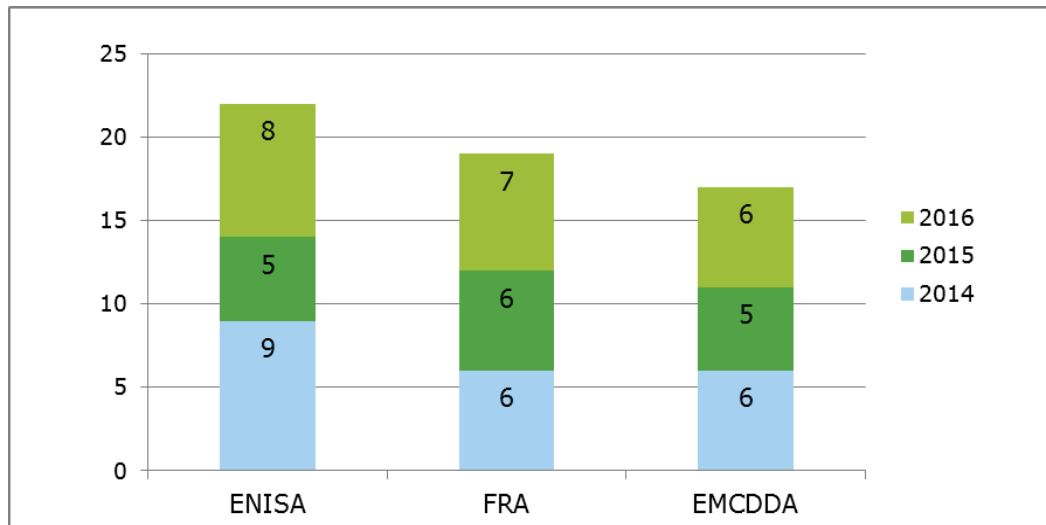


Source: Survey of ENISA staff and direct stakeholders

In particular, the establishment of an Executive Board was judged positively by more than half of respondents (56% or 49 out of 88 respondents) who saw this new board as bringing more efficiency to the functioning of the Management Board to some or to a high extent. A limited number of respondents (10% or 9 out of 88) saw this change as being conducive to more efficiency to a limited extent or not at all - a quarter of NLOs (25%) were of this opinion. In these cases, respondents questioned whether the Executive Board leads to a more efficient functioning of the Management Board, suggesting instead that it only increases the complexity and decreases the transparency of the structure. Interviewees from ENISA staff and direct stakeholders suggested that the Management Board could gain in efficiency by working in smaller, targeted groups that focus on a given topic before feeding back to the plenary (see also section 3.2.2.8). The 2014 and 2015 evaluations supported these findings with reference being made to a clear delineation of responsibilities within the organisation, leading to a good execution of the work.

The comparison with other EU agencies shows that ENISA had a comparatively high number of meetings with its governing bodies. The comparably higher number of Management Board and Executive Board meetings per year for strategic decision making supports the argument made by those respondents who judged that ENISA’s governance structure with two boards increased the complexity of the Agency. However, FRA also works with an Executive Board. At the same time, the high number of meetings shows the active engagement of the Management and the Executive Board in the running of the Agency.

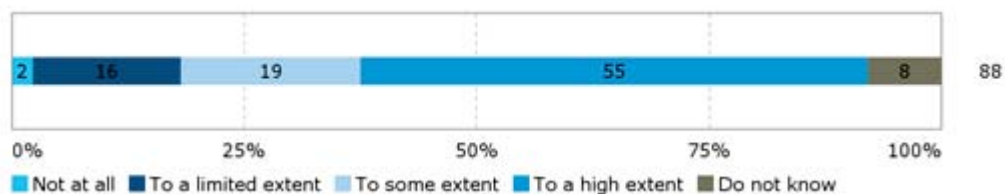
**Figure 36: Number of Management Board and Executive Board meetings per year for strategic decisions, 2014-2016**



Source: Data gathered through secondary sources and received by ENISA, FRA and EMCDDA.

**ENISA’s management practices are conducive to creating an efficient organisation.** The majority of respondents to the survey of ENISA staff and direct stakeholders (74% or 65 out of 88) saw ENISA’s management practices as being conducive to creating an efficient organisation (i.e. in terms of value for money) “to some” or “to a high extent”. The interviews with ENISA staff suggested that the fact that many of ENISA’s management staff come from the private sector assists in ensuring that the Agency is managed in an efficient way. The number of meetings at management level was also referred to as a means to facilitate the dissemination of information and make management more transparent. However, a total of 18% of respondents (16 out of 88) saw ENISA’s management practices as only conducive to such efficiency to a limited or to no extent; it was felt that management and administration overall had too large a role.

**Figure 37: Extent of agreement or disagreement with the following statement: ENISA’s management practices are conducive to creating an efficient organisation (i.e. in terms of value for money)?**



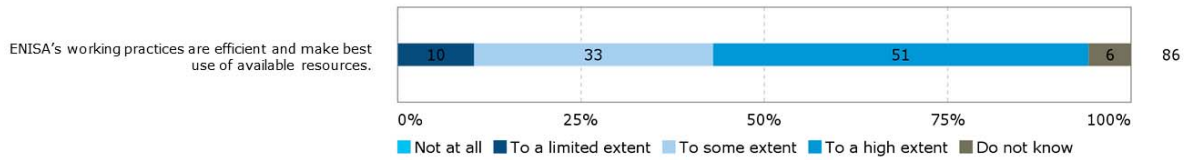
Source: Survey of ENISA staff and direct stakeholders

**The planning cycle of the Agency (work programme and budget) is lengthy.** The planning process is lengthy and burdensome for management in particular, as detailed in section 3.2.2.5, but was overall deemed necessary and leads to a necessary result. The findings in this same section point to ENISA’s work programme being a relatively rigid means of determining work priorities in such a fast-paced area and a lack of continuity in many of its activities from one year to the next due to its aim to cover a wide range of activities and sectors. It can be assumed that increasing the flexibility and continuity of the work programme from one year to the next would therefore likely lead to efficiency gains.

**ENISA’s working practices are efficient, leading to timely but not necessarily consistently useful, high quality outputs.** A large majority of respondents to the survey of ENISA staff and direct stakeholders (84% or 72 out of 86 respondents) saw ENISA’s working practices as efficient and making the best use of available resources to some or to a high extent. Some of the tools in place in the Agency are advanced compared to those used by other agencies

and favour efficiency, e.g. the Agency’s workflow paperless management system (use of e-signatures). However, nine respondents (16%) saw ENISA’s working practices as being conducive to such efficiency only to a limited extent or not at all. ENISA staff members (including management) were slightly more critical of ENISA’s working practices than the direct stakeholders with 16% of them regarding them as conducive to efficiency to a limited extent. Reasons provided for such assessments included the level of bureaucracy being too important within ENISA and administrative tasks having to be conducted by operational staff.

**Figure 38: Extent of agreement or disagreement with the following statement on ENISA’s working practices**

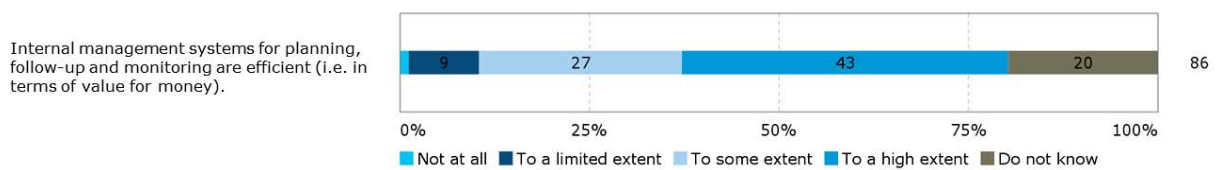


Source: Survey of ENISA staff and direct stakeholders

While ENISA’s working practices enable it to produce services in a timely manner, the quality, usefulness and added value of some of its outputs was questioned (see section 3.2.2.7). It was suggested by one interviewee that ENISA could gain in efficiency by procuring less work externally from contractors and drawing more on the expertise of national cybersecurity experts from national authorities, academics and the private sector to assist them in developing reports/publications in-house through a peer review process.

With regards to the internal management systems for planning, follow-up and monitoring the majority of respondents to the survey of ENISA staff and direct stakeholders (70%) saw them as creating value for money “to some” or “to a high extent”. This efficiency was viewed to be of “a limited extent” or to exist “not at all” by 10% of respondents. A large number of Management and Executive Board members saw the management systems to be bringing efficiency to some or to a high extent while ENISA staff was on average slightly more likely (16%) to consider the efficiency brought by management systems as being limited or non-existent.

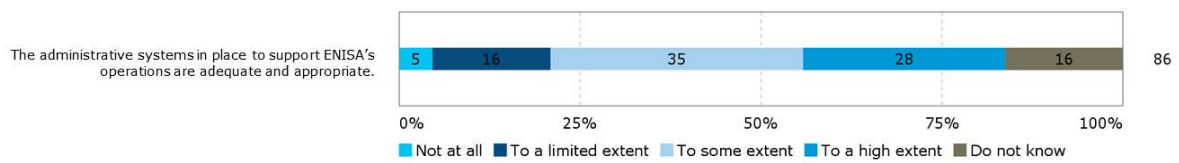
**Figure 39: Extent of agreement or disagreement with the following statement regarding ENISA’s internal management systems**



Source: Survey of ENISA staff and direct stakeholders

**ENISA’s administrative systems are adequate, but could be modernised to increase efficiency.** The administrative systems in place to support ENISA’s operations were seen by survey respondents as adequate and appropriate to some or to a high extent by a majority of respondents (63% or 54 out of 86 respondents) and to a limited extent or not at all by 21% (18 out of 86). ENISA staff (including management) was more critical than the average in this regard, with 35% of them stating that the administrative systems were adequate and appropriate only to a limited extent or not at all. Those who provided comments on their more negative assessment converged in saying that the administrative systems used were not modern enough and led to a duplication of work; required a lot of manual work to operate, not allowing for automation; and overall impeded the smooth functioning of the Agency.

**Figure 40: To what extent do you agree/disagree with the statements below regarding ENISA?**

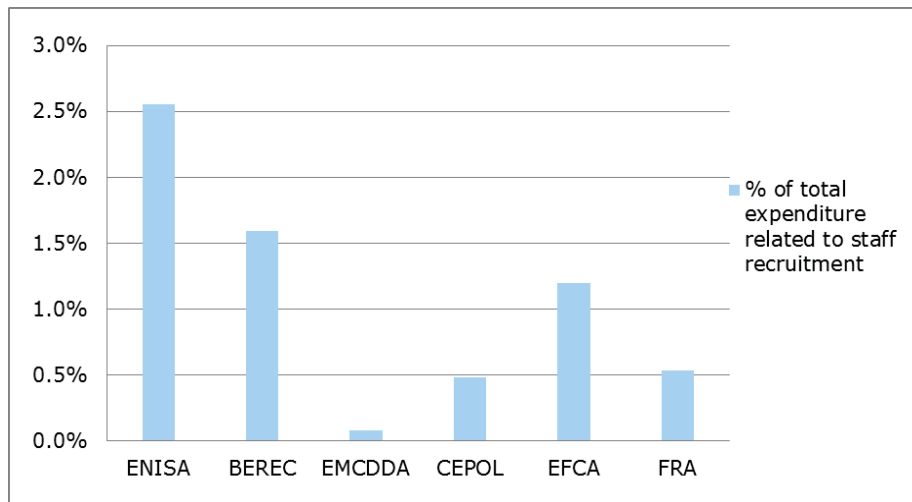


An example of a system referred to in the 2014 evaluation was the MATRIX project management system. Staff book their hours in the system and it provides an overview of resources for each project. MATRIX automatically generates reports for the management on a biweekly basis. However, the system was not considered relevant for generating management information at an operational level, and it was not used actively to steer projects. Instead, in addition to MATRIX, each Core Operations Department (COD) unit used spreadsheets to maintain an overview of projects on a daily basis. These sheets were individual to each unit and varied in content from one unit to another. During the interviews conducted in 2014, ENISA staff indicated that the MATRIX system did not provide for sufficient functions for project management at COD unit level, such as tracking risks and issues. For this reason the spreadsheets were set up, with plans to standardise them in the future.

**While the Agency’s staff was seen as a source of efficiency, human resource processes and issues are a source of inefficiency.** A number of interviewees (ENISA management and Executive Board members) referred to ENISA’s motivated, hard-working staff as a key factor to its efficiency. However, ENISA’s difficulty in recruiting and retaining staff (see section 3.2.2.8) is a source of inefficiency with significant efforts needing to be put into recruitment by the administrative department. Moreover, inefficiencies in the recruitment process were cited by ENISA staff with references to the lengthy process, the need to ask the same questions of all interviewees making them “unnatural”, difficulties in organising interviews when all interview committee members are present, and a lack of follow-up with candidates. It was hoped that the arrival of a new human resources manager in late 2016 would enable the process to become more efficient.

**The difficulties in attracting staff are also reflected in the expenditure allocated to recruitment; ENISA dedicates more financial resources to staff recruitment than any of the other agencies and bodies considered under the benchmarking exercise.** The figure below shows that 2.5% of ENISA’s total expenditure in 2015 was dedicated to staff recruitment; this figure is significantly higher than for agencies and bodies like BEREC, EFCA, CEPOL, EDA and EMCDDA. Despite these efforts, recruitment has not been successful.

**Figure 41: Staff recruitment expenditure compared to overall expenditure, 2015**

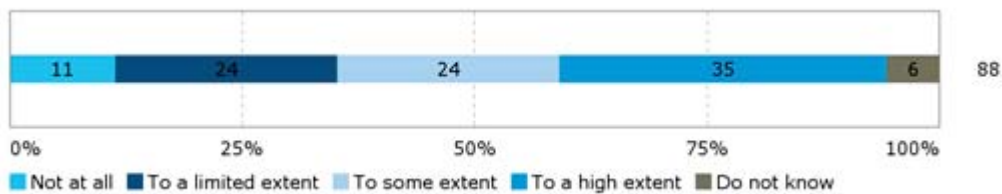


Source: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III Bodies set up by the EU and having legal personality and Public-Private Partnership.

**While the setting up of an office in Athens contributed to efficiency gains, the split location of the Agency is not conducive to its efficiency.** Moving ENISA’s operational units to Athens in 2013 meant an important increase in efficiency. As stated in a Commission cross-cutting study on the decentralised agencies of 2012<sup>55</sup>, the overall accessibility of EU agencies affects their efficiency. The study showed that agencies located in very remote places (including ENISA when located in Heraklion) faced difficulties in attracting and retaining staff from the rest of Europe, leading to difficulties in filling the establishment plans with appropriate staff and to geographical imbalances with a high representation of local staff. This issue has been alleviated to a great extent with the move of parts of ENISA to Athens but as shown below, inefficiencies linked to ENISA’s location persist.

Among the respondents to the survey of ENISA staff and direct stakeholders, ENISA’s current location was judged by 59% (52 out of 88 respondents) as enabling ENISA to conduct its work efficiently (i.e. in terms of value for money) to some or to a high extent. A total of 35% of respondents (31 out of 88) saw it as being conducive to this efficiency to a limited extent or not at all. There was a difference in the opinions of ENISA staff relative to other types of respondents: PSG members, NLOs and Management and Executive Board members saw ENISA’s location as only being conducive to its efficiency to a limited extent or not at all (respectively 54%, 50% and 47%) whereas three quarters (75%) of ENISA staff (including management) saw ENISA’s location as being conducive to its efficiency to some or to a high extent.

**Figure 42: Extent of agreement or disagreement with the following statement: ENISA’s location enables it to conduct its work efficiently (i.e. in terms of value for money)**



Source: Survey of ENISA staff and direct stakeholders

<sup>55</sup> European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No3 – Agencies’ seat and role of the host country. Available at: [http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche\\_3\\_sent\\_to\\_ep\\_cons\\_2010-12-15\\_en.pdf](http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_3_sent_to_ep_cons_2010-12-15_en.pdf)

The respondents who criticised the efficiency of ENISA’s location referred to the costs incurred by travel (direct costs and time commitment), and the duplications of costs related to ENISA’s facilities being divided over two locations (between Heraklion and Athens). A few ENISA staff (including management) respondents were critical of the fact that the Agency is divided in two, which it was judged decreased the Agency’s efficiency as its incurred additional travel costs, and led to duplications of work from an organisational set-up perspective, e.g. negotiations with landlords and other organisational questions. Inefficiencies in the split location were cited by interviewees as being primarily due to travel costs between Athens and Heraklion and to ensuring cohesion between the two offices, rather than the costs of maintaining an office in two locations. A variety of types of interviewee saw closing the office in Heraklion as a means to increase the Agency’s efficiency.

In fact, the Agency itself sees efficiency losses stemming from duplication of services across the two offices. This includes duplication of costs for security and cleaning services as presented in Table 19. The costs listed below for the office in Heraklion represent 24% of ENISA’s administrative expenditure in 2016.

**Table 19: Annual costs for renting and maintaining two offices**

Costs	Athens	Heraklion
<b>Rent of premises</b>	€316,450	€316,444
<b>Security services</b>	€51,000	€47,400
<b>Cleaning services</b>	€24,000	€15,180
<b>Total</b>	€391,450	€379,024

Source: Data provided by ENISA

To this, the staff costs for employees in Heraklion have to be added. According to data provided by ENISA, there were 13 staff members working in Heraklion in 2016, representing a cost of more than 300,000 EUR per year (the number of staff in Heraklion has been reduced to eight in 2017). Similar costs would have to be paid if these staff members were based in Athens. Only the travel costs to Athens of EUR 751 per staff member could be saved.

**Table 20: Costs for staff based in Heraklion**

Costs	Number of staff	Total
<b>Daily subsistence allowances</b>	13	€83,813
<b>Installation allowances</b>	13	€89,422
<b>Removals</b>	13	€139,000
<b>Travel expenses</b>	13	€751
<b>Total</b>	13	€312,986

Source: Data provided by ENISA

ENISA also assesses that the most important costs stemming from the two offices are related to a loss of productivity due to the separation of the teams and the needs to ensure coordination and across the offices.

**ENISA was not seen as achieving economies of scale to the extent that it could.** Where ENISA can achieve economies of scale is through its cooperation with other bodies, which as presented in section 3.2.4 is not as effective as it could be. In fact, it was suggested that from a European perspective, ENISA’s capabilities and skills could be used more efficiently and economies of scale could be achieved if ENISA is consulted/has a role in any European activity being linked to NIS/Cybersecurity in Europe such as the contractual public-private partnership (cPPP).

### 3.2.3.2 Implementation of annual budgets

#### **EQ15: Were the annual budgets of the Agency implemented in an efficient way considering the results achieved?**

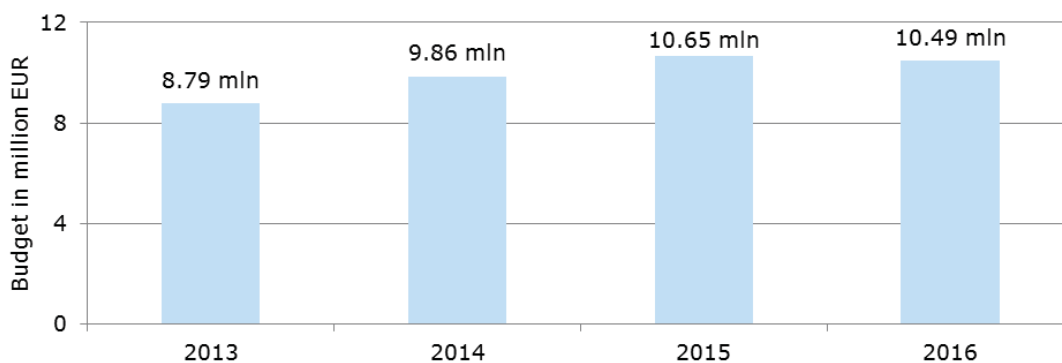
Taking into account the results achieved by the Agency and the limited budget available it can be concluded that ENISA implements its budgets in an efficient way. ENISA makes important achievements in terms of created outputs, such as high numbers of publications and fully uses the allocated funds. The Agency has been able to contribute to its targeted impact (an increased level of NIS in Europe) though could achieve more if more resources were available.

Improvements in budget implementation could be made by reducing the amount of carry-overs from one year to the next and ensuring that the budget is spent evenly within one year. Among the selected sample of EU Agencies, ENISA has the highest share of administrative expenditure.

**Over the period 2013 to 2016, ENISA’s budget has increased by 16%.** The budget of the ENISA comprises a subsidy from the EU budget which constitutes each year to 93% of the Agency’s revenue. In addition, revenue stems from rent subsidies from the Government of the Hellenic Republic (which constitutes between 6 and 7% each year), as well as contributions from third countries participating in the work of the Agency (around 1%).

In 2016, the Agency had a budget of EUR 10.5 million. Figure 43 shows the annual increase in ENISA’s budget. The overall increase in four years is EUR 1.7m or an increase of 16% relative to the 2013 budget.

**Figure 43: ENISA’s budget 2013-2016**



Source: ENISA’s Annual Activity Reports (2013, 2014, 2015, 2016)

A comparison to other EU agencies shows that ENISA is among the decentralised agencies with the lowest budget. This is further discussed in section 3.2.3.3 below.

**ENISA ensures full budget execution but carry-overs are high; a problem that is encountered by many EU agencies.** As shown in Table 21 below, ENISA reached a budget execution rate of its expenditure appropriations of 100% in 2014 and 2015, suggesting high efficiency in the use of its budget. The high payment rate also shows the capacity of the Agency to finalise its annual activities and execute payments as planned and on time. However, the Agency has made use of high carry-overs of committed appropriations from one year to the next.

**Table 21: Budget execution of EU subsidy<sup>56</sup>**

	2013	2014	2015
<b>Budget execution rate</b>	99.7%	100%	100%
<b>Payment rate on expenditure appropriations</b>	91.3%	85.6%	92.9%
<b>Carry-overs (share of committed appropriations)</b>	13.5%	49%	22%

Source: Court of Auditors reports

The European Court of Auditors commented in its reports on ENISA's high carry-overs. The reports stated that the appropriations primarily concerned administrative expenditure. They were intended for IT equipment and furniture.<sup>57</sup> However, in its 2015 "Summary of results from the Court's annual audits of the European Agencies and other bodies" the Court noted that a high level of carry-overs was a frequent comment and concerned many agencies.<sup>58</sup> In 2015, 32 out of 40 assessed agencies were concerned. On average, 36% of committed appropriations for administrative expenditure were carried over. ENISA was thus in 2015 below the average. The execution rates reflect the detailed planning of the EU agencies' budgets and the incentives to ensure full budget execution in order to avoid budget reductions in the following year. This shows that budget implementation could be further improved. ENISA staff and management noted during interviews that there were peaks in spending at the end of each year to ensure that a high budget execution is achieved.

**ENISA shows efficiency in the implementation of its different tasks.** The annual evaluations of ENISA concluded that processes generally were efficient and a clear delineation of responsibilities within the organisation led to a good execution of the work. ENISA staff and Management Board noted in the interviews that regular follow ups on costs were taking place. Expenditure was assessed to be comparable across the projects. Planning and monitoring of implementation of tasks was reported to be working well. ENISA produces a high number of deliverables and generates good outreach in terms of downloads.

**Despite its budget restrictions, the Agency is able to meet its objectives and contributes to some extent to targeted impacts.** As shown in sections 3.2.2.1 and 3.2.2.3 ENISA has been effective in implementing its tasks, though not to the extent of a full achievement of targeted objectives and impacts. ENISA is expected to contribute to a long list of tasks and it has proven difficult to contribute to all targeted objectives due to limited financial and human resources. The achievements that are being made show that considerations on the efficient implementation of resources are being made. Along the same lines, the 2015 evaluation indicated that the Agency risks dispersing already scarce resources across too many, too small activities, decreasing the chance of a real impact overall on NIS.

**Little potential to increase efficiency was identified.** In the annual evaluations of ENISA only small adaptations were suggested to increase efficiency. A main issue raised was the split of ENISA's location which to some extent explains the comparably high share of administrative expenditure of the Agency, as presented in the following section 3.2.3.3. As reported in section 3.2.2.11, monitoring and reporting requirements are generally found to be effective but represent an important burden for staff members.

<sup>56</sup> Annual Activity Report 2014

<sup>57</sup> Court of Auditors (2014): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2014 together with the Agency's reply, and Court of Auditors (2016): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2015 together with the Agency's reply

<sup>58</sup> Court of Auditor (2016): Summary of results from the Court's annual audits of the European Agencies and other bodies for the financial year 2015



3.2.3.3 Adequacy of allocated resources

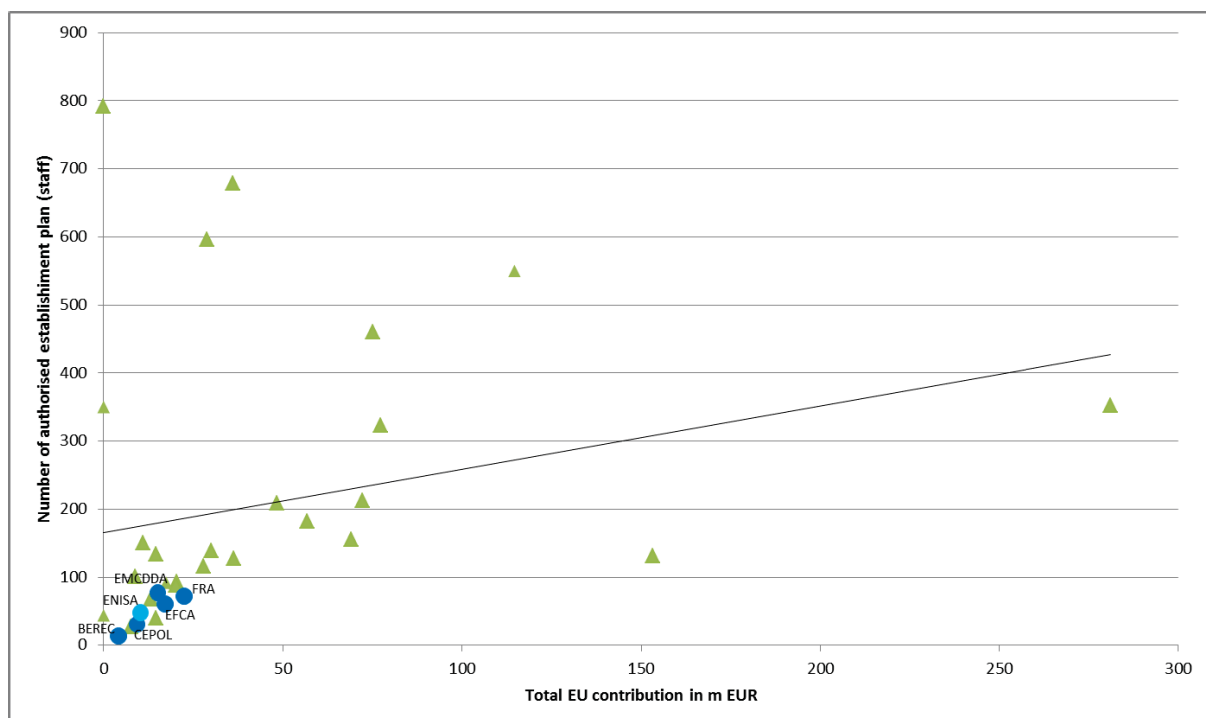
**EQ16: Have the resources allocated to the Agency been sufficient for the pursuit of its tasks (input/output analysis)?**

Compared to other EU agencies ENISA has a small budget and a low number of staff. The share of CAs among the staff is comparably high. There is concern among ENISA’s stakeholders that the Agency does not have sufficient resources to complete its tasks to its full potential; issues relating to the degree to which it is reaching its targeted objectives and impacts are presented in section 3.2.2.1. In particular, more staff is needed. As a consequence of the limited resources, ENISA’s Management Board has to prioritise tasks for the Agency. ENISA relies on the dedication of staff members to ensure the implementation of tasks despite insufficient resources.

**ENISA works with a comparably low budget and a low number of staff.** In 2016, ENISA had 69 staff members of which 24 were CAs. Staff increased by 14% between 2013 and 2016. At the same time, the share of CAs among staff increased from 22% to 35%. To some extent the increasing employment of CAs can be considered a cost-saving measure. The annual evaluations of ENISA’s activities noted that this would also represent a risk of increasing staff turnover and making positions less attractive, thus increasing the recruitment problem.

In fact, ENISA has one of the lowest budgets and levels of human resources compared to all EU agencies. The figure below positions ENISA among 40 agencies covered by the European Court of Auditors report on agencies in 2016. The figure shows that ENISA is among the agencies with the lowest budget and lowest number of staff. However, the figure also shows that comparably small agencies tend to have low staff numbers in relation to their budget when compared with the trend line.

Figure 44: Comparison of EU agencies based on staff and budget, 2017

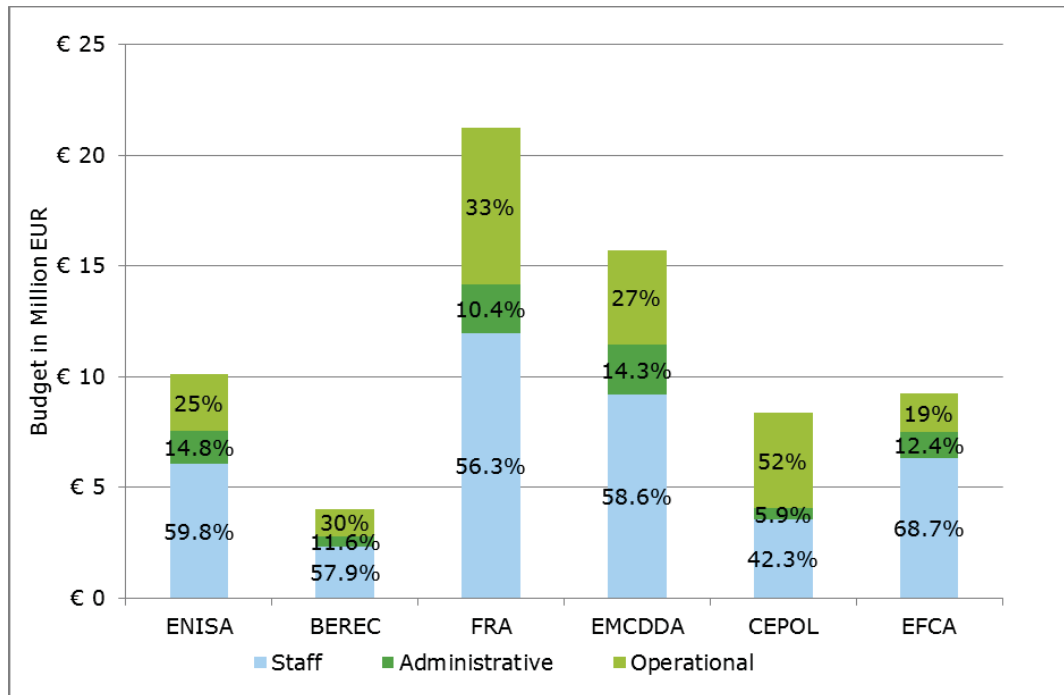


Source: Ramboll Management Consulting, based on Draft General Budget of the EU for the financial year 2018 - Working Document Part III - Bodies set up by having legal personality and Public-Private Partnership (COM(2017) 400 - June 2017)

**The share of administrative expenditure of ENISA is higher than that of other EU agencies considered in the benchmarking exercise.** For example, in 2015 CEPOL, with a total budget similar to ENISA’s but slightly lower staff numbers, used less than 6% of its budget as administrative expenditure. EFCA, even more similar in its total budget and staff numbers to

ENISA, used 12.42% of its budget for administrative expenditure in the same year, while ENISA’s administrative expenditure amounted to 14.8% of its total budget.

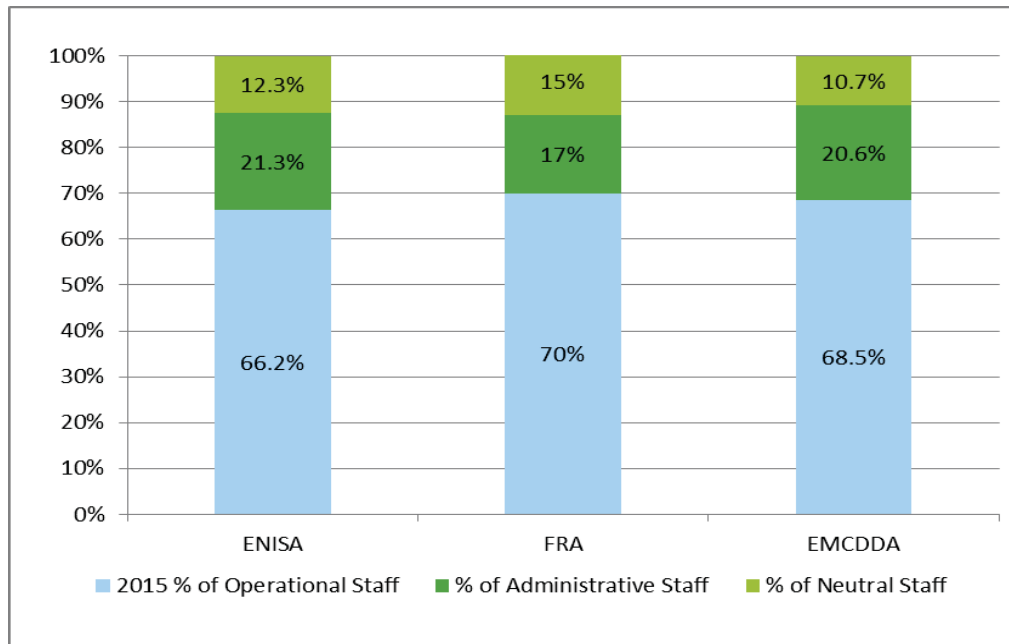
**Figure 45: Distribution of commitment appropriations between staff, administrative and operational expenditure, 2015**



Source: presentation by Ramboll, data from European Commission: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III

When comparing the distribution of staff between operational and administrative roles, as presented in Figure 46 below, it shows that ENISA has with 21% a very similar share of administrative staff as EMCDDA. However, FRA has a share of administrative staff of only 17%. Considering the much higher budget of FRA, this suggests that there are some economies of scale for larger agencies when it comes to the execution of administrative tasks. ENISA, as a small agency, cannot benefit from these.

**Figure 46: Staff distribution between operational and administrative staff for ENISA, FRA and EMCDDA, 2015**

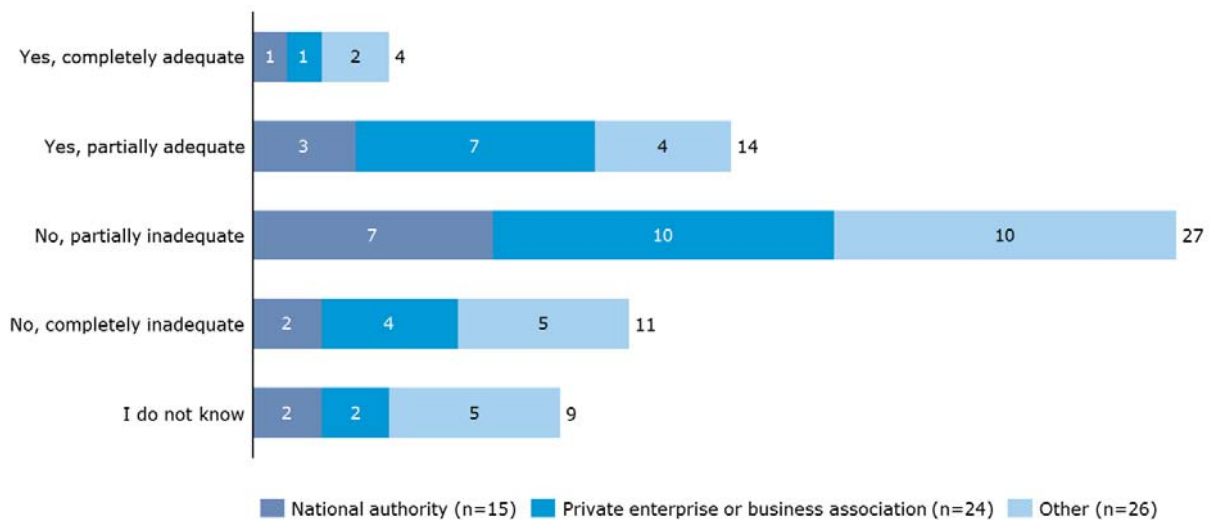


Source: Data gathered through secondary sources and received by ENISA, FRA and EMCDDA.

**There is concern among ENISA’s stakeholders that the Agency does not have sufficient resources to meet the challenges in the cybersecurity area.** Direct stakeholders, such as the Member States, see that ENISA is not able to respond to all their needs. This is reflected in the process of setting ENISA’s annual work programme where it is not possible to include requests from all members of the Management Board. More external stakeholders, such as other EU agencies, stressed that ENISA is also affected in its day-to-day work by its limited resources, for example in it being absent from key cybersecurity events. In the end, as shown in section 3.2.2, ENISA has difficulties to meet its objectives due to an important scope of its mandate which is matched with only a limited number of resources.

Moreover, among the open public consultation respondents, 58% (38 out of 65) considered the size of the agency with 84 staff members to be partially or completely inadequate. There were no notable differences between the different respondent groups.

**Figure 47: Adequacy of the size of the Agency for the work entrusted to it (n=65)**



Source: Open public consultation

Please also refer to the findings on ENISA’s human resources in section 3.2.2.8.

**The insufficient human and financial resources require a lot of dedication from the staff to complete their work and a strict prioritisation of tasks in the work programme.** ENISA is not able to respond to all needs of its stakeholders but has to focus on the most urgent ones. The Management Board has to set priorities within the tasks ENISA is supposed to fulfil based on its mandate.

The limited resources represent a burden on staff who take on additional work. ENISA’s management and Management Board confirmed that ENISA was highly dependent on the dedication and willingness of staff to work overtime in order to implement the work programme and meet expected standards. The small budget also limits ENISA’s visibility. The main concern is to implement the Work Programme rather than build relationships with the stakeholders and, for example, visit all Member States at least once a year or follow up on the use of publications to gain insights on stakeholder requests for future work.

#### 3.2.3.4 Influence of external factors on efficiency

**EQ21: To what extent and how have external factors influenced the efficiency of ENISA?** Evidence shows that ENISA’s efficiency is negatively influenced by limited exchanges with the Commission on its plans for the Agency, and limited exchange and cooperation with other EU bodies.

**Limited communication of the Commission when deciding on (new) tasks for ENISA has a negative impact on the Agency’s efficiency.** The findings from interviews and the annual evaluations of ENISA suggest that there is some concern that the Commission does not sufficiently exchange with the Agency on the feasibility of implementing additional tasks when planning the allocation of new responsibilities. One example given was the role of ENISA under the NIS Directive. ENISA’s staff and management reported that they were not sufficiently able to comment on the feasibility of the tasks foreseen in the legislative text, as developed by the Commission, the European Parliament and the Council. Inefficiencies are created where the Agency then needs to adapt its Work Programme and drop tasks on which work was already planned or even started.

**The fragmentation of cybersecurity across different European Commission DGs, EU bodies and agencies creates inefficiencies where information is not shared or work is duplicated.** Besides ENISA, a number of other EU agencies and bodies (including CERT-EU and Europol’s EC3) are active in different fields relating to cybersecurity. Also a number of European Commission DGs are touching in their work upon cybersecurity issues. These are for example beside DG Connect, DG Energy when covering security of energy grids or the DG for Economic and Financial Affairs when considering security of online banking. ENISA staff and management, as well as other interviewed stakeholders, expressed concern that inefficiencies were caused by two or more organisations working on the same topic and insufficiently sharing information about their work with one another. A further assessment of ENISA’s cooperation with EU bodies and potential duplication of efforts is presented in section 3.2.4.

### 3.2.3.5 Conclusion on efficiency

#### **Conclusion – Efficiency**

*The baseline situation, (established based on an evaluation of all EU agencies including ENISA in 2009<sup>59</sup> and an impact assessment of changes to ENISA’s mandate in 2010<sup>60</sup>) points to ENISA being one of the smallest agencies in the EU. In 2009, ENISA had 57 staff members and a budget of EUR 8 million. Together with its location in Heraklion, this factor was considered to impact on its efficiency. Since then, this evaluation shows that ENISA has slightly grown in size but the resources allocated to it are still not considered to be sufficient. The move of ENISA’s operational staff to Athens increased ENISA’s efficiency.*

ENISA demonstrates efficiency in the implementation of its tasks. ENISA has among the lowest budgets and levels of human resources compared to other EU agencies. In order to complete the various tasks set out in its mandate, ENISA has to be very efficient in the implementation of its budget and carefully consider where resources and working hours can be spent. The Agency develops a high number of publications every year and implements many other activities. Despite its small budget, the Agency has been able to contribute to targeted objectives and impacts, showing efficiency in the use of its budget.

The assessment of the distribution of financial resources showed that while ENISA has a similar budget execution rate, relative to the other agencies reviewed as part of the benchmarking exercise. Its administrative expenditure was higher. The Agency has to fulfil a number of administrative requirements as set by the Commission. These requirements are the same for all EU agencies but weigh more heavily on smaller agencies.

One of the main challenges to the Agency’s efficiency relates to ENISA’s difficulties in recruiting and retaining staff, also compared to other agencies and bodies considered as part of the benchmarking exercise. Despite allocating the highest level of expenditure to staff recruitment in comparative terms, posts are not being filled. The data showed that ENISA’s ability to maintain staff gradually decreased over the years, whereas other agencies such as FRA and ECMDDA maintained roughly the same number of staff.

ENISA’s efficiency is further limited by its split location: having two offices means that the Agency has to implement additional efforts to ensure coordination between the offices and bear the extra travel costs.

### 3.2.4 Coherence

The evaluation criterion coherence assesses how well or not different actions work together.<sup>61</sup> For this evaluation, the focus has been set on the external coherence of ENISA’s work with other EU Agencies and institutions, as well as with the Member States. This section also integrates the positioning exercise, under which the scope of services and products offered by ENISA has been compared to that of other EU agencies and bodies, as well as to Member States’ cybersecurity organisations. The complete data of the positioning exercise is presented in Appendix 4.

<sup>59</sup> Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

<sup>60</sup> European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

<sup>61</sup> Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

**Table 22: Evaluation questions covered under the coherence criterion**

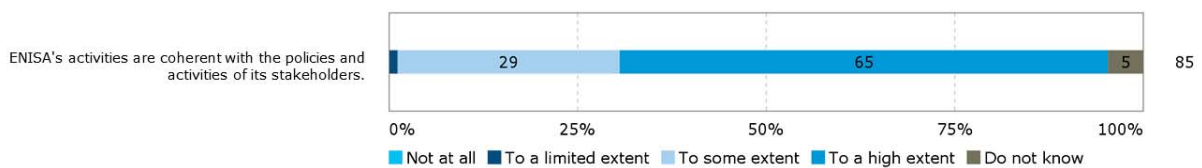
Main evaluation question	Other evaluation questions
<b>EQ24: To what extent are ENISA activities coherent with the policies, strategy documents and activities of other stakeholders?</b>	<p><b>Retrospective</b></p> <p>EQ9: How does ENISA compare to the other EU and national bodies offering similar services in relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency?</p> <p>EQ10: To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements?</p> <p>EQ22: To what extent is ENISA acting in cooperation with <i>the European Commission and other EU bodies</i>, to ensure complementarity and avoid duplication of efforts?</p> <p>EQ23: To what extent is ENISA acting in cooperation with the <i>Member States</i> to ensure complementarity and avoid duplication of efforts?</p> <p>EQ25: Are the procedures put in place effective to ensure that ENISA's cooperation activities are coherent with the policies and activities of its stakeholders?</p> <p>EQ26: What are the risks/sources of overlaps/conflict of interests?</p>

3.2.4.1 ENISA’s cooperation with the European Commission and other EU bodies

**EQ22: To what extent is ENISA acting in cooperation with the European Commission and other EU bodies to ensure complementarity and avoid duplication of efforts?**  
 ENISA’s activities were found to be generally coherent with the activities of the European Commission and other EU bodies. Some cooperation is taking place and leads to complementarity. Nevertheless, the cooperation between ENISA and the different Commission DGs could be increased. It seems as if so far there is no reflex to involve ENISA in all Commission activities concerning cybersecurity. With some EU bodies, including the Commission’s DG Energy and EC3, ENISA is successfully cooperating by developing and implementing common activities.

**ENISA’s activities were identified as being coherent with the policies and activities of its stakeholders.** Almost all respondents (94%) to the survey of ENISA staff and direct stakeholders regarded ENISA’s activities as being coherent with the policies and activities of its stakeholders to some or to a high extent.

**Figure 48: Extent of agreement or disagreement with the following statement on the coherence of ENISA’s activities**



Source: Survey of ENISA staff and direct stakeholders

The coherence of ENISA’s activities with EU political priorities was also confirmed during interviews as outlined in 3.2.1.2.

**There were diverging assessments of cooperation between ENISA and the European Commission and other agencies but a desire for more cooperation was expressed.** The annual evaluations of ENISA’s activities in 2014 and 2015 concluded that the Agency actively pursued cooperation with other relevant EU stakeholders. Many interviewees across all stakeholder groups noted that coordination efforts were high and systematic exchanges took place but were limited by constraints in resources on ENISA’s side. In contrast, even more interviewees, including several Commission representatives thought that cooperation between ENISA and the Commission

could be further improved. The location of ENISA was cited as one source for this lack of coordination by several members of the Commission. No overlaps or conflicts of interest were identified between ENISA and the Commission due to lacking cooperation but stakeholders saw room for improvement to allow for more coordinated planning of ENISA's activities. From the perspective of ENISA's staff and management, as well as the Management Board, a desire was expressed that the different Commission DGs should rely more on ENISA's services and systematically involve the Agency when dealing with cybersecurity issues. Cooperation between the DG JRC and ENISA was generally assessed to be limited to specific projects. The DG JRC conducts research on request by DG CNECT, and where ENISA covers the same issue some degree of coordination is implemented to avoid duplication of work. However, there was no evidence of more systematic coordination to ensure synergies.

**The cooperation with other EU bodies and agencies could be further improved to enhance synergies.** There are some efforts by ENISA to cooperate with other EU bodies like Europol's EC3. EC3 is represented in ENISA's PSG and the organisations have cooperated in the past on some activities, like the organisation of workshops aimed at defining a common taxonomy between CERTs/CSIRTs and law enforcement.<sup>62</sup> However, the European landscape of cybersecurity remains fragmented with many actors covering specific fields and without an organisation acting as an umbrella for these different activities guiding the distribution of tasks. Duplications of efforts easily arise, as stakeholders are not fully aware of all activities of the different organisations active in the field of cybersecurity. A detailed assessment of overlaps and complementarities between ENISA, CERT-EU, the DG JRC and EC3 is presented in section 3.2.4.3. In particular, the positioning of ENISA relative to CERT-EU showed a risk for overlap in certain areas.

#### 3.2.4.2 ENISA's cooperation with the Member States

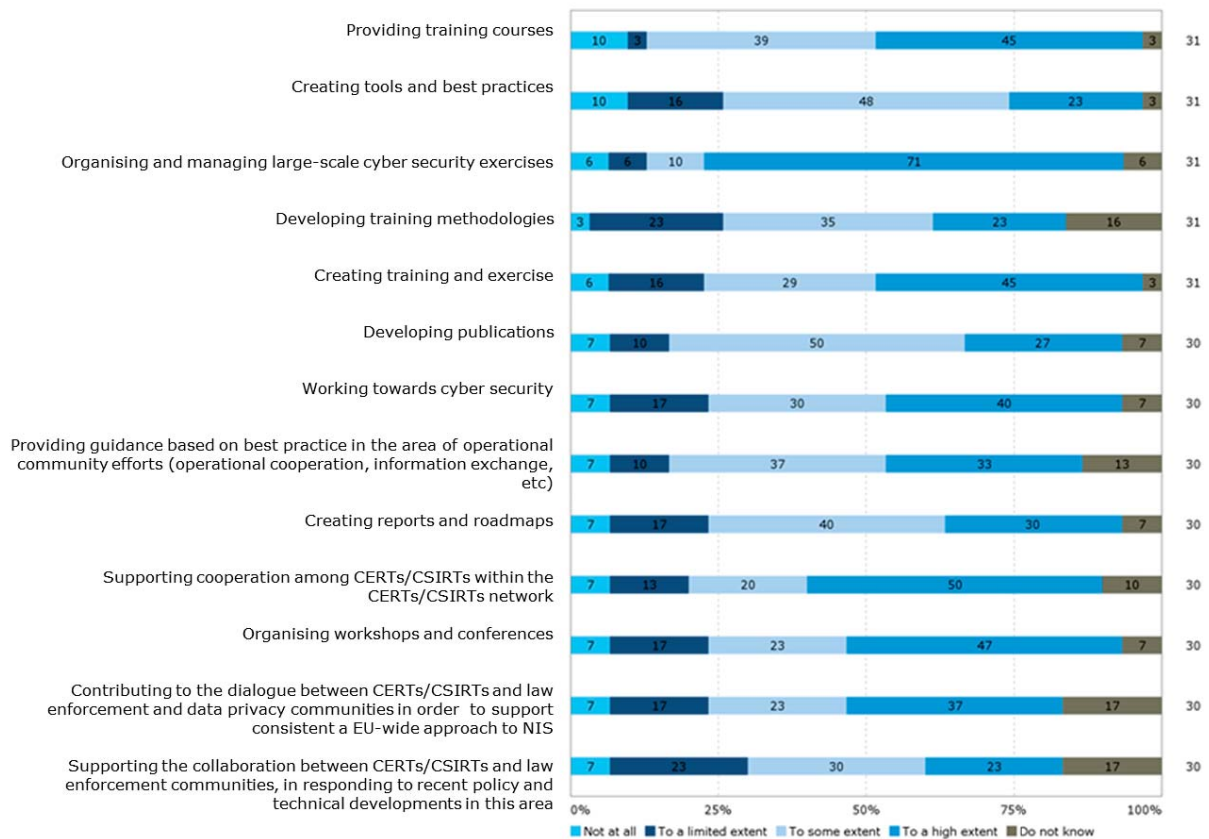
##### **EQ23: To what extent is ENISA acting in cooperation with the Member States to ensure complementarity and avoid duplication of efforts?**

In general, ENISA's activities are coherent with the activities of the Member States. There is a strong coherence and there are synergies between ENISA's activities and those of the national CERTs/CSIRTs. ENISA is duplicating the efforts of some of the Member States' national cybersecurity authorities. This applies mainly to Member States with a lot of experience and resources in cybersecurity, whereas Member States with fewer resources and capacities are more reliant on ENISA's support.

**Overall, there is a good level of cooperation between Member States and ENISA which ensures complementarity and avoids a duplication of efforts.** CERT/CSIRT stakeholders were asked in a survey to assess the extent to which the activities conducted by ENISA to support CERTs/CSIRTs over the 2013-2016 period were coherent with and complementary to (i.e. not overlapping or duplicating) what CERTs/CSIRTs were doing. For each of ENISA's activities, a large majority of respondents saw a high or some coherence with CSIRT's activities. The three most coherent activities cited were "organising and managing large-scale cybersecurity measures", "supporting cooperation among CERTs/CSIRTs within the CERT/CSIRT network" and "organising workshops and conferences". The activity that was seen as least complementary with CERTs/CSIRTs' activities was "supporting the collaboration between CERTs/CSIRTs and law enforcement communities, in responding to recent policy and technical developments in this area". Also "creating tools and best practices" and "developing training methodologies" were considered to be less complementary.

<sup>62</sup> <https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop>

**Figure 49: Extent to which ENISA’s activities towards CERTs/CSIRTs were coherent with and complementary to (i.e. not overlapping or duplicating) what CERTs/CSIRTs were doing**



Source: CERT/CSIRT survey

**To some extent duplication of efforts can be observed between Member States with strong expertise in cybersecurity and ENISA.** The positioning exercise showed a duplication of efforts between ENISA and these Member States, as can be seen in the analysis of the services of ANSSI, NCSC and INCIBE (see section 3.2.4.3). The same activities are however benefiting Member States which do not have the same capacities and resources as their larger neighbours.

3.2.4.3 Positioning of ENISA relative to other EU bodies and national organisations active in the NIS area

**EQ9: How does ENISA compare to the other EU and national bodies offering similar services in relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency?**

ENISA is able to some extent to respond to the cybersecurity needs of its constituency. There are however certain needs being covered by other EU bodies or within the Member States. Considering the growth in relevance of activities in promoting NIS in the past few years, there is room for a lot of different actors to cover the various thematic fields and the different needs of a growing group of stakeholders concerned by NIS. ENISA is not able to respond to all these needs but meets stakeholders’ expectations in specific areas, such as the implementation of exercises and fostering cooperation between the Member States.

In comparison to CERT-EU, ENISA is perceived as being less flexible in responding to unforeseen needs but is valued for its independent point of view. In those Member States where resources and capacities in the area of cybersecurity are high, national sources of information are preferred over ENISA’s reports as they come in national language and are perceived to be more tailored to given



Member States' circumstances. However, for stakeholders in Member States with fewer resources being invested in cybersecurity, ENISA represents a valued source of information and provider of services.

As presented in section 3.2.1.3, most of ENISA's stakeholders do not expect ENISA to cover digital privacy needs.

**EQ10: To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements?**

ENISA was found to be only partially effective in the achievement of targeted results, primarily due to its limited resources and the broad mandate to be covered. Compared to other current EU bodies active in the area of NIS, ENISA seems to be more restricted in its capacity to effectively achieve results. For example, CERT-EU has for some stakeholders become the preferred source of expertise when setting up a CERT or when searching for information on threats even though its mandate points to it being a body at the service of EU institutions, agencies and bodies.

Compared to Member States' organisations, ENISA provides value in particular where it brings together stakeholders from across the EU and representing different sectors. However, the degree to which ENISA has been effective at achieving its intended results varies from one Member State to another. In general terms, the cybersecurity bodies of more experienced Member States are effective in policy development, capacity building and the provision of expertise, while in Member States with less capacity and expertise, ENISA's activities lead to better results.

**EQ26: What are the risks/sources of overlap/conflict of interests?**

The evaluation identified risks of overlap between ENISA and CERT-EU, specifically in the area of fostering cooperation across the Member States and the advice provided to CERTs/CSIRTs. CERT-EU is implementing activities that do not only target its constituents (i.e. the EU institutions, agencies and bodies) but also those of ENISA. In the provision of analysis of risks and threats and training activities, CERT-EU has become a relevant source for national public and private stakeholders. No overlaps were identified between ENISA and EC3. The DG JRC and ENISA cover similar topics and have published reports with comparable content, but the DG JRC implements research and testing in the field of cybersecurity which is something that does not fall within the mandate of ENISA. There is no direct coordination of the work between ENISA and the DG JRC which gives rise to a potential for a duplication of efforts. However, DG CNECT coordinates the distribution of work, thereby reducing this potential for a duplication of efforts.

Member States with strong capacities in cybersecurity tend to implement similar activities as ENISA. While these are focussed on the national context and produced in the national language, there is some doubt whether ENISA actually needs to provide similar services. In some cases the EU level perspective can add another useful layer of information and exchange, but in other cases it is not clear whether ENISA adds any value. This however applies only to Member States with strong capacities and experience in cybersecurity. Member States with fewer resources rely on ENISA's services.

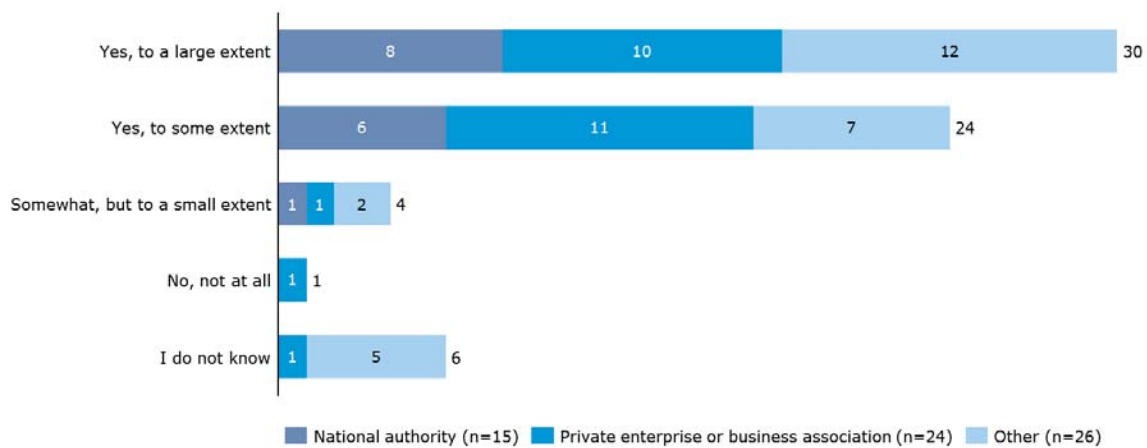
This section of the report is based on the positioning exercise which evaluated how ENISA is positioned vis-à-vis a sample of other EU and national bodies working on cybersecurity and digital privacy on the basis of the services offered and the needs expressed by the Agency's stakeholders. The organisations covered in the positioning exercise are CERT-EU, EC3, the DG JRC, the French ANSSI, the Spanish INCIBE and the Dutch NCSC. ENISA's activities have been mapped across the Agency's four tasks: enhancing cooperation, develop and maintain a high level of expertise,

enhancing capacity building and developing and implementing policies. Sub-categories of these have been developed to understand more specific tasks that have been implemented. The complete mapping of ENISA’s services and the detailed assessment of the services of the other organisations under review is attached in Appendix 4. The methodology applied for this exercise is described in section 2.3.

**ENISA responds to some extent to the needs of its constituency by providing expertise, enhancing capacity and cooperation, and supporting the development and implementation of policy.** As outlined in section 3.2.1, ENISA’s focus is set on cybersecurity needs. There is less demand for support in the digital privacy area. The findings of the evaluation also show that ENISA is not able to meet all the needs of its stakeholders, primarily due to its limited resources.

Respondents to the open public consultation were asked to assess whether the activities of ENISA were coherent with the policies and activities of their own organisation. 83% of respondents (54 out of 65) considered ENISA’s activities to be to a large or to some extent coherent (e.g. take into account, do not overlap, do not conflict with) with the policies and activities of their organisation. This was the case for respondents across all categories.

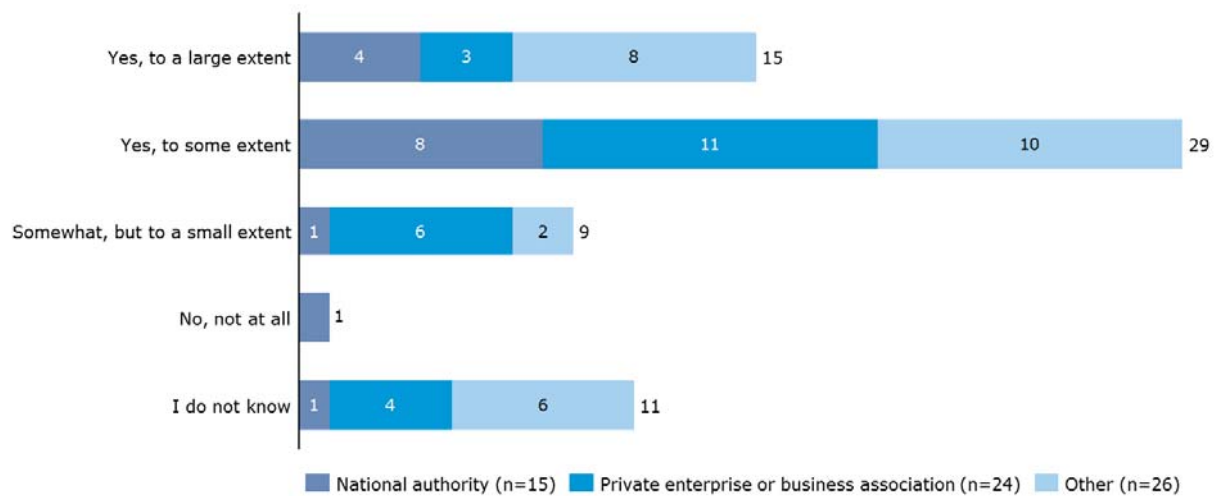
**Figure 50: Extent to which ENISA’s activities are coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of respondent’s organisation, (n=65)**



Source: Open public consultation

Respondents were further asked whether they considered ENISA’s activities to be coherent with the policies and activities of its stakeholders, including other EU agencies and bodies. In total, 68% of respondents (44) considered ENISA’s activities to be largely or to some extent coherent. This is comparably lower than for the coherence with respondents’ own organisation. Also the share of respondents considering ENISA’s activities to be coherent to a large extent was lower for this second question (46% against 23%).

**Figure 51: Extent to which ENISA’s activities are coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of its stakeholders, (n=65)**



Source: Open public consultation

Respondents who indicated in one or both of the questions that ENISA’s activities were coherent to only a small extent or not at all, were asked to provide further explanations. Those that considered ENISA’s activities not to be coherent with their own organisation’s activities mainly referred to issues with ENISA being up-to-date with the latest developments with regard to legislation or technical evolution. Respondents that saw ENISA’s activities to be coherent only to a small extent or not at all with policies and activities of other stakeholders mentioned a lack of clear distinction between the roles of ENISA and CERT-EU. Respondents also mentioned potential overlaps with other organisations (including the cybersecurity bodies of the Member States and the European Cyber Security Organisation).

## **EU bodies**

### **ENISA and CERT-EU**

**A comparison between the activities of ENISA and those of CERT-EU shows that there are some complementarities but also a risk of overlap.**<sup>63</sup> CERT-EU is the Computer Emergency Response Team for the EU institutions, agencies and bodies, established in 2012. The team is made up of IT security experts from the main EU institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, and the Economic and Social Committee).<sup>64</sup> Its Steering Board is composed of one member of senior management designated by each of the EU institutions or bodies, the Commission may designate up to two further members. EU agencies are represented by ENISA.<sup>65</sup> CERT-EU’s mission is to support the EU institutions, agencies and bodies to protect themselves against cyber-attacks. This is done by providing information on threats, vulnerabilities and protection measures, by disseminating information to its constituents in case of an attack and to ensure coordination of response.<sup>66</sup> The activities also include the delivery of extended security services, such as

<sup>63</sup> According to the Commission’s Better Regulation Guidelines, “complementarity” means that similar initiatives (of different organisations) contribute to the same overall objective and approach it from different perspectives. “Overlap” signifies that several interventions are delivering the same effects for the same people and at the same time.

<sup>64</sup> [https://cert.europa.eu/cert/plainedition/en/cert\\_about.html](https://cert.europa.eu/cert/plainedition/en/cert_about.html)

<sup>65</sup> Council of the European Union (2014): Information note - Recommendations by the inter-institutional Steering Board of the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) on the future mandate, governance, organisational setup, staffing and funding of CERT-EU. Brussels, 9 September 2014 – document number 12992/14

<sup>66</sup> CERT-EU (2013): RFC 2350

penetration testing and vulnerability assessment. The scope of CERT-EU's activities thus covers prevention, detection, response and recovery.

In general, the services provided by CERT-EU to the EU institutions, bodies and agencies are complementary to the work undertaken by ENISA to coordinate and promote cooperation at EU level among the Member States. The work of both bodies touches upon the field of prevention, for example, through the preparation of regular threat analysis reports and knowledge and methodology enhancement. In the field of threat analysis, the two bodies complement one another as CERT-EU provides daily, current information, while ENISA's Threat Landscape reports are published on an annual basis, thus providing more in-depth assessments. In theory, the targeted audience of the two bodies differs. However, CERT-EU's mandate includes a provision stating that the body may undertake any activities going beyond its mandate with the prior approval of the Steering Board.<sup>67</sup> In practice, CERT-EU has become a reference point for technical advice for organisations interested in building up a CERT. CERT-EU also acts as a point of exchange between the Member States on cybersecurity issues. The body is aware of threats and issues in the different Member States and to some extent shares this information with the other Member States. Here CERT-EU enhances capacity and cooperation beyond its core stakeholders and implements activities that would also be within the scope of ENISA's mandate. CERT-EU responds to a need that ENISA has not been able to fill due to limited financial and human resources (see section 3.2.3.3).

A high number of interviewees from different stakeholder groups expressed concern about this and saw a risk of overlap in the activities of the two bodies. For example, CERT-EU's website provides a news monitor on vulnerabilities, threats and incidents, but also on the activities of different CERTs/CSIRTs. Another example of CERT-EU's activities targeted at national CERTs/CSIRTs were workshops on Malware Information Sharing Platforms. The described activities do not represent an overlap with ENISA's activities because the Agency does not provide the same services at the moment. However, they fall within the remit of ENISA's mandate and there is a risk of duplication of work if both organisations were to provide similar services to national CERTs/CSIRTs.

**CERT-EU seems to be closing a gap in services that are needed by ENISA's constituents, but that the Agency, as a decentralised, neutral source, cannot provide due to its limited resources.** According to some of the interviewed stakeholders (direct stakeholders), CERT-EU is being contacted by stakeholders beyond its constituents for specific advice, for example on creating a CERT. CERT-EU is considered to be quicker in providing responses to such specific requests. CERT-EU also has the advantage of being located in Brussels which a few interviewees suggested was one of the reasons why CERT-EU was considered to be more accessible by CERTs/CSIRTs but also the broader stakeholder community. While this study showed that ENISA's lack of visibility is not only due to the perceived distance of its location to Brussels, these stakeholder views show that there is some importance placed on the Agency's location when comparing it to other bodies or agencies. As CERT-EU is an inter-institutional body and not a decentralised agency it can more easily ensure direct cooperation with the different DGs of the Commission. However, as a decentralised agency, ENISA is recognised by the Member States and the private sector as a neutral and independent source of information. This was reflected in the open public consultation, where national authorities very frequently and respondents from the private sector frequently indicated "the products and services provide information that is independent and neutral" as a reason for using ENISA's products and services. Interviewees from ENISA's staff and Management Board reported that with additional resources some of the services provided by CERT-EU could also be implemented by ENISA. However, as presented in section 3.2.3.3, with limited staff available ENISA needs to focus on given tasks in order to be able to implement its work programme.

---

<sup>67</sup> Council of the European Union (2015): Information note - CERT-EU mandate, service catalogue and information sharing and exchange framework. 3 March 2015 – document number 6738/15

## ENISA and EC3

**Little to no overlap was identified between ENISA and Europol's EC3; the two organisations seem to cooperate well.** The European Cybercrime Centre was set up by Europol in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime.<sup>68</sup> The organisation implements capacity building and policy development and implementation in the area of cybercrime. There are some topics in which the activities of ENISA can touch upon what EC3 does. For example, EC3 works on the development of a common taxonomy for CERTs/CSIRTs to facilitate cooperation and implements training to authorities in Member States. The evaluation findings show that in these cases ENISA and EC3 tend to work together rather than creating duplications.

**While there is some institutionalised coordination between ENISA and EC3, day-to-day cooperation could be further improved.** ENISA sits on the Steering Board of EC3. In turn, EC3 is represented in ENISA's PSG. This allows for coordination of the organisations' work. However, interviewees suggested that there could be even more coordination to avoid duplication of efforts on a daily level. While the reports of EC3 take a cybercrime perspective on topics that might be covered by ENISA, ENISA staff and management suggested that this does not fully avoid any overlaps.

## ENISA and the DG JRC

**Generally, there is complementarity between ENISA's work and that undertaken by the DG JRC Science Hub as the organisations vary in the stakeholders they target and approach issues from different perspectives.** The DG JRC is the Commission's science and knowledge service, carrying out research in order to provide independent advice and support to EU policy. The DG JRC conducts research in the NIS area on issues that are very similar to what ENISA covers. However, as a research centre, the DG JRC implements research and testing which in this form is not provided by ENISA. The DG JRC's activities primarily come in the form of a contribution to the Commission's work and are in this sense complementary to ENISA's work which is more targeted at Member States and a broader stakeholder group. For example, the DG JRC published a risk assessment of cloud computing for citizens in 2012.<sup>69</sup> ENISA published a study on the same topic in 2017, but provided an overview of different components to protect data in the cloud and discussed challenges to privacy as well as security.<sup>70</sup> With an overview of different benefits and weaknesses, ENISA's publication was more directly targeted to the Agency's stakeholders.

Where the DG JRC targets stakeholders beyond the Commission with its work, the organisation complements ENISA's work by taking different angles. Through the ITIS project, the DG JRC provides news bulletins on vulnerabilities and threats for the energy sector in the EU and prepares reports on foresight for emerging threats. This complements ENISA's annual threat landscape reports which cover a broader range of sectors. In the past, the two organisations have cooperated in the organisation of exercises such as the first Pan-European CIIP exercise in 2010.

<sup>68</sup> <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

<sup>69</sup> JRC (2012): Will the cloud make the citizen more vulnerable? Risk and vulnerability assessment in times of cloud computing. Available at: <https://ec.europa.eu/jrc/en/publication/contributions-conferences/will-cloud-make-citizen-more-vulnerable-risk-and-vulnerability-assessment-times-cloud-computing>

<sup>70</sup> ENISA (2017): Privacy and Security in Personal Data Clouds. Available at: <https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds>

**There is a risk of duplication of efforts between ENISA and the DG JRC as both organisations cover very similar issues and no systematic coordination is in place.** There are a number of topics on which both bodies are conducting research and producing publications. This includes the threat analysis, as mentioned previously, but also the identification of good practices and recommendations as well as knowledge and methodology enhancement. For example, ENISA published a study on approaches to risk assessment for cybersecurity in the Member States in 2013.<sup>71</sup> This study had a strong focus on the protection of critical infrastructures. In 2015, the DG JRC published a report entitled “Risk assessment methodologies for critical infrastructure protection”<sup>72</sup> also assessing Member States’ practices. With such similar focus of their work, there is a clear need to ensure coordination or at least some awareness of what is being done in each organisation to avoid duplication of work. During the interviews ENISA management noted that there was no formal coordination process set up between ENISA and the DG JRC, but that it was rather DG CNECT that guided the scope of the work of DG JRC in the cybersecurity area and thus looking to identify any potential overlap with ENISA’s work. While there seems to be well functioning ad-hoc/informal coordination, whereby the DG JRC and ENISA are aware that they are working on similar issues, a risk of duplication of efforts remains if this awareness is not systematically ensured.

### **National organisations**

ENISA’s activities have been further compared to those of national bodies. Organisations from Member States with rather developed experience and capacities in the field of NIS have been selected for this purpose.

**The Spanish INCIBE implements similar activities to ENISA in the area of expertise, policy development, capacity building and cooperation; in most fields they cooperate with and complement ENISA, there is however some potential overlap.** The Spanish National Cybersecurity Institute is a subsidiary of the Secretary of State for the Information Society and Digital Agenda (SESIAD) and acts as a point of contact in Spain on cybersecurity. Its activities include research, service delivery and coordination.<sup>73</sup> INCIBE organises workshops together with ENISA which are intended to develop and implement policies and to foster cooperation between the Member States.

INCIBE’s expertise and capacity building is in Spanish and limited to stakeholders in Spain. It is however not clear to what extent ENISA can provide additional value to stakeholders in the Member State, specifically through its threat analysis reports, support in the field of critical infrastructures and incident analysis.

**The Dutch NCSC conducts very similar activities to ENISA by providing expertise, developing and implementing policies and enhancing capacity building.** The National Cyber Security Centre, working under the Ministry of Security and Justice, is the national centre in charge of promoting cybersecurity and ensuring capacity for response in the Netherlands. The NCSC complements ENISA’s activities in the area of fostering cooperation between the Member States and other NIS related communities and by conducting cyber exercises with its neighbouring countries. Risks of overlap were identified in the threat analysis reports, provision of good practices, white papers for the Dutch government and trainings which CERTs/CSIRTs attend. Similar to the case of INCIBE, it is not clear whether ENISA’s activities in these specific areas are adding to what is done at national level.

<sup>71</sup> ENISA (2013): National-level Risk Assessments. Available at: [https://www.enisa.europa.eu/publications/nlra-analysis-report/at\\_download/fullReport](https://www.enisa.europa.eu/publications/nlra-analysis-report/at_download/fullReport).

<sup>72</sup> JRC (2015): Risk assessment methodologies for critical infrastructure protection. Available at: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf>

<sup>73</sup> <https://www.incibe.es/en>

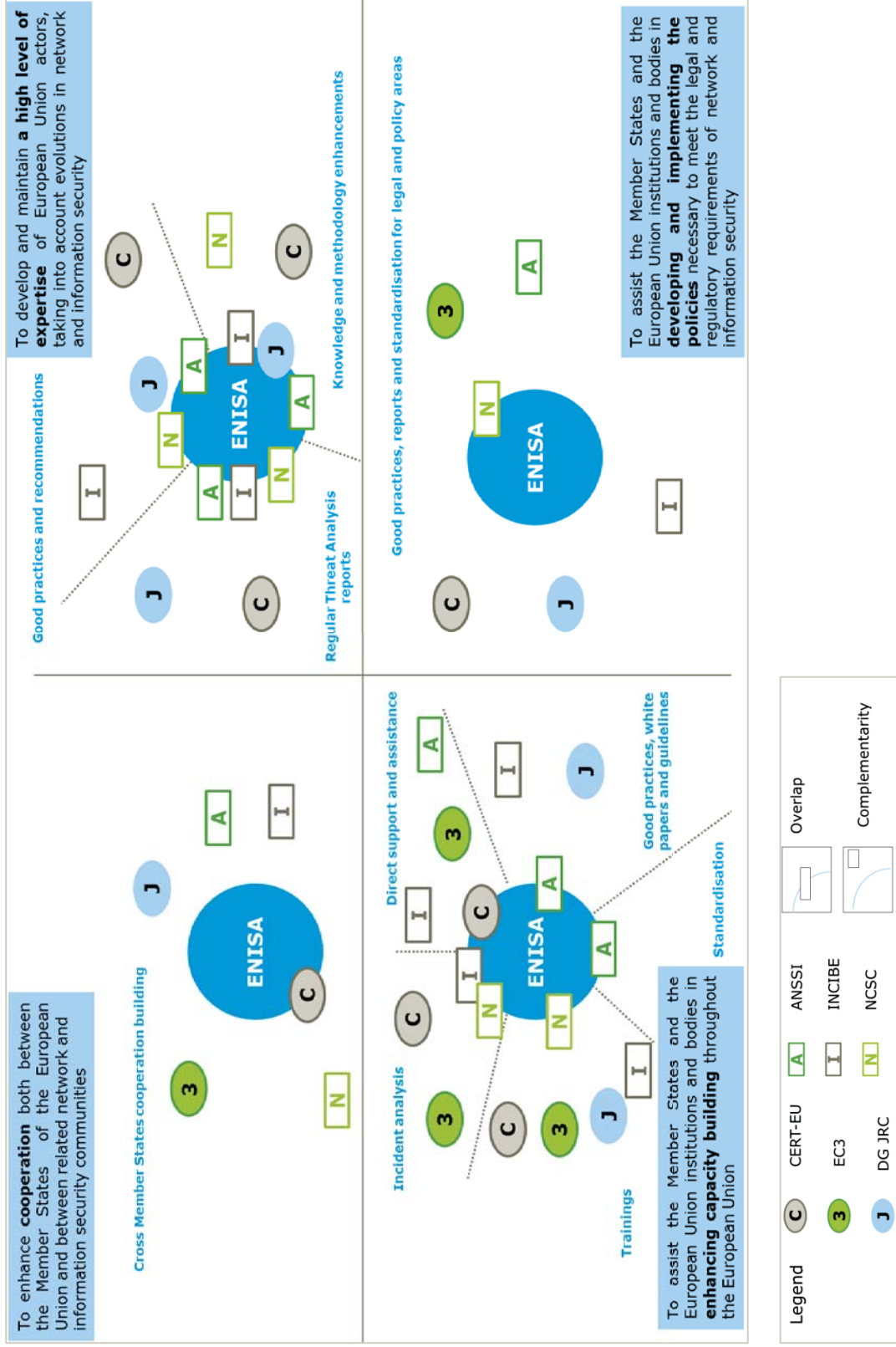
**The French ANSSI collaborates with ENISA to enhance cooperation and develop policy but activities overlap in the area of providing expertise to stakeholders and some capacity building activities.** The National Agency for the Security of Information Systems which works under the General Secretary of Defence and National Security is responsible for promoting cybersecurity and ensuring capacity for response in France. By organising events in collaboration and by supporting ANSSI to foster cybersecurity policy in France, ENISA and ANSSI complement each other. Although ANSSI provides its expertise in the form of reports and recommendations in French, there is a lot of overlap in terms of the topics covered and thus it can be questioned to what extent ENISA's activities are needed in addition.

**There is strong coherence between the needs of Member States with fewer resources and capacities, and the services provided by ENISA.** The national organisations selected for the positioning exercise are those of Member States with a comparably high budget and capacity in the area of cybersecurity. Many other Member States do not allocate the same resources to cybersecurity and thus rely more on the services provided by ENISA. This is in particular the case in the areas of capacity building, provision of expertise and support in the implementation of policies, as presented in section 3.2.1.4. The evaluation of ENISA's activities in 2015 also found that there is a tendency that Member States with lower NIS capacity or maturity benefit in particular from the exchange of best practice (e.g. on national cybersecurity strategies), while Member States with higher NIS capacity tend to benefit from technical studies, and contribute with best practices. Hence, there is less of a risk of duplication of efforts between ENISA and such Member States where ENISA's spectrum of services area relevant overall.

**Stakeholder interviews show that some of the activities are more effective when implemented by ENISA rather than at national level. For other activities the cybersecurity organisations of the Member States assessed in the positioning exercise are better equipped.** In general, ENISA's expertise is valued in all Member States as providing an additional, independent source of information. Often the comparison across the EU provides added value. However, some Member States (those with high resources for cybersecurity) were rather critical in the interviews, stating that ENISA's reports did not match the quality and topicality of national-level reports. By contrast, ENISA has developed a strong capacity to bring different stakeholders to the table and ensure cooperation across the EU, adding to the stakeholders that Member States could reach individually when organising events or exercises. With regard to policy development and implementation, Member States' cybersecurity organisations tend to have a more direct link to their government than what ENISA has been able to build. Here national organisations can provide legal and policy input more effectively. Finally, the quality of ENISA's cyber exercises is considered high and allows ENISA to make an important contribution to capacity building, especially in Member States with fewer resources and capacities. However, some of the Member States have organisations which are also strong in providing training and organising smaller scale exercises.

The complementarities and risks of overlap between ENISA and the assessed EU bodies and national organisations are summarised in further detail in Figure 52 below. The activities of ENISA have been structured across the four main tasks: enhancing cooperation, develop and maintain a high level of expertise, enhancing capacity building and developing and implementing policies. Sub-categories of these tasks present more specific activities. A potential overlap of an organisation's activities with those of ENISA is indicated by a visual overlap of the symbol used for an organisation with the blue circle in middle, representing ENISA. The symbols of organisations that do not overlap with the blue circle representing ENISA represent organisations that implement the described activity or service, but where there are sufficient differences (e.g. in the approach, the scope, the target group) in the activities implemented that no potential overlap was identified. The complete assessment on which this figure is based can be found in Appendix 4.

**Figure 52: Positioning map**





#### 3.2.4.4 Procedures to ensure coherence

##### **EQ25: Are the procedures put in place effective to ensure that ENISA's cooperation activities coherent with the policies and activities of its stakeholders?**

Only few coordination procedures are in place to ensure coherence. As potential overlaps have been identified there is a need to develop better procedures to avoid overlaps in the future.

**Besides the representation in the Management Board or the PSG, few coordination procedures are in place that aim at ensuring the coherence of ENISA's activities with the policies and activities of its stakeholders.** The 2014 and 2015 annual evaluations of ENISA's activities did not identify many formal mechanisms in place to ensure coherence. It can be concluded that based on being represented in the Management Board or the PSG and the feedback process in connection to the work programmes, the Commission, other EU bodies and agencies, and the Member States are able to point to any potential overlaps.

**The identified risks of overlap suggest that there is a need to ensure further coordination between ENISA and some of its stakeholders.** In particular with CERT-EU there is a need to clarify roles. The Commission foresees to present a cooperation blueprint to handle large-scale cyber incidents on the EU level in the first half of 2017.<sup>74</sup> Based on this, the roles of CERT-EU and ENISA when handling mayor incidents could be clarified. As shown in section 3.2.4.1, there is a need for more trust and willingness to cooperate between the two organisations. In theory, one solution could be to merge ENISA and CERT-EU into one organisation. More generally, there is a need to consolidate the fragmented field of cybersecurity and ensure coordination across the different actors involved at EU level but potentially also beyond.

#### 3.2.4.5 Conclusion on coherence

##### **Conclusion – Coherence**

*The baseline situation (established based on an evaluation of all EU agencies including ENISA in 2009<sup>75</sup> and an impact assessment of changes to ENISA's mandate in 2010<sup>76</sup>) points to coherence between ENISA and the EU strategies and policies. Unlike over the period 2013-2016, there were no other EU agencies or bodies covering cybersecurity. Therefore no overlaps were identified in the 2009 evaluation.*

ENISA's activities are generally coherent with the policies and activities of its stakeholders but there is a need for a more coordinated approach to cybersecurity at EU level. The findings of the evaluation study suggest that the potential for cooperation between ENISA and the European Commission, as well as other EU bodies, is not fully utilised. There is room for more coordination to ensure better coherence and complementarity in order to attain increased NIS in Europe. For example, enhanced coordination between ENISA and the DG JRC would avoid the current (although low) risk of overlap. In addition, the division of responsibilities between ENISA and CERT-EU should be clarified.

ENISA's activities are largely coherent with the work done at national level in the area of cybersecurity. Coherence is particularly strong between the CERTs/CSIRTs and ENISA. Some

<sup>74</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry; COM (2016) 410 final

<sup>75</sup> Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

<sup>76</sup> European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

overlaps between ENISA’s activities and those of Member States with strong cybersecurity expertise were identified, but Member States with less capacity and resources in the area of cybersecurity still benefit from these activities.

### 3.2.5 EU-added value

EU-added value looks for changes which can be assigned to EU intervention, rather than any other factors.<sup>77</sup> To some extent the questions presented below bring together the findings of the previous evaluation criteria. This section responds to prospective questions as listed in the roadmap for the evaluation of ENISA. In addition to the questions from the roadmap, a retrospective sub-section on the added value of ENISA over the years 2013-2016 has been added.

The following questions are responded to in this section:

**Table 23: Evaluation questions covered under the EU added value criterion**

Main evaluation question	Other evaluation questions
<p><b>EQ27: What would be the most likely consequences at the EU level of stopping ENISA?</b></p>	<p><b>Retrospective</b></p> <p>EQ45: What has been the added value of having an EU cybersecurity agency such as ENISA over the period 2013-2016?<sup>78</sup></p> <p><b>Prospective</b></p> <p>EQ28: How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place?</p> <p>EQ35: What would be the most likely consequences at the EU level of stopping ENISA's activities?</p>

#### 3.2.5.1 EU-added value of ENISA

**EQ45: What has been the added value of having an EU cybersecurity agency such as ENISA over the period of 2013-2016?**

ENISA is providing significant added value to the cybersecurity activities implemented in the Member States. Most importantly, ENISA ensures cooperation in the prevention and mitigation of cybersecurity incidents. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. In addition, the Agency’s activities to provide expertise and capacity building represents important added value for Member States with little national resources for cybersecurity.

**ENISA fills a gap at EU level.** Without ENISA there would be no EU-level mechanism seeking to bring together and bridge the diverse field of cybersecurity. Through its community-building objective in particular, ENISA brings together a variety of stakeholders representing different sectors. As mentioned in section 3.2.2.1, ENISA has made a clear contribution to the overall goal of increasing network and information security in Europe, including by sharing good practices in NIS (as shown in the stakeholder survey carried out by the 2015 evaluation) and through its work on developing networks, the Cyber Europe Exercises and training activities, awareness raising activities and the provision of the Agency’s expertise. Stakeholders appreciate ENISA’s publications for providing an EU wide overview and perspective on cybersecurity issues which is not available elsewhere.

<sup>77</sup> Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

<sup>78</sup> This question has been added by the evaluator based on comments received from the Commission to the Interim Report. It was not presented in the Roadmap for the evaluation of ENISA.

**ENISA adds value to the cybersecurity activities implemented by national authorities.**

Interviews with Member States but also with ENISA’s users and advisors show that some of the activities are more effective when implemented by ENISA rather than at national level. In general, ENISA’s expertise is valued in all Member States as providing an additional, independent source of information. Often the comparison of threats and chosen responses across the EU provides added value. As the positioning exercise has shown (section 3.2.4.3), ENISA’s added value is not the same in all Member States. In Member States with more cybersecurity capacity and resources, national expertise and capacity tends to be better adapted to the national context than what is provided by ENISA. This is also reflected in the responses to the open public consultation where the option “products and services provide unique information (not offered by other bodies or organisations)” was one of the least selected reasons for using ENISA’s products or services. However, for Member States with fewer resources, ENISA’s capacity building and expertise provides significant added value.

3.2.5.2 Potential to increase added value

**EQ28: How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place?**

ENISA could increase its added value by ensuring better coordination with national cybersecurity authorities to ensure that there is no duplication of efforts. Under the current circumstances the Agency could also ensure increased exchange with other EU bodies such as CERT-EU to avoid any overlap. Beyond this, there is very limited scope for any increase in added value as the Agency is restricted by its financial and human resources.

**To some extent ENISA could increase its added value by ensuring better coordination with national cybersecurity authorities and other EU bodies.** The annual evaluation of ENISA’s activities in 2015 suggested that ENISA could increase its added value by avoiding a duplication of efforts in its activities relative to those of Member States with strong cybersecurity capacities and with other EU institutions. This has also been confirmed by the present study (see section 3.2.4). Better coordination of activities with EU level actors in the field of cybersecurity such as CERT-EU and the DG JRC could create new synergies. Similarly, ENISA should continue to ensure that publications are not restating what is already known at national level but provide an added European perspective on a given topic.

**The potential to increase the added value of ENISA’s contribution to NIS in Europe is limited by the Agency’s restricted financial and human resources.** Stakeholders’ suggestions from interviews across all consulted groups and in general the findings of this study point to a high potential for ENISA to expand and enhance its activities to create more value for its stakeholders. This includes an improved outreach to and cooperation with the private sector, developing and providing more technical expertise, and reaching out to third countries or even globally. However, under the current circumstances, ENISA will not be able to fulfil its potential. The findings of the evaluation show that in the next years ENISA will have to focus its resources on the implementation of the NIS Directive. There is limited capacity and budget available to take on any tasks in addition.

3.2.5.3 Consequences of stopping ENISA’s activities

**EQ35: What would be the most likely consequences at the EU level of stopping ENISA’s activities?**

A discontinuation of ENISA would most likely lead to other organisations taking up part of ENISA’s activities. Member States could bilaterally replace some of the coordination efforts and support to CERTs/CSIRTs. The Commission might take on the planned role for ENISA under the NIS Directive.

The consequences of stopping ENISA would be most felt by Member States with fewer resources being invested in the cybersecurity area that would risk falling further behind more advanced Member States. While there might be no immediate severe consequences in stopping ENISA for Member States with greater capacity, it can be considered a lost opportunity over the medium- to long-term. Most stakeholders expect a growing role for ENISA in the coming years to ensure NIS coordination and strengthen resilience in the EU.

**There is a need for coordination across the Member States to ensure NIS, therefore without ENISA another way of cooperation will have to be put in place. Most likely ENISA's activities would be dispersed across several organisations.** During the interviews ENISA's direct stakeholders suggested that a discontinuation of ENISA would likely lead to more bilateral cooperation between the Member States, but not all the activities of the Agency could be replaced this way. As shown in section 3.2.5.1, ENISA's added value lies in particular in the cooperation across all the Member States and in activities such as the Cyber Europe exercises and the support to the network of CERTs/CSIRTs. In particular for Member States able to invest comparably few resources in the cybersecurity area, ENISA represents significant added value. Interviewees from the EU institutions and bodies suggested an increased role for CERT-EU should ENISA be discontinued, but it was judged that none of the potential organisations that could take on the tasks of ENISA could be considered as a real alternative to having a decentralised agency covering NIS. These services would thus most likely cease to be provided.

According to some of the users and advisors to ENISA, the division of ENISA's activities across different organisations could lead to further fragmentation in the cybersecurity field in Europe as sector specific cybersecurity organisations could be created. Other EU agencies, such as the European Aviation Agency, already have built up some capacities in the area of cybersecurity. Member States investing fewer resources in the cybersecurity area would fall behind in their capacities, ultimately making the entire EU more vulnerable to threats.

Another solution for the implementation of the NIS Directive would need to be identified. A few stakeholders from the EU institutions and bodies suggested that the Commission would have to take on this role, but Member States might be less willing to cooperate directly with the Commission relative to a decentralised agency with a Management Board in which they are represented (and can thus steer the activities to a large extent).

**Stopping ENISA would represent a lost opportunity.** ENISA is needed over the medium- to long-term for its ability to ensure cooperation across the Member States and most stakeholders see a growing role for ENISA in the future. Many direct stakeholders and users and advisors envisage a role for ENISA in the future as a key player in European cybersecurity and there seems to be no immediate alternative option to ENISA, which is recognised by CERTs/CSIRTs as a trusted partner to ensure cooperation. Many of the interviewed direct stakeholders of ENISA concluded that the most likely consequence of stopping ENISA would be the creation of another agency down the line, potentially with more resources and a stronger mandate than ENISA has now, as an EU agency in the area of cybersecurity is needed.

### 3.2.5.4 Conclusion on EU added value

#### **Conclusion – EU-added value**

*The baseline situation (established based on an evaluation of all EU agencies including ENISA in 2009<sup>79</sup> and an impact assessment of changes to ENISA's mandate in 2010<sup>80</sup>) shows the added value of an EU agency covering NIS issues which were found to be more effectively addressed at EU level than by individual Member States. This added value was also identified in the present evaluation study focusing on the 2013-2016 period, as further described below. The evaluation of 2009 found that ENISA was still building up a role which was expected to allow the Agency to deliver "true European value-added" in the future. This was also a conclusion reached as part of the present evaluation based on stakeholder feedback, suggesting that ENISA still has not been able to fully meet its potential.*

ENISA's added value lies primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related NIS communities. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. The added value of ENISA differs between Member States, depending on their cybersecurity capacities and resources. The Agency's activities of providing expertise and capacity building represent important added value for Member States with few national resources dedicated to cybersecurity. This is less the case for Member States with more cybersecurity capacities.

Consequently, a discontinuation of ENISA would impact Member States differently. While Member States with strong cybersecurity capacities will be able to replace the services provided by ENISA at least to some extent, this will not be the case for Member States with fewer resources. The latter Member States rely more on ENISA's services in terms of capacity building, access to expertise and support in the implementation of policy and legislation. Cybersecurity crosses borders, so there is a need to build capacity to avoid weaker links that can impact on cybersecurity in the EU as a whole, as well as a need to provide a cross-EU response. It will not be possible to ensure the same degree of community building and cooperation across the Member States without a decentralised EU agency for cybersecurity; the picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA. Therefore, coordination at EU level is needed.

A potential discontinuation of ENISA would be a lost opportunity for all Member States. Most stakeholders were of the opinion that ENISA could take on a more important role in the EU cybersecurity landscape in the future, ensuring a common response capacity. This potential for the Agency to capitalise on future opportunities would be lost should it be discontinued.

<sup>79</sup> Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

<sup>80</sup> European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

### 3.3 Assessment of ENISA’s strength, weaknesses, opportunities and threats

Based on an analysis of the context – namely the evolution, since the last revision of ENISA's mandate in 2013, of the cybersecurity and digital privacy landscape - the evaluation study provides an assessment of the main strengths and weaknesses of ENISA within its current mandate, organisational set-up and resources, in the new cybersecurity and digital privacy landscape. The evaluation study also examines whether a fixed-term mandate is coherent with the new challenges and tasks ENISA will have to take on. In the analysis of the context, the aim of the study is to assess if and how the increase in the frequency, sophistication and potential impact of cyber-threat trigger new needs of ENISA's constituency, and how the changed policy and regulatory landscape, having regard to the recently adopted NIS Directive and the priorities set by the Digital Single Market Strategy impact on ENISA's activities. This allows the identification of opportunities and threats emerging from such a landscape.

This section relates primarily to the prospective aspects of the evaluation study. The table below presents the six evaluation questions which are covered in this section.

**Table 24: Evaluation questions covered under the assessment of ENISA’s SWOTs**

#### Prospective

EQ36: Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent is ENISA best placed to respond to these needs? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?

EQ37: How does the new policy and regulatory landscape, having regard for the recently adopted Network and Information Security Directive and COM(2016) 410, and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?

EQ38: What are the main strengths and weaknesses of ENISA in taking up new challenges, considering its current mandate and organisational set-up and capacity?

EQ39: If ENISA should take on any new challenges and tasks, would a fixed-term mandate be suitable?

EQ40: Which are the concrete needs and opportunities for further increased practical cooperation with Member States and EU bodies?

EQ41: Which are the concrete needs and opportunities for cooperation and synergies with international bodies working in adjacent fields, like the NATO Cooperative Cyber Defence Centre of Excellence?

EQ42: Could ENISA's mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape or would another EU initiative be more efficient?

This section draws on the summative elements of the assessment of ENISA's performance, governance and organisational structure and of the positioning exercise, as presented in section 3.2 and a review of the evolution, since the last revision of ENISA's mandate in 2013, of the cybersecurity and digital privacy landscape. Based on this, the key strengths, weaknesses, opportunities and threats of ENISA in the current, changed policy and regulatory context are established. In so doing, the section contributes to the more formative, forward-looking dimension of this evaluation and will assist in ascertaining what type of mandate for ENISA would best fit the current, evolving context. A desk-based review of key documents was the main source of information for this part of the study, in addition to in-depth interviews to help identify key opportunities and threats. Moreover, three subcontracted policy, legal and technical cybersecurity experts provided their support on the subject and helped to assess how this has/will impact on ENISA as an organisation and the activities it carries out. Further input was obtained through the open public consultation and the validation workshop.

Subsection 3.3.8 below summarise the preliminary findings and conclusions of this section in the form of an analysis of the different strengths, weaknesses, opportunities and threats faced by

ENISA. The following subsections responds to the prospective evaluation questions of the study. A more comprehensive table, summarising ENISA’s SWOTs can be found in Appendix 5.

### 3.3.1 New needs for ENISA’s constituency

**EQ36: Does the new scenario with increased frequency, sophistication and potential impact of cyber-threats trigger new needs from ENISA’s constituency? To what extent is ENISA best placed to respond to these needs? To what extent could ENISA’s current mandate, tasks and/or capabilities address these needs?**

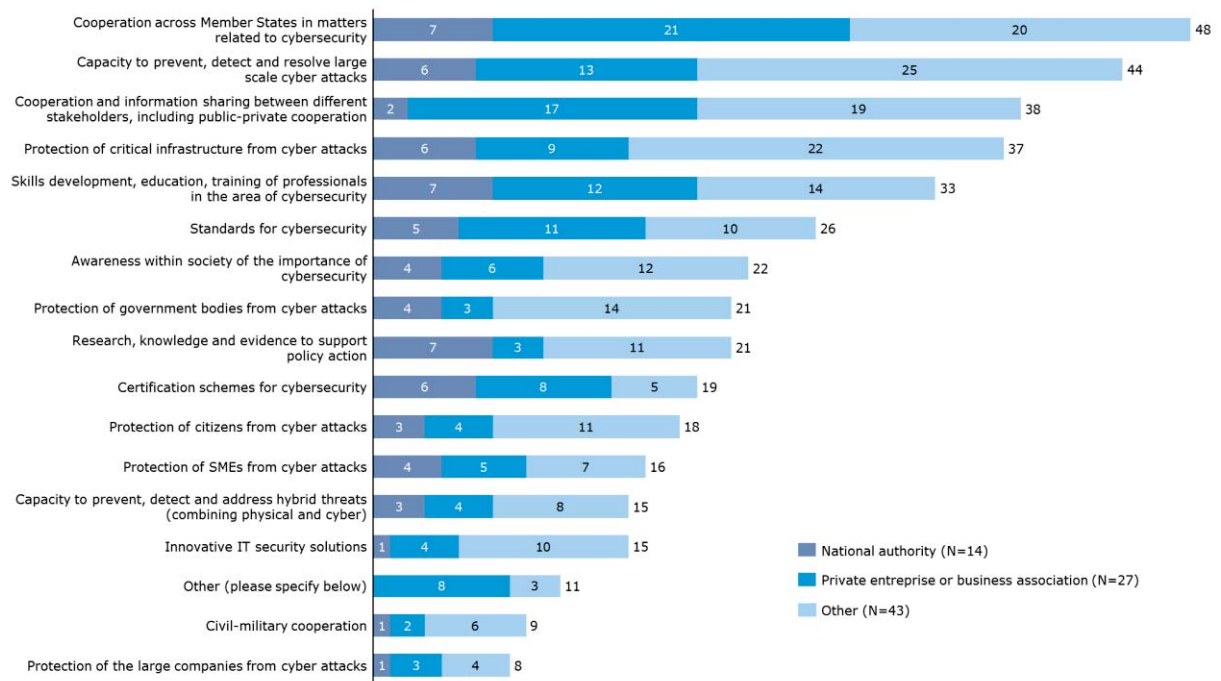
Although there are differing opinions on which stakeholders make up ENISA’s constituency and there are strong divergences in the needs of different stakeholder groups, there is agreement that there are new needs as a result of increased cyber threats. The field most regularly mentioned concerns the rise of the IoT and new demands to increase the safety of connected devices. To respond to these, stakeholders see a need for increased cooperation between different authorities and communities (public and private), increased capacities at Member States level and further research into cybersecurity challenges. ENISA was considered to be able to provide activities that respond to such needs. Many stakeholders agree that a more operational role for ENISA with regard to collecting and sharing information on cyber incidents would be desirable. Although some of the stakeholders from all consulted groups see the NIS Directive as a step towards a more operational role, a majority of consulted stakeholders believe an extended mandate to be necessary to fully address the need for more effective information sharing. In addition, ENISA’s current financial and human resources are perceived to be insufficient to address these needs.

**ENISA has a constituency with diverse needs.** Interviewees’ opinions differ on which stakeholder groups make up ENISA’s constituency. Some of ENISA’s stakeholders across all groups even criticise ENISA for the lack of a clearly defined constituency. According to certain interviewees (including Member States), this is sometimes reflected in ENISA’s deliverables in terms of inappropriate writing style and dissemination channels to reach the intended target audience. ENISA’s direct stakeholders noted that ENISA’s role concerning Member States’ needs requires clarification because of the strong differences between more experienced and resourced Member States and Member States which are more limited in their capacity and resources. Also the extent to which ENISA should prioritise the support to EU institutions requires clarification. Arguably, Member States are ENISA’s primary stakeholders. As shown in the section on relevance (3.2.1), the demands and priorities vary from one Member State to another. There is a tendency for Member States with more resources and capacity in cybersecurity to be less dependent on ENISA and to see the Agency’s role in responding to cybersecurity needs as more limited than other Member States. Meanwhile, a number of stakeholders from industry see a need for more action of direct benefit to industry.

**There is a wide spread perception that the increased frequency, sophistication and potential impact of cyber-threats triggers new, and reinforces current, needs from ENISA’s constituency.** The majority of the interviewed stakeholders from all groups view that there are increased risks, in particular in relation to the rise of the IoT and new demands to increase the safety of connected devices. In this regard, rapidly evolving cyber threats create a need for more rapid responses. In line with this, “cooperation across Member States in matters related to cybersecurity” and “the capacity to prevent, detect and resolve large scale cyber-attacks” were identified by the largest number of respondents to the open public consultation as a main gap or need in the cybersecurity field in the EU over the next ten years. A majority of the respondents in each of the three categories of respondents (i.e. national authorities, private enterprise or business association, and other) were of the opinion that these were needs or gaps, as Figure 53 illustrates. Respondents that commented in their open responses on the need for increased cooperation across Member States suggested that cooperation was necessary not only to bridge the security gaps that arise from a lack of cross-country cooperation, but also to build trust

and confidence within the EU in matters of cybersecurity. Some respondents (including Member States) pointed to additional benefits of such cooperation, including increased market integration through the provision of internet services, support to the increase in cybersecurity capacity of less advanced Member States, and innovation for responses to current and future threats. Additionally, three respondents referred to an additional need, namely the need for “effective international cooperation” (i.e. EU and third countries such as the US, Japan, Korea and India). Comments on the need to increase capacity to prevent, detect and resolve attacks pointed to the fact that the EU should step up the detection and real-time response to cyberattacks in information, communication technology (ICT), critical infrastructures, SMEs, government and public agencies. Others felt that while detecting and responding to cyberattacks is important, the priority should be placed on developing a prevention-focused approach that allows protection from loss of intellectual property and personal data as well as loss of trust. The views of the different open public consultation respondent groups in relation to each of the options were relatively balanced, with the notable exception - among the most referred to gaps or needs - of “cooperation and information sharing between different stakeholders, including public-private cooperation” where only two national authority respondents (out of a total of 38 respondents) identified it as a need or gap.

**Figure 53: Most urgent needs or gaps in the cybersecurity field in the EU in the next ten years (multiple choice question)**

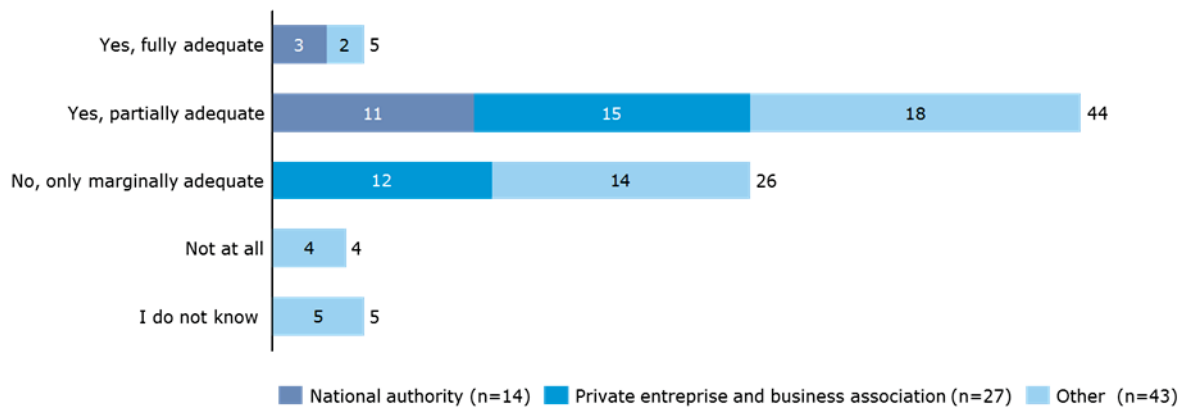


Source: Open public consultation

**Instruments and mechanisms at EU level were not judged fully adequate to promote and ensure cybersecurity within such a context.** Taking into consideration the above mentioned needs, only 6% of the open public consultation respondents judged the current instruments and mechanisms at European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be fully adequate to promote and ensure cybersecurity. A great majority of the respondents (including Member States) regarded them as partially adequate or only marginally adequate (52% and 31% respectively) and 5% found them not at all adequate. As shown in Figure 54 below, national authority respondents appear to be more positive about the adequacy of these instruments and mechanisms in comparison with representatives from private enterprises or business associations and other respondents.



**Figure 54: Adequacy of current instruments & mechanisms at European level to promote and ensure cybersecurity**



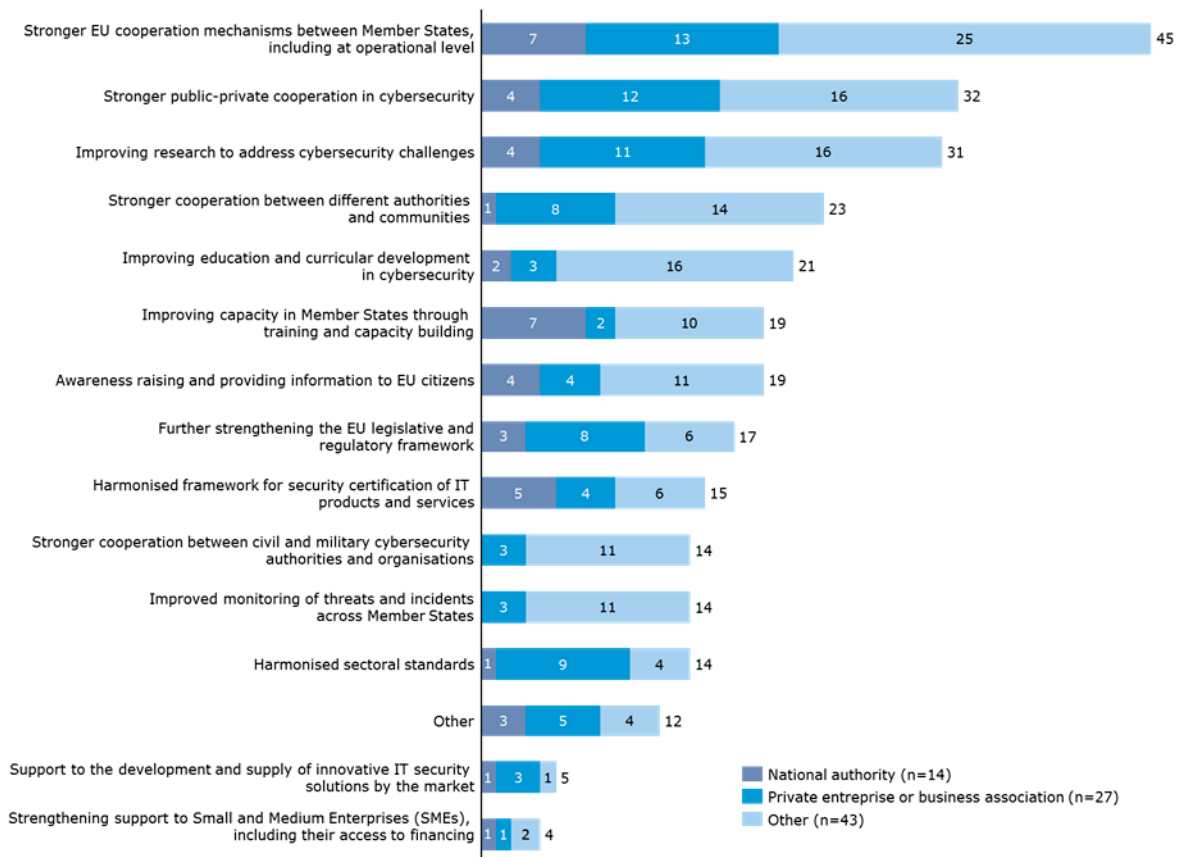
Source: Open public consultation

The open public consultation respondents were asked to elaborate on their answers and 51 contributions were received, providing further assessments and recommendations for improvement. Some examples of the inputs from respondents who assessed the current instruments and mechanisms as “partially adequate” are summarised here. In their comments respondents positively assessed the progress the EU has made in the set-up of its *regulatory and institutional framework* for cybersecurity. However, respondents also felt that the majority of the instruments have yet to be implemented, enter into force or still need to be developed. Three respondents stated that the framework is too often open to interpretation, which “leaves the possibility of non-harmonised implementations” that are contrary to its aim. Considering the fast-paced development of technology and cybersecurity needs today, respondents recommended that current policy instruments continue to evolve, change and adapt: “it is therefore important that the European agencies and bodies assess and evaluate the cybersecurity landscape to ensure the needs of the governments, industry and citizens are being met”. It was also suggested that cooperation mechanisms created by the *NIS Directive* should be evaluated after two years. Other respondents commented that the development of *standardisation and certification* regarding information security at EU level should be improved and accelerated. As a final example, on *IT solutions* respondents felt Internet-of-Things-risks ought to be addressed more strongly and EU-made cybersecurity solutions developed by the private industry (SMEs) should be supported.

**Enhanced cooperation between Member States and with the private sector is considered to be the primary solution to the new and enhanced needs of ENISA’s stakeholders.**

Based on the identified needs or gaps, open public consultation respondents were asked to consider what the priorities for EU action should be from now on and select up to three responses out of a list of 15. As revealed in Figure 55 below “stronger EU cooperation mechanisms between Member States, including at operational level” was clearly considered to be the most important action, followed by “stronger public-private cooperation in cybersecurity” and “improving research to address cybersecurity challenges”. When analysing the number of responses from the three different groups of respondents, considering also the size of each group, it can be noted that the action “improving education and curricular development in cybersecurity” received relatively higher support from “other” respondents. In contrast, the action “improving capacity in Member States through training and capacity building” was comparatively more supported by national authorities. It should also be mentioned that three of the actions were not selected as a priority by any national authority representative, namely: “stronger cooperation between different authorities and communities (e.g. between CERTs/CSIRTs and law enforcement authorities; Information Sharing and Analysis Centres and CERTs/CSIRTs)”, “stronger cooperation between civil and military cybersecurity authorities and organisations”, and “improved monitoring of threats and incidents across Member States”.

**Figure 55: Top priorities for EU action from now on in the area of cybersecurity**

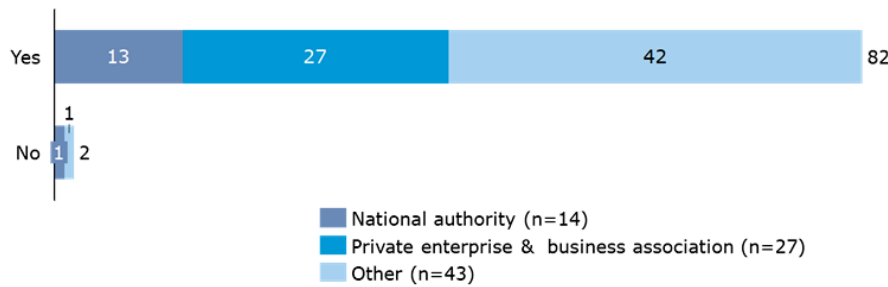


Source: Open public consultation

Among the twelve open responses who selected the option “other” (see Figure 55 above), fourteen additional “top priorities for EU action” were identified. Among these, six of the priorities mentioned were also related to *cooperation*. Besides pushing for “stronger public-private cooperation” respondents pointed to “establishing stronger international / trans-Atlantic cooperation and collaboration” including regulatory convergence, as well as “developing policy and operational support for cooperation and information sharing between different stakeholders and Member States”. Five priorities mentioned concerned *support and guidance*, e.g. “Support uptake of new privacy techniques”, “Improved monitoring of threats”, “Provision of implementation, application and enforcement tools” and an “EU-reviewed open source, for public administration i.e. communes”. Finally, three matters related to *cybersecurity regulation* and the respondents asked for “more flexibility in regulation to allow adapting to nature of organisations, services and markets” and believed that ENISA’s role in relation to this should be that of “sign-posting relevant and robust standards that function at global level” given its “important role in harmonisation across the EU”.

**ENISA is expected and considered capable of taking on a role in responding to stakeholder needs in the future.** Following on from the assessment of needs, gaps and top priorities for action, the open public consultation respondents were asked about ENISA’s future role. As illustrated in Figure 56 below, 98% of respondents (82) thought that there is a role for an EU-level body in improving cybersecurity across the EU.

**Figure 56: Is there a role for an EU-level body in improving cybersecurity across the EU?**



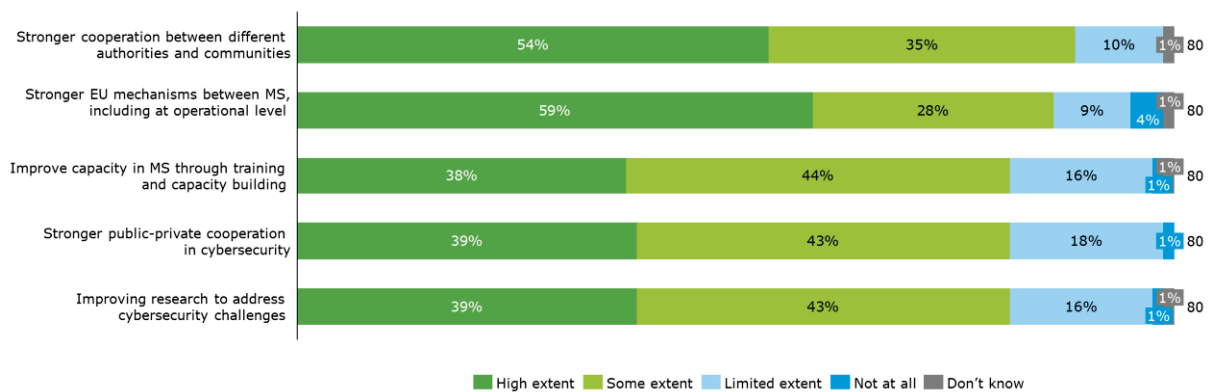
Source: Open public consultation

Furthermore, almost all of the respondents (81 of 82) who saw a role for an EU-level body in improving cybersecurity considered that ENISA could fulfil a role in bridging the different gaps in the future. The Agency, if sufficiently mandated and resourced, was perceived as *most able* to contribute to the following five areas (percentages and numbers reflect respondents that considered ENISA to be able to a *high extent or to some extent* to fulfil a specific role; see Figure 57 below for further details):

- Stronger cooperation between different authorities and communities, 89% (71);
- Stronger EU mechanisms between MS, including at operational level, 87% (69);
- Improve capacity in Member States through training and capacity building, 82% (65);
- Stronger public-private cooperation in cybersecurity, 82% (65); and
- Improving research to address cybersecurity challenges, 82% (65).

In summary, open public consultation respondents consider ENISA to be the right body to respond to the needs they identified as most pressing. In-depth analysis of the answers indicates clear differences in opinion per type of respondent group in some areas. In this sense “stronger cooperation between different authorities and communities” was less supported as a role for ENISA by national authorities (69% selected to a high extent or to some extent) compared to private enterprise & business association (92%) and other respondents (93%). In similar manner “stronger public-private cooperation in cybersecurity” received higher support from private enterprise & business association (96% selected to a high extent or to some extent) compared to national authorities (69%) and other respondents (76%).

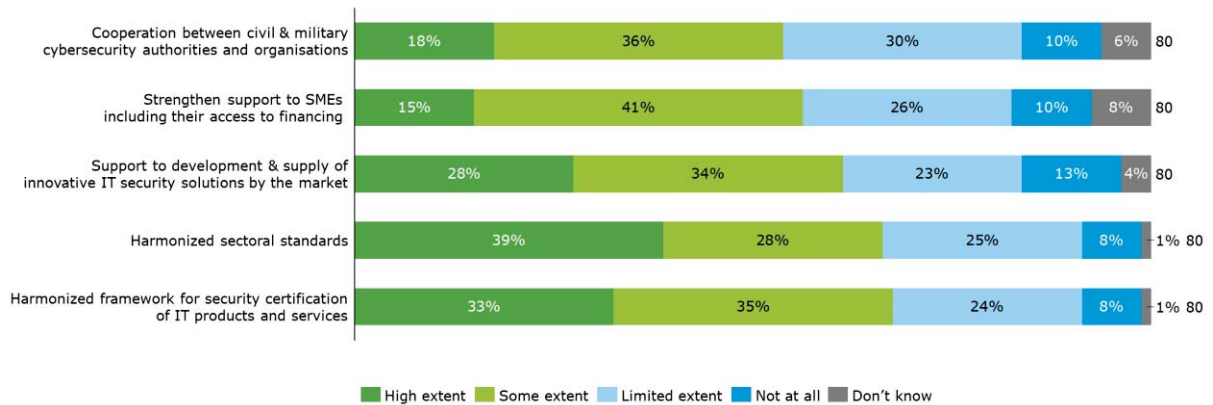
**Figure 57: Gaps and needs for which ENISA is perceived to be most able to fulfil a role**



Source: Open public consultation

The gaps and needs for which ENISA is perceived to be least able to fulfil a role correspond with the needs selected by fewer open public consultation respondents as being urgent, as presented in Figure 58.

**Figure 58: Gaps and needs for which ENISA is perceived to be least able to fulfil a role**



Source: Open public consultation

**A variety of suggestions of tasks and activities that ENISA could add to its portfolio to further increase network and information security in the future were made by stakeholders.** Interviewees and respondents to the open public consultation made the following suggestions for ENISA to expand its tasks and contribute even more to NIS in Europe:

- Increase the Agency’s visibility and involve a broader group of stakeholders in the activities, including capacity building and awareness raising in the private sector and civil society
- Develop more internal expertise rather than providing support based on data collected from other experts; taking on research on cybersecurity in cooperation with research centres
- Cover the areas of standardisation and certification
- Build more trust between the Member States to increase willingness to exchange information on threats and incidents. This could be based on further capacity building in less experienced Member States.
- Work closer together (possibly even merge) with other EU institutions such as Europol’s EC3 and CERT-EU
- Enhanced cooperation with third countries, in particular with CERT-equivalents to obtain timely information on cybersecurity threats and incidents to diffuse across the Member States.

Interviewed Member State authorities suggested that ENISA’s current tasks which will increase in relevance over the coming years include the Cyber Europe Exercises, training of Member States and fostering cooperation between the cybersecurity communities.

**Industry stakeholders would like ENISA to respond more to their needs in the future.**

The interviewed industry representatives saw an important role for ENISA in acting as a link between the public and private sector. This was confirmed in the open public consultation. The Agency could support industry in the future by ensuring harmonisation of baseline requirements for cybersecurity across the EU. Also a more operational role for ENISA to collect data on threats across the EU and make this data available to the industry would be welcomed by these stakeholders. Some areas that ENISA should be focussing on more as priority areas than is currently the case, according to industry stakeholders in particular, included the Internet of Things, certification and standardisation, the move to big data and machine intelligence, and becoming more active in the educational field, e.g. by supporting the creation of Massive Open Online Courses (MOOC) in the field of cybersecurity.

**Many of ENISA’s stakeholders - beyond its group of direct stakeholders - see a need to extend ENISA’s mandate to embrace more operational roles.**

In particular, industry stakeholders regularly advocate ENISA taking on a more operational role to collect data on threats and cybersecurity incidents across the EU and share this information with industry. A few comments from the open public consultation respondents relating to this matter largely confirm

that the group of private enterprises & business associations is more positive about ENISA taking on a more operational role, while national authorities are less supportive of such a development. Findings from the workshop revealed equally that the majority of stakeholders see a need for a clearer definition of the term “operational”, as it is currently used by many as a synonym for information sharing while others understand it to mean actual response to incidents. During the workshop some of ENISA’s direct stakeholders suggested that there could be some interest in enhanced cooperation on threat intelligence/situational awareness led by ENISA. While some interviewees indicate that the NIS Directive already goes in this direction, the majority thought that a review of the current mandate would be necessary for ENISA to be more actively involved in information sharing on cybersecurity incidents.

**A concern voiced among all consulted stakeholder groups was whether ENISA would be able to take on the new needs of its constituency given its currently limited resources.** In light of the multiple obligations of ENISA today and the identified difficulties to fully respond to stakeholder needs over the period 2013-2016, there is a certain degree of doubt on the extent to which ENISA will be able to respond to the new needs of stakeholders with its current financial and human resources. This is in particular the case considering the additional tasks under the NIS Directive (presented in the following section) which will require an important share of ENISA’s staff in the coming years. A majority of the interviewees think that the scope of the Agency’s work will further grow in the future.

### 3.3.2 The impact of new policy and regulatory landscape on ENISA’s activities

**EQ37: How does the new policy and regulatory landscape, having regard for the recently adopted Network and Information Security Directive and COM(2016) 410, and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?**

There is agreement among all of ENISA’s consulted stakeholders that ENISA as the main European entity mandated will be affected by the NIS Directive in multiple ways. While the NIS Directive is seen as an opportunity for ENISA to increase its influence in the current fragmented EU cybersecurity policy landscape, many of ENISA’s direct stakeholders, users and advisors see challenges for ENISA in terms of financial and human resource constraints and the risk of overlap with other agencies, above all CERT-EU.

**The NIS Directive will have a notable impact on ENISA’s activities.** There is consensus among all stakeholder groups that the NIS Directive will have a significant impact on ENISA’s activities since ENISA is mandated to be the main European entity supporting the transposition of the Directive in the Member States. Several direct stakeholders refer to a large initial impact on ENISA’s organisation and activities, but interviewees’ opinions differ as to whether this is a temporary effect or whether it will be more long-lasting. A few experts even refer to the NIS Directive as being a “main disruption” and “game changer” in EU cybersecurity policy foreseeing long-lasting changes.

**The view of the majority of stakeholders is that the NIS Directive is an opportunity for ENISA to increase its influence.** The general perception is that the NIS Directive strengthens ENISA’s influence within EU cybersecurity policy by giving the Agency a more operational role in supporting its implementation by the Member States. However, some observers voiced concern about whether the Agency is taking full advantage of the opportunity it is being provided with or whether it is acting too prudently. On the other hand, certain direct stakeholders of the Agency pointed out that ENISA is not equipped with a right to initiate action, but limited to proposing things to the Commission.

**The implementation of the NIS Directive currently takes up a large part of ENISA’s resources which poses a challenge for the Agency.** As presented in section 3.2.1.5, the NIS

Directive is perceived as not only impacting on ENISA’s type of activities but also on increasing the overall volume of its responsibilities and work load. According to some of ENISA’s direct stakeholders, the Work Programme is currently dominated by the NIS Directive with around 20 staff members having been designated to be work on the NIS Directive. Several interviewees (including Member States) think that without a corresponding increase in financial and human resources, or a reduction of ENISA’s activities in other topics, the additional tasks imposed by the NIS Directive are very challenging (by a few even considered impossible) for the Agency to perform. As a result, a number of direct stakeholders of ENISA point out that a potential threat for ENISA lies in capacity constraints to fulfil other tasks to the high standard. However, a few of those stakeholders (including Member States) are more optimistic seeing these challenges to be only temporary until the NIS Directive’s transposition in Member States.

**Despite the opportunities provided, there are risks of overlap with CERT-EU.** The positioning exercise (section 3.2.4.3) detected a risk for overlap between ENISA and CERT-EU; this might increase in the future. Interviewed stakeholders described ENISA’s role in supporting the national CERTs/CSIRTs as foreseen under the NIS Directive as more operational and several stakeholders across all consulted groups perceived this new role to create (or increase the risk for) overlaps and conflicts of interest with CERT-EU. Examples referred to include the fact that CERT-EU already implements activities that could fall within the scope of ENISA’s mandate by working with stakeholders that are among ENISA’s constituency (and go beyond CERT-EU’s main constituency of the EU institutions) or by getting in touch with commercial organisations through the use of CERTs/CSIRTs. One of ENISA’s direct stakeholders argues that the best option would have been to create CERT-EU as a part of ENISA from the start, but indicates that resistance from some of the Member States prevented this from occurring.

**ENISA’s new role as the main body mandated to assist national CERTs/CSIRTs puts higher requirements on ENISA to be better connected geographically.** Some interviewed stakeholders (including Member States) stakeholders consider that the new obligations under the NIS Directive, e.g. working with the national CERTs/CSIRTs, require increased co-operation with other EU-bodies, in particular with CERT-EU. Following this argumentation, there is a need for ENISA to be more agile and connected to the cybersecurity policy environment.

### 3.3.3 Main strengths and weaknesses of ENISA

**EQ38: What are the main strengths and weaknesses of ENISA in taking up new challenges, considering its current mandate and organisational set-up and capacity?**

The assessment of the main strengths and weaknesses of ENISA in taking up new challenges indicates that, in the current set-up, ENISA’s weaknesses outweigh its strengths. With regard to the Agency’s strengths, the perception of ENISA as a neutral facilitator, mediating the divergent policy priorities of Member States, has helped it gain trust at European level. Its role in fostering collaboration, community building, as well as supporting Member States in their cybersecurity capacities, also deserve a mention. However, ENISA is faced with many obstacles. Given its lack of expertise, weak communication and marketing, and limited self-assertion within the EU cybersecurity landscape, ENISA lacks overall visibility. ENISA also lacks a long-term vision, often being constrained by its fixed mandate and annual work programme. Finally, ENISA lacks resources, both financial and human, in terms of the Agency’s limited size and the staff’s composition which is being aggravated by the NIS Directive. In addition, ENISA’s split location in Athens and Heraklion causes difficulties for the Agency for attracting and retaining qualified staff members.

### **ENISA’s strengths in taking up new challenges**

**ENISA is perceived as a “trusted” actor<sup>81</sup> within the EU’s cybersecurity policy landscape, free from commercial interests or political bias.** As presented in section 3.2.2.2, one of the main strengths of the Agency is its reputation as an independent and neutral facilitator<sup>82</sup> that is capable of navigating a highly fragmented policy domain, while also being faced with the different priorities of Member States.<sup>83</sup>

**Furthermore, collaboration and community building belong to the Agency’s core strengths.** As presented in section 3.2.1.4, ENISA has proven its capability to maintain a viable network with a range of different stakeholders including national governments, industry, the EU institutions and other EU and international bodies. ENISA acts as a node to gather and exchange information and best practices among Member State, EU and international players. ENISA is also involved in fostering cooperation with the private sector and encourages the setup of PPPs as a way to increase the operational capabilities in the sector.<sup>84</sup>

**ENISA maintains good and recognised working relationships with its direct stakeholders.** The survey of ENISA staff and direct stakeholders further shows that the Agency’s relationship with its stakeholders and its efforts for cooperation were particularly well considered. A vast majority of 93% of respondents (including Member States) thought that ENISA had built strong and trustful relationships with its stakeholders when executing its mandate. Furthermore, 93% of the survey respondents agreed to some or to a high extent that ENISA was open to cooperating with a variety of stakeholders. Meanwhile ENISA’s systems and procedures in place for stakeholder consultation and management were considered to be well-working by 84% of respondents.

**ENISA is very active in capacity building assistance.** This includes organising trainings, cybersecurity exercises, development of manuals, studies trying to reach a broad sector including Member States, private actors, EU institutions and agencies. The aim of this capacity building activity is to develop the capabilities of the agents, providing them with the necessary tools to prevent, detect and handle incidents.<sup>85</sup>

**The organisational solutions and procedures of ENISA were ranked positively by ENISA’s stakeholders.** As presented in section 3.2.2.8, 80% of survey respondents<sup>86</sup> regard the current solutions and procedures as adequate. Moreover, the current governance structure, with a Management Board, an Executive Board and the PSG, was assessed as conducive both to the effective functioning of the Agency (i.e. in terms of meeting its objectives) and to the efficient functioning of the Agency (i.e. in terms of value for money), by 85% of the respondents in both cases. Finally, 73% and 74% of respondents respectively saw ENISA’s management practices as conducive to creating an effective organisation and an efficient organisation to some or to a high extent.<sup>87</sup>

<sup>81</sup> See section 3.2.2.8 for further information.

<sup>82</sup> Finding obtained from interviews with ENISA’s direct stakeholders.

<sup>83</sup> See section 3.2.1.5 for further information on diverging priorities of Member States.

<sup>84</sup> See, for example: Carrapico, H., Barrinha, A. (forthcoming). The EU as a coherent (cyber)security actor; Bendiek, A. (2012) ‘European Cyber Security Policy’, SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017; ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0; ENISA (2016) Evaluation Roadmap 25/07/2016.

<sup>85</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0; ENISA (2016) Evaluation Roadmap 25/07/2016; ENISA (2015). Threat Landscape and Good Practice Guide for Software Defines Networks/ 5G: ISBN: 978-92-9204-161-8, DOI: 10.2824/67261.

<sup>86</sup> Source: The survey on ENISA’s governance, organisational set-up and working practices

<sup>87</sup> See section 3.2.2.8 for further information.

**As the European cybersecurity agency ENISA has significant horizontal expertise to assess how every EU Member State is performing in cybersecurity.** ENISA is equipped with a broad mandate, allowing it to take on a wide variety of different tasks ranging from capacity support of Member States to the development of cybersecurity reports/expertise. Thanks to Article 14, ENISA is able to react to ad-hoc requests from the EU institutions and Member States in the field of policy development and policy implementation. This mechanism is used by some of the Member States (see section 3.2.2.6).

### **ENISA's weaknesses in taking up new challenges**

**A recurring finding from interviews with ENISA's users and advisors is the Agency's limited visibility.** Several root causes are identified to play a part in this: ENISA is seen to lack, in particular technical, expertise and it has relatively weak communication and marketing, giving it marginal presence in the press and media. Indeed, other European agencies, e.g. Europol, FRA or the European Food Safety Authority, have managed to be more present in the media and the public. Potentially as a result of its limited visibility, ENISA has not managed to carve out its own space in the EU's cybersecurity landscape. A few interviewed industry stakeholders expressed their support for the Agency more strongly engaging in commenting on headline events, such as major cyber-attacks on governments or companies in Europe, in order to increase the visibility of ENISA. It should be noted though, particularly in the case of governmental attacks, that ENISA would probably need the prior approval of the impacted Member State to be able to do so.

**ENISA lacks a more strategic, long-term vision.** Unlike other EU agencies, ENISA has a fixed mandate which in the eyes of a few users and advisors is counterproductive to developing a more strategic, long-term vision. Furthermore, Member States' dominance in the Management Board often leads to an annual work programme characterised by the individual priorities of Member States rather than a more strategic approach to cybersecurity. Finally, a few of ENISA's users and advisors perceive ENISA as being too tied to fulfilling its work programme, contributing to the lack of a strategic approach.

**An important weakness concerning ENISA's organisational set-up and capacity relates to its limited size and financial resources.** The surveyed group of all stakeholders<sup>88</sup> provided the least positive assessment of the size of the Agency among all elements in the Agency's organisational set-up, with 51% of them perceiving it as being only appropriate to a limited extent or not at all appropriate to the work entrusted to ENISA and to its workload. ENISA's surveyed direct stakeholders were by far the most pessimistic about its size. The open public consultation results overall confirmed this finding as 58% of respondents considered the size of the Agency to be partially or completely inadequate, with no major differences among different respondent groups having been identified. Negative assessments concerning the size of ENISA by interviewed experts – direct stakeholders as well as users and advisors – were often accompanied by comments on a need for more financial resources. The majority of interviewees (including Member States) saw a need to increase ENISA's staff and resources with a few referring to a drastic increase, e.g. doubling the currently available resources. A number of interviewees also pointed out that the NIS Directive placed an additional burden on the Agency without reducing its other tasks or increasing its resources.

**Another tangible weakness with regard to ENISA's organisational set-up relates to ENISA's split office location in Heraklion and Athens.** While the survey findings only point to ENISA's location being a moderate weakness, the majority of interviewees (including Member States) regard the Agency's location as a major weakness. Accordingly, ENISA's location was reviewed by 67% of surveyed respondents<sup>89</sup> as enabling, to some or to a high extent, ENISA to effectively conduct its work (i.e. in terms of meeting its objectives) and by 59% to conduct its

<sup>88</sup> Source: The survey of ENISA staff and direct stakeholders

<sup>89</sup> Source: The survey on ENISA's governance, organisational set-up and working practices



work efficiently (i.e. in terms of value for money). The location was reviewed as not enabling such effectiveness and efficiency, or only to a limited extent, by 28% and 35% of surveyed respondents respectively. From the surveyed respondents, ENISA's direct stakeholders were most critical of ENISA's office location.<sup>90</sup> Meanwhile, all groups of consulted stakeholders were very critical of the office location's impact on the Agency.

One of the arguments supported by a certain number of respondents is that ENISA's effectiveness is impacted by being too far from Brussels, hence complicating ad hoc exchanges with the EU institutions. Various respondents were also critical of the fact that the Agency is divided in two, which decreases its efficiency by creating additional costs and requiring additional efforts to ensure internal communication. Meanwhile, all of ENISA's consulted stakeholder groups admit that the establishment of an office in Athens improved the situation, in particular for the travel of ENISA's stakeholders. Respondents also indicated that ENISA's location is not fit for recruiting and retaining qualified staff due to the lack of facilities for international employees and their families, as well as the low pay and economic uncertainties faced by Greece.

**The staff composition of ENISA presents a more moderate weakness.** Approximately 65% of surveyed respondents<sup>91</sup> viewed the Agency's staff composition as adequate for its work to some or to a high extent, while 30% viewed it as only adequate to a small extent or not at all. ENISA staff was particularly critical with more than one third of the respondents seeing the staff composition to be adequate only to a limited extent or not at all. Some recurring, highlighted weaknesses concern the need to develop more internal expertise by hiring *more senior staff*, and the need for *more technical staff* to improve the balance between administrative staff and operational staff. Some of ENISA's direct stakeholders also reported that the Agency's recruitment difficulties had led to an over-representation of Greek nationals in ENISA with often low incentives for job rotation.

**Along with the staff composition, the recruitment and training procedures can be considered a moderate weakness.** Among the surveyed respondents, 33%<sup>92</sup> found the recruitment and training procedures of ENISA not to be appropriate or to be only appropriate to a limited extent to manage ENISA's workload. Additional comments revealed that the recruitment *process is considered too slow* and therefore not well adapted to the cybersecurity domain which is fast paced. The *lack of training* that the staff experienced over the five years prior to writing was linked to the *absence of a dedicated HR department within the Agency*.

#### 3.3.4 Format of ENISA's mandate

##### **EQ39: If ENISA should take on any new challenges and tasks, would a fixed-term mandate be suitable?**

Clear advantages for ENISA having a permanent mandate were identified. This would allow it to develop a more long-term strategy and increase its effectiveness. It could also alleviate current recruitment difficulties. A permanent mandate should not exclude the need for regular evaluations and revisions of ENISA's mandate.

**The findings from the interviews show that views diverge on whether a fixed-term mandate would be suitable to help ENISA take on new challenges and tasks.** ENISA's Regulation foresees an end date by which the Agency's mandate expires. Among the EU agencies, ENISA is the only one with such a mandate since the European Agency for Reconstruction was

<sup>90</sup> See section 3.2.3.1 for further information.

<sup>91</sup> Source: The survey on ENISA's governance, organisational set-up and working practices

<sup>92</sup> Ibid.

disbanded in 2008.<sup>93</sup> Many direct stakeholders see clear benefits in ENISA having a permanent mandate. The reasons for supporting a permanent mandate are linked to allowing ENISA to plan over the longer term and support the development of a greater vision. Aside from generating greater independence, these stakeholders also claimed that a permanent mandate would lead to more effectiveness. However, others were more in favour of a fixed-term mandate, thinking that this would provide for greater levels of flexibility to adapt the Agency's mandate to the rapidly evolving cybersecurity landscape. Another recurring view in support of a fixed-term mandate was that ENISA's performance could be more easily evaluated or re-evaluated in the case of changing needs. Yet, supporters of a fixed-term mandate also admitted that it can cause negative side effects, such as the Agency's recruitment problems and political uncertainty. In the discussion at the workshop, a clear preference was shown for a permanent duration of the Agency with a mandate that is evaluated and reviewed every few years, as is the case for other EU agencies.

### 3.3.5 Concrete needs and opportunities for practical cooperation with Member States and EU bodies

#### **EQ40: Which are the concrete needs and opportunities for further increased practical cooperation with Member States and EU bodies?**

With regard to practical cooperation with Member States, stakeholders agree that this needs to be further increased, in particular with the CERTs/CSIRTs. Aside from providing direct support and helping CERTs/CSIRTs to respond to the requirements under the NIS Directive and to further build their capacity, additional training and increased interaction between ENISA and the CERT/CSIRT community were found to be important.

With regard to cooperation between ENISA and other EU bodies, only few consulted stakeholders suggested that there was a need to increase the interaction. However, the fragmentation of cybersecurity across different DGs of the European Commission and agencies, shows that there is in fact a need to enhance cooperation and coordination.

**Cooperation with Member States was seen as one of the top priorities to respond to stakeholder needs, while less emphasis was put on cooperation with EU bodies.** The findings of the open public consultation showed that stakeholders expect ENISA to further foster increased Member State cooperation to respond to new and reinforced cybersecurity challenges, as presented in section 3.3.1. Fewer open public consultation respondents and interviewed direct stakeholders of ENISA considered cooperation between ENISA and EU bodies as a priority. Nevertheless, interviews with representatives from the Commission, other EU agencies and ENISA's staff, as well as the assessment of ENISA's coherence (see section 3.2.4), show that there is a need to enhance cooperation and coordination across EU bodies to create synergies and develop an EU approach to cybersecurity.

**ENISA's new role under the NIS Directive will allow the Agency to better address the needs of CERTs/CSIRTs.** An overwhelming majority (85%) of the respondents to the CERT/CSIRT survey were of the opinion that the new role foreseen for ENISA in relation to CERTs/CSIRTs as part of the NIS Directive will enable ENISA to better cover CERTs/CSIRTs' needs. With respect to the activities to be carried out by ENISA, facilitating cooperation was seen as key by a large number of respondents. Fields where further assistance of ENISA would be useful included better understanding the needs of CERTs/CSIRTs and providing direct support and helping CERTs/CSIRTs implement the NIS Directive and build capacity. In terms of what ENISA could do to better cover CERTs/CSIRTs' needs, more trainings and increased interaction of ENISA with CERTs/CSIRTs were seen as particularly important by respondents. The call for more training opportunities is largely confirmed by the different stakeholders. A few interviewed users and

<sup>93</sup> European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No4 – Ending of agencies. Available at: [http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche\\_4\\_sent\\_to\\_ep\\_cons\\_2010-12-15\\_en.pdf](http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_4_sent_to_ep_cons_2010-12-15_en.pdf)

advisors particularly point towards the opportunity for ENISA to train the trainers, i.e. to develop harmonised European training packages on different levels – from the citizens to the professionals and decision-makers – to be used by the Member States.

### 3.3.6 Concrete needs and opportunities for practical cooperation with international bodies

**EQ41: Which are the concrete needs and opportunities for cooperation and synergies with international bodies working in adjacent fields, like the NATO Cooperative Cyber Defence Centre of Excellence?**

All groups of consulted stakeholders were generally in favour of increased cooperation with international bodies and several examples of such bodies were presented as opportunities for future cooperation. These concern, for example, the United Nations' International Telecommunication Unit (UN/ITU), the Forum of Incident Response and Security Teams (FIRST), the US National Institute of Standards and Technology (NIST) and third country governments. However, with respect to the North Atlantic Treaty Organisation (NATO), stakeholders' views on the possibilities for efficient collaboration differed significantly.

**There is a strong consensus among ENISA's direct stakeholders, advisors and users that increased international collaboration is important, however, opinions differ on whether NATO is the most appropriate partner.** A majority of the interviewed stakeholders were supportive of increased cooperation with international bodies working in adjacent fields. The open public consultation confirmed this, showing that several respondents suggested that there is a need for more international cooperation but suggested approaches focussed on direct cooperation with third countries. Some direct stakeholders indicated in the interviews that there are both strong needs and good opportunities for collaboration with NATO and that there is a movement in the direction to combine civil and military aspects of cybersecurity. However, other direct stakeholders as well as advisors and users were either sceptical of the benefits of collaboration or indicated barriers to it, mainly in the form of reluctance and lack of trust from some Member States (e.g. not all Member States are NATO members), as well as uncertainty on whether this fell within ENISA's mandate. In the open public consultation, civil-military cooperation was among the needs least frequently selected by respondents (see Figure 53).

**In terms of needs and opportunities, several other international bodies were mentioned as interesting for further collaboration in the future.** Apart from the discussion above regarding NATO, the interviews with ENISA's various stakeholders indicated good opportunities for increased collaboration with several international bodies, for example: UN / ITU (brings on-board the poorer countries lacking means to deal with cybersecurity problems), third country governments (exportation of European model legislation, as has been done already for Japan and Qatar), the FIRST community, standard developing organisations (e.g. NIST or similar bodies at international level, the European Telecommunications Standards Institute (ETSI) and the Organisation for the Advancement of Structured Information Standards (OASIS)), Europol and Interpol (as cybercrime and security threats are often closely related).

**ENISA needs to be more clearly positioned as the focal point of cybersecurity in Europe and a natural contact point for international collaboration.** As presented in section 3.2.2.4, ENISA is not widely described as a centre of expertise or as a reference point for stakeholders in the NIS area, mainly due to little visibility and lacking expertise in certain technical fields. Additionally, interviews with direct stakeholders indicated that a clarification with respect to international collaboration in ENISA's future mandate would be useful. It is natural, given ENISA's name, that international actors perceive ENISA as the Single Point of Contact of cybersecurity in Europe and contact the Agency to discuss cybersecurity matters and international cooperation. However, according to one of ENISA's direct stakeholders, it is not clear whether this falls within their current mandate.

### 3.3.7 ENISA’s future mission, tasks, working practices or activities

**EQ42: Could ENISA’s mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape or would another EU initiative be more efficient?**

Although the broad scope of the current mandate was seen as adequate by given stakeholders, others saw a need for more clarity with respect to the activities to be performed. Many direct stakeholders, advisors and users linked the limited resources of the Agency to a need for a clearer mandate, with the work being more focused on key priorities. Furthermore, there was also broad consensus that ENISA needs to develop its in-house expertise in key areas. The difficulties faced by ENISA in recruiting competent staff were identified as a key barrier to its development in this regard. No other EU initiatives were identified as being more efficient or effective than ENISA in responding to the new cybersecurity landscape but open public consultation respondents pointed to other potential EU initiatives that could complement ENISA’s work in the field of cybersecurity.

**Many of ENISA’s stakeholders would like a revision of the mandate, with clarifications of the field of actions and key priorities.** Stakeholders have different views on whether the mandate of ENISA needs to be changed or not to reflect new needs posed by the evolving cybersecurity landscape. Some of the interviewed direct stakeholders, as well as users and advisors of ENISA, think that the current mandate is wide enough (or flexible enough) to cover evolving needs, while other stakeholders think that there are some limitations to the current mandate, e.g. related to uncertainty of which actions ENISA can take to meet the needs from its users and regarding a change towards a more operational role of the Agency. As already pointed out (see e.g. section 3.2.2.8) the size of the Agency is assessed as a weakness by a close majority of surveyed stakeholders<sup>94</sup>. This point is confirmed by the interviews in terms of frequent requests for more resources, particularly from ENISA’s direct stakeholders. Linked to the comments on ENISA’s limited resources numerous interviewees (including Member States) also call for a clearer mandate and better definition of key priorities.<sup>95</sup> A few interviewees also see a need for an improved description of ENISA’s role compared both to other EU agencies (particularly EC3 and CERT-EU) and national cybersecurity agencies. Examples of issues proposed to be clarified or to be specifically mentioned in the mandate are: the Agency’s role in cyber crisis collaboration and support activities for the private.

**There seems to be a general consensus among the stakeholders that ENISA needs to develop its in-house expertise in key areas.** In relation to the need for more staff and greater focus on key priorities, the interviewed stakeholders (both direct stakeholder and users and advisors) see a need for ENISA to develop its expertise and concentrate its resources on fewer projects. The problems identified (see e.g. section 3.2.2.8) in attracting and retaining competent staff, particularly senior experts and technical experts, are reported as a barrier in this sense, together with the need for a revision of the current recruitment procedures. A few direct stakeholders propose increased interaction and knowledge sharing with Member States cybersecurity and NIS experts to increase the competencies of ENISA’s staff. This latter approach is in line with the results of the CSIRT survey, as increased interaction between ENISA and CSIRT, together with more training activities, were seen as particularly important by respondents.

**While respondents to the open public consultation pointed to other EU initiatives to help respond to current gaps and needs, these were not seen as alternatives to ENISA.** Open public consultation respondents were asked to propose what other, if any, EU initiatives could be

<sup>94</sup> This refers to the “ENISA survey”.

<sup>95</sup> This is in line with previous evaluations key explanations to some of the shortcomings regarding effectiveness, namely 1) the broad mandate and the variety of tasks it seeks to fulfil, and 2) issues with staff recruitment and limited resources.

put in place to address the gaps and needs identified (see section 3.3.1). In total, 38 respondents commented on what these other EU initiatives could be:

- National authority respondents felt that other EU initiatives could focus on “increased funding for capacity building and joint operational ventures, particularly for smaller Member States” and “further financial programmes to support CSIRTs capabilities and SMEs protection”. For this, ENISA should be allowed to participate in funding programmes to ensure more effective work with Member States and to extend the range of activities it offers.
- Respondents from private enterprises and business associations commented on various topics: Specifically on the NIS Directive, a few respondents felt the current legislation was already outdated before the implementation process had been completed in Member States; therefore a revision of the Directive was considered necessary. One respondent proposed to adopt an EU-wide implementation of the US NIST framework which provides flexible and cost-effective risk based approaches and supply chain resilience, and suggested that its implementation would enable to streamline best practices across all sectors. Other contributions showed strong support for the EU to invest more in addressing the cyber skills gap ranging from basic education to professional qualification and advanced training of skilled and specialised cyber experts.
- Respondents from the other stakeholder groups agreed that there must be an approach to legislation, particularly since the “slightly chaotic process surrounding the launch and subsequent debate on the NIS Directive”. Additional laws were not seen as necessary, but rather “effective continuous action” by focusing on education and information sharing at a fast pace. Other respondents also saw the need for the “establishment of a dedicated funding or financial programme for cybersecurity research”, suggesting it as a “powerful incentive for government, universities and the private sector to help archive security goals”.

### 3.3.8 Conclusions on ENISA’s SWOTs

In the context of the rapid evolution of the technological landscape and the related intensification of cybersecurity threats, increased cooperation between different authorities and communities (public and private), increased capacities at Member States level and further research into cybersecurity challenges, were identified as particularly important needs. Overall, if sufficiently mandated and resourced, ENISA was considered to be able to contribute to addressing the evolving needs of the NIS domain.

On the **strengths** side, taking into account the borderless nature of cyber-attacks, as well as the concerns Member States have in disclosing sensitive information, ENISA is a neutral facilitator with policy expertise in the domain of cybersecurity.<sup>96</sup> The Agency is well placed to help Member States and EU institutions find common ground for agreement in the face of divergent priorities, and strengthen the levels of cooperation and collaboration among them. As noted by s noted by all of the consulted stakeholder groups and in the reviewed documentation<sup>97</sup>, cyber resilience is a key element in the cybersecurity domain, and thus ENISA’s central role in strengthening cyber resilience, by helping Member States to foster their capability and capacity development, has been identified as one of the Agency’s strongest assets. The prompt eruption of new vulnerabilities and the difficulty to mitigate the attacks point to the need to involve different kinds of stakeholders in order to present a more comprehensive approach. ENISA has extensive experience engaging with different types of stakeholders which, combined with its expertise in collecting and sharing pan-

<sup>96</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0.; See ENISA (2015). CYBER 7: Seven messages to the edge of Cyber-Space; Catalogue Number: TP-04-15-745-EN-C; ISB: 978-92-9204-133-5. And Largely confirmed by ENISA stakeholder interviews.

<sup>97</sup> See, for example European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe’s Cyber Resilience System and Innovative Cybersecurity Industry; Bendiek, A. (2012) ‘European Cyber Security Policy’, SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

European data, can facilitate the identification and dissemination of best practices to overcome diverse challenges.<sup>98</sup>

ENISA is faced with several **weaknesses** that affect its role and effectiveness in the European cybersecurity landscape. ENISA has limited visibility in the press, media and among the general public due to weak communication and marketing, as well as limited self-assertion, meaning that its voice is only softly heard in the EU's diverse, fragmented cybersecurity landscape. What is more, ENISA's lacks a long-term vision as it is too constrained by its annual work programme. Aside from these substance-related challenges, there are more structural weaknesses that also have been identified in the evaluations of ENISA's activities in 2014 and 2015. ENISA lacks sufficient human and financial resources to complete its various activities to a high standard. The size of the Agency was considered by several stakeholders<sup>99</sup> to be insufficient to handle all the tasks entrusted to it, including the new tasks imposed by the NIS Directive. An additional burden concerns ENISA's difficulties to attract and retain qualified human resources.

The NIS Directive can be seen as an **opportunity** for ENISA to increase its role and importance in the cybersecurity landscape. In the light of increased levels of digitisation and rapidly evolving cyber-threats, ENISA could profit from growing demands for synergies between operators, e.g. digital service providers, encouraging collaboration across different sectors and stakeholders concerned or affected by cybersecurity policies. According to several industry representatives, one area of great potential for ENISA concerns the introduction of ICT standardisation and certification with a view to supporting further integration of the Single Market and consumer trust.<sup>100</sup> In addition, ENISA's users and advisors agree that there is an acknowledged need and demand for awareness raising in the field of cybersecurity and ENISA could have a strong role in coordinating future action in this regard.

From a formative, future-oriented perspective, ENISA is faced with several **threats** that impact on the cybersecurity context in which the Agency is operating. Attacks are not only becoming more sophisticated, but are also more pervasive. The rapidly changing landscape, in addition to the growth in the interconnectivity of devices, have been recognised in several studies<sup>101 102</sup> as contributors to the prompt eruption of new vulnerabilities and difficulties in mitigating attacks. A lack of capacity to meet such rapidly changing threats is considered an important threat faced by ENISA. Furthermore, ENISA is dominated by Member States' divergent priorities and capabilities. Since Member States have difficulties agreeing on common action in ENISA, the outcome is often the least threatening action to all Member States. This in turn is limiting ENISA's scope of action.<sup>101</sup> A further contextual threat concerns the general fragmentation of EU cybersecurity policy with several, at times competing, agencies active in the cyber-policy domain. Last but not least, there is a recognised lack of trained experts in cybersecurity in Europe which aggravates the Agency's recruitment difficulties.<sup>103</sup>

The table in Appendix 5 presents a more comprehensive compilation of ENISA's SWOTs, while Figure 59 below summarizes the main SWOTs identified.

---

<sup>98</sup> European Commission (2013). JOIN (2013) 1 final: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

<sup>99</sup> Findings from the ENISA survey as well as from stakeholder interviews

<sup>100</sup> See interviews; the proposal for further action equally appears in: See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

<sup>101</sup> Accenture and HfS Research (2016). The State of Cybersecurity and Digital Trust 2016.

<sup>102</sup> EY (2015). Cybersecurity and the Internet of Things.

<sup>103</sup> Finding from ENISA stakeholder interviews.

**Figure 59: ENISA's main SWOTs**

<p><b>Strengths</b></p> <ul style="list-style-type: none"> <li>- Neutral, facilitator, free of political bias or commercial interests</li> <li>- Recognised support to Member States in capacity building &amp; capability development to strengthen resilience to cyber-threats</li> <li>- Acknowledged collaboration &amp; community building reaching wide range of actors, incl. Member States, industry, EU bodies etc.</li> <li>- Horizontal expertise, "landscape overview" of Member States cybersecurity policies</li> </ul>	<p><b>Weaknesses</b></p> <ul style="list-style-type: none"> <li>- Low visibility for various reasons: Lack of expertise, weak communication/marketing and limited self-assertion within the EU cybersecurity policy landscape</li> <li>- Lack of a long-term, strategic vision</li> <li>- Recruitment difficulties</li> <li>- Reduced efficiency due to split location</li> <li>- Distance to EU decision makers in Brussels</li> <li>- Lack of financial and human resources to make a difference</li> </ul>
<p><b>Opportunities</b></p> <ul style="list-style-type: none"> <li>- Growing need for synergies between ICT operators to ensure concerted and collaborative NIS policy actions</li> <li>- NIS Directive bears the potential to strengthen ENISA's role in EU cybersecurity policy</li> <li>- There is an acknowledged need and demand of stakeholders to strengthen awareness raising of cybersecurity</li> <li>- Stronger support in the community is evolving for ICT standardisation and certification</li> </ul>	<p><b>Threats</b></p> <ul style="list-style-type: none"> <li>- Policy fragmentation at EU level and diverging policy priorities in EU Member States constrain ENISA's scope of action</li> <li>- Rapidly evolving and complex threat landscape involving multiple disciplines create new vulnerabilities, e.g. IoT</li> <li>- Lack of overall (technical) talent in the field of cybersecurity aggravates ENISA's recruitment difficulties</li> </ul>

## 4. CONCLUSIONS AND RECOMMENDATIONS

On the basis of the findings presented above, this section presents overall conclusions on the successes of ENISA and the most pressing issues that need to be addressed in order to ensure a coherent approach to NIS in Europe in the future. These issues are situated at the more strategic, policy level and at the level of ENISA as the subject of this study and one of the current players in this sphere. Following on from these, a series of possible options to review the current mandate of ENISA have been presented, including an assessment the costs of each of these options, their potential EU added value and their impact on ENISA's coherence with national and EU cybersecurity bodies.

### 4.1 Successes of ENISA

Over the 13 years of its existence ENISA has made some important achievements towards increasing NIS in the EU. The main successes of ENISA, identified on the basis of the findings and conclusions of this evaluation study are presented below.

**ENISA implements activities and provides services in an area of rapidly increasing relevance.** The increased frequency, sophistication and potential impact of cyber-threats shows the need for a coordinated approach across the EU. This is where ENISA's objectives to contribute to securing NIS in Europe through the provision of expertise, increasing capacities, fostering cooperation and supporting the development and implementation of legislation and policies is of high relevance. Overall, if sufficiently mandated and resourced, ENISA was considered to be able to contribute to addressing the evolving needs of the NIS domain.

**ENISA has contributed to building a community of cybersecurity stakeholders across the EU.** ENISA has proven capable of maintaining a viable network with a range of different stakeholders comprising national authorities, the EU institutions and bodies, academia, civil society organisations and to some extent also the private sector. ENISA is perceived as a trusted partner and acts as a node between the different organisations to gather and exchange information and best practices among Member States and beyond. A main success is the establishment of the a network of CERT/CSIRT which benefitted from training and workshops thereby fostering coordination and exchange.

**ENISA's has increased capacity and coordination on cyber-attacks in the EU.** In particular with the cyber exercises ENISA has brought together public and private stakeholders to increase their understanding of and capacities in NIS. As one of the Commission representatives pointed out in the context of the study, following the recent attack of multiple variants of a ransomware named WannaCry which affected many organisations in the European Union, ENISA successfully ensured cyber cooperation at EU level for the first time<sup>104</sup>. Other capacity building activities, such as trainings and the provision of manuals further contribute to better prevention, detection and response to incidents across the EU.

**ENISA makes NIS knowledge available and accessible.** Some of ENISA's publications have been highly appreciated and are considered to be very useful. ENISA's publications provide relevant information on cybersecurity issues from an EU-wide perspective. The publications present technical expertise in a language that is accessible to policy makers and a broader public. Publications that were specifically highlighted by stakeholders as contributing to the study cover

---

<sup>104</sup> See also: ENISA's press release on the issue. Available at: <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level>



issues such as incident reporting, cloud computing and crisis management. ENISA's neutrality as a decentralised EU agency is appreciated by the public and private sector.

**Finally, ENISA has contributed to increasing awareness about cybersecurity across the EU through the cybersecurity month.** While the activities are increasingly organised by Member States with more independence from ENISA, the Agency has contributed to setting up this activity which reaches public and private stakeholders, as well as citizens across the EU with the aim of increasing their understanding of the risks posed to NIS.

**ENISA efficiently implements its assigned tasks.** ENISA's staff are highly dedicated to their work and ensure that despite tight resources, planned outputs are delivered. Within the Agency efficient work processes have been established with a clear delineation of responsibilities.

#### 4.2 Most pressing issues at the strategic / policy level

The most pressing issues that need to be addressed in order to ensure a coherent approach to cybersecurity in Europe on the basis of the findings and conclusions of this study are presented below.

**Cybersecurity at the EU institutional level is fragmented:** There are a number of EU-level actors that are active in the cybersecurity area including ENISA, CERT-EU and EC3 (Europol), leading to a fragmented approach towards cybersecurity among EU institutions. There is no one central point of reference for cybersecurity in Europe. While the mandates of these organisations are in theory different, their roles are not clearly defined in practice and there is a potential for overlap, as the positioning exercise presented in section 3.2.4.3 points to. Within this context, ENISA has had difficulty carving out a place for itself and has found other organisations such as CERT-EU in particular filling a gap by carrying out activities that would from a legal perspective fall within ENISA's remit.

**The institutional and legal framework for cybersecurity in Europe is rather weak:** Cybersecurity has not been seen as a legal priority at EU-level until more recently. The Single Market acquis<sup>105</sup> do not apply to digital services to the same extent as to other areas. This has had an impact on the degree to which cross border cooperation in relation to NIS is working. Cybersecurity is primarily an area of national competence, while in reality it is an issue that transcends borders; an effective strategy for the prevention, mitigation and response to cyber threats/attacks requires cooperation across Member States. The advent of the NIS Directive, the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (COM(2016) 410), and the priorities set by the Digital Single Market Strategy (COM(2015) 192) represent key new pillars to strengthening the institutional and legal framework for cybersecurity in Europe going forward.

#### 4.3 Most pressing issues at the ENISA level

At the level of ENISA, the study's findings point to a series of issues that would need to be addressed in order for the Agency to play a key role in cybersecurity in Europe going forward.

**ENISA lacks visibility:** ENISA has not been able to carve out a strong, clear place for itself within the European cybersecurity landscape. While it is known and recognised within its circle of stakeholders, it has not managed to develop a strong brand name or be seen as the one point of reference at European level for cybersecurity. A number of factors help to explain this, including the fragmented nature of cybersecurity in Europe with multiple actors seeking to position

---

<sup>105</sup> [http://ec.europa.eu/internal\\_market/copyright/acquis/index\\_en.htm](http://ec.europa.eu/internal_market/copyright/acquis/index_en.htm)

themselves within the areas of prevention, mitigation and response. Finally, the degree to which ENISA has been “allowed in” and consulted by the Commission and other players acting at EU level in this field has impacted on its visibility. While ENISA is more frequently consulted than in the past, it is not necessarily present in all relevant fora dealing with or funding programmes (e.g. CEF) related to cybersecurity at European level.

**ENISA does not have sufficient financial or human resources at its disposal to effectively respond to its broad mandate:** Despite evolutions over the past few years in the degree of importance of cybersecurity and an according increase in the scope of ENISA’s mandate, ENISA’s budget has remained very limited. With the advent of the NIS Directive and the new tasks entrusted to it, e.g. taking part in the Cooperation Group and acting as the secretariat for the CSIRT Network, it has also had to prioritise and set aside some of the areas it has previously focussed on, thereby further depleting resources. While the evaluation suggests that there is potential for ENISA to increase its efficiency by introducing more flexibility in their programming cycle or automatization of some of the administrative processes, such improvements would not be sufficient in their scope to allow it to effectively respond to its broad mandate. An important area for improvement is recruitment. ENISA has difficulty recruiting and retaining the staff required for it to have the necessary expertise at its disposal to perform tasks in-house and in some cases to the quality standards expected (i.e. reference was made by stakeholders to the varying levels of quality of ENISA reports/publications in particular). This is due to both internal (i.e. slow recruitment procedures in a fast-paced, competitive environment; a lack of career progression prospects) and external factors (i.e. small budget; constraining staff management rules (e.g. number of CAs versus TAs); an expertise shortfall in the sector; and a lack of competitive salaries in an area that is dominated by demand from the private sector.

**ENISA is not perceived as a proactive, visionary Agency:** ENISA’s mandate is broad enough to be all encompassing and allows for flexibility in the tasks it carries out. This leads to it being reactive by seeking to fulfil needs of as many stakeholders as possible and not being focussed, proactive and visionary. Stakeholders suggested that increased expertise within the Agency and a stronger focus on research could allow for ENISA to be more abreast of developments in cybersecurity. To make use of this knowledge, ENISA would need to be able to be more flexible in setting its own work priorities. One of the factors explaining this is the Member State dominance (via the Management Board) of the work programme. Given the differing needs and priorities of Member States, there is not a common line among Member States and the work programme tends to lead to ENISA having work priorities that represent the lowest common denominator among Member States and are not perceived as threatening to the national competence of given Member States. As such, ENISA has a tendency to spread itself too thin, as also concluded in the 2015 evaluation.

**There is little consensus on what the future role of the Agency should be:** The divergent needs of ENISA’s stakeholders lead to a lack of consensus on whether the Agency should take on a more operational role, or continue to be an Agency acting solely at the strategic level. In taking on a more operational role, it could gather data, monitor and share information on incidents occurring throughout the EU in order to ensure increased transparency and enable Member States to coordinate joint responses to incidents where this proves necessary. While Member States with fewer resources at their disposal and industry would perceive this as a positive development, Member States with strong cybersecurity capacity tend to see it as an encroachment on their area of national competence.

#### 4.4 Options for the future

Table 26 below sets out a set of possible options to review the current mandate of ENISA, including the issues that they would seek to address and expected results of the different factors for change that could be considered under each option. It also presents an assessment of the added value of each of the new changes foreseen and of the risk of overlap with the tasks and activities of other national, European or international bodies. The third table provides an estimation of the costs related to each of the factors for change derived from the results of the evaluation; these are based on a series of assumptions, as presented in the table.

The section therefore serves to respond to the evaluation questions presented below.

**Table 25: Evaluation questions on the options for the future of ENISA**

<p><b>Prospective</b> EQ43: What would be the financial implications associated with each of the possible options for modifying ENISA’s mandate as they emerge from the evaluation?  EQ44: If any new tasks for ENISA are identified (e.g. through EQ4 and EQ37), do these represent EU added value?  EQ 45: Taking into account the new tasks (identified during the evaluation), will there be any risk of ENISA’s tasks and activities overlapping with those of other national, European or international bodies?</p>
---

**Table 26: Options for the future – the key issues they will address and expected results**

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
<p><b>Option 0: Baseline, maintain the status quo</b>  This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation and Telecoms Framework Directive would need to be taken into account.</p>	<p>N/A as status quo</p>	<p><b>Revise ENISA’s mandate to make its new tasks as per recent/upcoming legislation more specific:</b></p> <ul style="list-style-type: none"> <li>• <b>Involvement in Cooperation Group:</b> Support MS cooperation on drafting and maintaining over time voluntary guidelines on security measures</li> <li>• <b>CSIRT Network Secretariat:</b> Provide technical support for back-end services that enable CSIRTs to exchange information on best practices</li> </ul>	<p>Continuation of status quo</p> <p>If factor for change is implemented (review of mandate in light of new tasks) – Increased coherence of ENISA’s mandate and thus activities with EU cybersecurity policies</p>	<p>N/A as status quo (see section 3.2.4.5 and section 3.2.5.1)</p>

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
		<p>and actual incidents and threats, as well as support voluntary cooperation in case of incidents</p> <ul style="list-style-type: none"> <li>• <b>Electronic communications code, recital 92:</b> Contribute to an enhanced level of security of electronic communications by, amongst other things, providing expertise and advice, and promoting the exchange of best practices</li> <li>• <b>eIDAS:</b> (1) Recital 39 - Enable the EC and MSs to assess the effectiveness of the breach notification mechanism introduced by this Regulation by, for example, aggregating the national reports provided by supervisory bodies into an annual Report on EU Breaches in Trust Service Providers. (2) Support supervisory authorities in the drafting and supervision of security measures of Trust Services through, for example, supporting national regulators in the drafting and maintenance of guidelines on security measures and incident notification formats and procedures on Trust Services</li> </ul>		
<p><b>Option 1: Expiry of ENISA mandate (terminating ENISA)</b></p> <p><b>This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under,</b></p>		N/A	See section 3.2.5.3	N/A

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
<p><b>for example, the NIS Directive and bilateral or regional ties at Member State level.</b></p>				
<p><b>Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate)</b></p> <p><b>This option concerns making significant revisions to ENISA’s mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.</b></p>	<p>The current level of cyber threats in the EU requires an enhanced, coordinated approach</p> <p>Member States with fewer cybersecurity capacities need support to prevent, mitigate and respond to cybersecurity threats</p> <p>ENISA is not perceived as a proactive, visionary agency</p>	<p><b>Strengthen ENISA’s operational role:</b></p> <ul style="list-style-type: none"> <li>• <b>Provide periodic threat intelligence and ad hoc alerts:</b> ENISA would develop and maintain its own threat intelligence capacity in order to monitor the threat landscape and provide MSs fast alerts/warnings on emerging threats and risks and monitor security incidents, including those affecting specific MSs. This would involve: (1) producing regular threat intelligence reports including high-level strategic analyses on threats, incidents and trends (e.g. key technological developments) and (2) collecting and analysing public communications on an event and compiling EU-level flash reports and guidance to businesses and citizens.</li> <li>• <b>Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level:</b> ENISA would: (1) organise cybersecurity exercises to test the Blueprint at all levels – operational, tactical and strategic) with all stakeholders; (2) collect and aggregate reports from national sources (CSIRTs) to establish a common situation awareness report for decision</li> </ul>	<p>Based on information shared by the Member States, ENISA will be able to provide a common baseline and up-to-date threat analysis</p> <p>The Agency will ensure cooperation and coordination across the Member States in case of an incident concerning several Member States</p> <p>ENISA would support capacity building in Member States through the provision of technical assistance on an on-demand basis</p> <p>ENISA will further assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents</p>	<p><u>EU added value of new tasks:</u> These tasks aimed at strengthening ENISA’s operational role represent EU added value as there is a need for data to be gathered at EU level to provide a common baseline and up-to-date threat analysis in order to share knowledge, foment cooperation among Member States and help better respond to cyber security incidents that are cross-border in their nature</p> <p>There is also a need for capacity to be increased, in particular among smaller Member States that tend to invest fewer resources in cyber security, through the exchange of knowledge and expertise <u>at EU level</u></p> <p><u>Coherence with tasks of other bodies:</u> With a strengthened operational role foreseen for ENISA there will be a need to clarify the respective roles of other EU bodies active in the area and which have been seeking to fill a vacuum in some of these areas (e.g. CERT-EU), as well as increase coordination between them</p>

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	<p>The institutional and legal framework for cyber security in Europe is rather weak</p> <p>The current level of cyber threats in the EU requires an enhanced, coordinated</p>	<p>makers in the event of an incident; (3) support technical handling of the incident, including facilitating sharing of technical solutions between MSs; (4) handle public communication around the incident; (5) in case of a major crisis, propose the activation of the political decision making (IPCR) by alerting all or one of the EU institutions; (6) publish flash report or alerts in the event of significant events or incidents based on publically available information OR information made available through the CSIRT Network</p> <ul style="list-style-type: none"> <li>• <b>Provide emergency cybersecurity response:</b> ENISA would provide on-demand technical assistance to MS bodies and institutions by creating and maintaining a team of experienced senior cybersecurity incident advisors who may be sent to MSs upon their request to assist and contribute to cybersecurity incident response and recovery</li> </ul> <p><b>Strengthen ENISA’s role in policy development and implementation:</b></p> <ul style="list-style-type: none"> <li>• Establish ENISA as an agency that has to be involved by other EU bodies, including the Commission, when cybersecurity matters are being considered</li> <li>• Formally involve ENISA in the implementation of the Connecting Europe Facility on</li> </ul>	<p>ENISA will play a stronger role in assisting the Union institutions, bodies, offices and agencies and Member States in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to a</p>	<p><u>EU added value of new tasks:</u>                      These tasks aimed at strengthening ENISA’s role in policy development and implementation represent EU added value in that this policy development is happening at the EU level and ENISA has a cross-Member State perspective on cyber security on the basis of the multi-stakeholder network it has managed to establish and can draw on</p>

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	<p>approach</p> <p>ENISA lacks the visibility required to ensure it is seen as a key player and called upon to play an active role in EU policy making on cybersecurity</p>	<p>Telecom as an advisory body</p> <ul style="list-style-type: none"> <li>Establish semi-formal governance structures with regular meetings between ENISA and other agencies/international organisations (e.g. on given common themes such as training) to increase cooperation at EU institutional level</li> </ul> <p>Increase ENISA's visibility:</p> <ul style="list-style-type: none"> <li>Set-up a liaison office in Brussels with two to three permanent employees</li> <li>Create a dedicated communications team within ENISA</li> </ul>	<p>less fragmented, more coherent legal and institutional framework and ultimately the proper functioning of the internal market</p> <p>ENISA will be able to more easily and cost-effectively ensure a presence in Brussels and build awareness, notably when it comes to its strengthened role in policy development and implementation, but also in relation to research and innovation</p> <p>EU institutions and bodies will benefit from ENISA's input on cybersecurity</p> <p>EU institutions and bodies, Member States and other stakeholders will be more aware of the expertise and support available through ENISA</p>	<p>Coherence with tasks of other bodies:</p> <p>Increasing ENISA's involvement in policy development and implementation will imply the Agency increasing its ties and involvement with other bodies active in the area, thereby increasing the potential for synergies to be developed</p>
	<p>The institutional and legal framework for cyber security in Europe is rather weak</p> <p>There is limited long-term planning for ENISA's activities</p> <p>ENISA's work programme is dominated by the interests of Member</p>	<p><b>Make ENISA's mandate permanent:</b></p> <ul style="list-style-type: none"> <li>This would involve ENISA having a permanent mandate, but still allow for the periodic evaluation of the performance of the Agency</li> </ul> <p><b>Strengthen ENISA's governance structure:</b></p> <ul style="list-style-type: none"> <li>Formally involve other stakeholders in the</li> </ul>	<p>ENISA will be put on the map, ensuring a more permanent presence and longer-term, strategic outlook</p> <p>Will lead to an increase in staff retention, planning and competence development by providing a more long term perspective</p> <p>ENISA will be less Member State dominated, thereby leading to a work programme that takes into</p>	<p>EU added value of new tasks: N/A</p> <p>Coherence with tasks of other bodies: N/A</p> <p>EU added value of new tasks: N</p>

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	States	<p>governance of ENISA by increasing the weight of the PSG in playing an advisory role on ENISA's Work Programme</p> <ul style="list-style-type: none"> <li>Allow more flexibility for ENISA to determine its own work priorities at Executive Board level</li> </ul>	<p>account the needs of a variety of stakeholders including those of the EU institutions and the private sector</p> <p>The Agency will use its expertise to stimulate further cooperation between actors from the public and private sector</p> <p>The needs of the private sector will be better addressed</p>	<p>Coherence with tasks of other bodies: N/A</p>
	<p>There is a need for EU level coordination on standardisation and certification of ICT</p>	<p><b>Include a role for ENISA in EU-level standardisation and certification:</b></p> <ul style="list-style-type: none"> <li><b>Support the EU ICT Security Certification Framework:</b> Put in place an EU ICT security certification framework whereby ENISA would play a supporting role by (1) providing the secretariat and actively supporting the work undertaken (e.g. convene meetings of the framework's governance structures and meetings and engagements with industry stakeholders);(2) providing technical expertise to Member States (e.g. MS taking part in the framework on issues related to security testing and vulnerabilities in ICT products); and (3) compiling and publishing guidelines concerning the security requirements of ICT products and services in cooperation with national authorities and</li> </ul>	<p>Standardisation will be further supported</p> <p>ENISA would support capacity building in the Member States through the provision of technical expertise</p>	<p><u>EU added value of new tasks:</u> These tasks aimed at strengthening ENISA's role in standardisation and certification represent EU added value in that action in this area needs to take place at a cross-European level and ENISA, with its wide network of EU-level stakeholders, demonstrated ability as a neutral player to support cooperation across Member States and stakeholders with differing views and its ability to compile and report on technical issues, will be key in ensuring this</p> <p><u>Coherence with tasks of other bodies:</u> In performing these tasks, ENISA will draw on existing sources to come up with assessments and guidelines and fill a void in this area at EU level. There is therefore limited risk of overlap of its activities in this area with other bodies at EU and international level. At national level, there is a risk of duplication of efforts where given Member States make their own recommendations/provide guidelines in this area.</p>



Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	<p>industry, thereby communicating the work of the framework to industry, consumers at EU and international level</p> <ul style="list-style-type: none"> <li>• <b>Support ICT security standardisation</b> : ENISA would provide a supportive role in facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services, including by cooperating with Member States on technical areas concerning the security requirements for operators of essential services and digital service providers. This could involve supporting the work of the EU ICT Security Certification Framework in EU and international standard organisations; taking part in and contributing to the work of cybersecurity working groups of the European Standardisation Organisations (ESCs); performing reviews and assessments of cybersecurity related standards when associated with regulatory and legal requirements (e.g. eIDAS)</li> </ul>	<p>Research and development will be further supported</p> <p>ENISA's presence in this area will be strengthened, thereby increasing its visibility and its access to information on latest technological</p>	<p>EU added value: These tasks aimed at strengthening ENISA's position relative to R&amp;I represent EU added value in that ENISA has a cross-Member State perspective on what is going on in the cyber security field on the basis of the multi-stakeholder network it has</p>	
<p>Cyber security at the EU institutional level is fragmented</p> <p>ENISA is not perceived as a proactive, visionary Agency</p>	<p><b>Strengthen ENISA's position relative to research and innovation:</b></p> <ul style="list-style-type: none"> <li>• <b>Take part in programming implementation</b>: ENISA would implement parts of the Framework Programme for R&amp;I which relates to</li> </ul>			

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	<p>ENISA lacks the visibility required to ensure it is seen as a key player and called upon to play an active role in contributing to research and innovation</p>	<p>cybersecurity whereby the EC delegates the relevant powers by performing the following tasks: (1) managing some stages of the programme implementation and some phases in the lifetime of specific projects on the basis of WPs adopted by the EC; (2) adopting the instruments of budget execution for revenue and expenditure and carrying out all the operations necessary for the management of the programme; and (3) providing support in programme implementation. Examples of the activities ENISA could perform include implementing calls on Public Procurement of Innovation (PPI) in close collaboration with MS authorities, and supporting MS public procurers in identifying common research and innovation requirements</p> <ul style="list-style-type: none"> <li>• <b>Take part in programming through playing an advisory role:</b> ENISA would play an expert advisory role in the cyber security-related elements of EU R&amp;D funding programmes (H2020, CEF) by sitting on an advisory committee, providing independent advice and input and feeding into ideas for research.</li> <li>• <b>Benefit from EU R&amp;I funding:</b> Open ENISA's mandate to take part in EU R&amp;D funding programmes (H2020, CEF) as a recipient of</li> </ul>	<p>developments</p>	<p>managed to establish and can draw on</p> <p><u>Coherence with tasks of other bodies:</u> By taking part in programming implementation, ENISA would take on a series of tasks currently implemented by the European Commission, thereby ensuring a lack of overlap. Moreover, there is no other cyber security-focussed body at EU level involved in advising at programme level.</p>

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
<p><b>Option 3: European Agency with full operational capabilities (Establish a European Centre of Cybersecurity)</b></p> <p><b>This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.</b></p>	<p>Cyber security at the EU institutional level is fragmented</p> <p>The current level of cyber threats in the EU requires an enhanced, coordinated approach</p>	<p>funding by changing the provisions on source of revenue but not adding it as a task. ENISA can provide added value to industry and academia in R&amp;I by leveraging its practical expertise in areas such as cooperation, information sharing and regulatory requirements.</p> <p><i>Note: Either one or the other options set out above could be pursued due to issues of conflict of interest.</i></p> <p><b>Create an EU level cyber security umbrella:</b></p> <ul style="list-style-type: none"> <li>Develop an umbrella organisation covering ENISA and CERT-EU, thereby bringing together three main functions, namely policy advice, centre for information and Computer Emergency Response Team. The operational role of CERT-EU in responding to cyber incidents in the EU institutions would therefore be combined with ENISA's role of ensuring cooperation in the event of an incident. The new organisation would act as an EU contact point for cybersecurity related issues in close coordination with the EEAS. Options include merging ENISA and CERT-EU and having a governance structure that would allow different reporting lines and oversight for the team dealing with the EU institutions, or integrating (part of) CERT-EU within ENISA as one of the</li> </ul>	<p>A more coordinated response to cyber incidents would be ensured across the EU and its various players</p> <p>Member States would receive direct support when responding to cyber incidents</p>	<p><u>EU added value of new tasks:</u> N/A</p> <p>Coherence with tasks of other bodies: The potential for overlap between ENISA's work and that of CERT-EU would be avoided</p>

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	<p>Cyber security at the EU institutional level is fragmented</p> <p>The current level of cyber threats in the EU requires an enhanced, coordinated approach</p> <p>ENISA is not perceived as a proactive, visionary Agency</p>	<p>Agency's departments.</p> <p><b>Create a virtual European CSIRT:</b></p> <ul style="list-style-type: none"> <li><b>Coordinate CSIRT Network operations:</b> Enable the Agency to coordinate the operations of MS CSIRTs, collecting information and pooling national resources on analysing threats and responding to incidents</li> <li><b>Produce real time situational awareness and intelligence feeds:</b> Enable ENISA to act as a broker, sharing information on incidents between Member States in the form of real-time situational awareness and dynamic (live) threat intelligence feeds on the basis of information exchanged on the CSIRT Network</li> <li><b>Maintain and provide own cybersecurity incident response capacity to public and private sector:</b> ENISA would create and maintain the capacity to provide on-demand technical operational assistance to MS CSIRTs, operators of essential services, EU bodies and institutions for the prevention, detection and response to incidents</li> </ul>	<p>Creation of a more coherent, stronger CS presence in Europe</p> <p>Based on information shared by the Member States, ENISA will be able to provide a real time threat analysis</p> <p>The European CSIRT will ensure cooperation and coordination across the Member States in case of an incident concerning several Member States</p> <p>The European CSIRT would support capacity building on an on-demand basis in the public and private sector</p> <p>The European CSIRT would further assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to security problems and incidents</p>	<p><u>EU added value:</u></p> <p>These tasks aimed at creating a virtual European CSIRT represent EU added value as there is a need for real-time data to be gathered, assessed and shared at EU level to provide common, real-time situational awareness and dynamic (live) threat intelligence, foment cooperation among Member States and help better respond to cyber security incidents that are cross-border in their nature</p> <p>There is also a need for capacity to be increased, in particular among smaller Member States that tend to invest fewer resources in cyber security, through the exchange of knowledge and expertise at <u>EU level</u></p> <p><u>Coherence with tasks of other bodies:</u></p> <p>Such a body aimed at providing response services to stakeholders other than EU institutions, agencies and bodies does not currently exist at EU level.</p> <p>However, if such a body were created independently of CERT-EU, there would be a need to clarify the respective roles of other EU bodies active in the area and which have been seeking to fill a vacuum in some of these areas (e.g. CERT-EU), as well as increase coordination between them</p> <p>As above</p>
	<p>As above</p>	<p>All factors related to Option 2 would/could be fulfilled under Option 3 as well</p>	<p>As above</p>	<p>As above</p>

#### 4.5 Costs of the options

This section provides an estimation of the costs related to each of the factors for change derived from the results of the evaluation of ENISA. The estimations are presented in two tables: The first table (Table 27) provides an **overview of the estimated costs per option and per grouped factors of change**. It should be read in combination with the second table (Table 28) which provides more **detail on the costs per factor of change** and the **specific assumptions** applicable to the estimations of each of the individual cost factors.

The costs are based on a series of **general assumptions**:

- It has been assumed that the Greek government will continue to provide its current financial contribution (of EUR 640,000 per year) for the offices in Heraklion and Athens.
- It has been assumed that Temporary Agents (TAs) would implement the new tasks foreseen and averages of the salaries (as per Article 66 of the Staff Regulations, applicable from 1 July 2016) of categories of TAs minus the 79.3% corrective coefficient for Greece have been applied as follows: Junior experts/analysts (grades AD5 to 6 – EUR 4,214/month, equivalent to EUR 50,568/year), Senior experts/analysts (grades AD7 to 12 – EUR 7,046/month, equivalent to EUR 84,552/year) and Heads of Unit (grades AD9 to 14 – EUR 9,020/month, equivalent to EUR 108,240/year). For staff based in Brussels, no coefficient applies.
- For the calculation of overall costs per option, efforts have been made to take potential synergies between the different factors for change listed under each option into account. However, it can be expected that there are further synergies to be gained should ENISA be changed to take into account all the factors for change listed under Options 2 and 3 in the evaluation study report.
- Additional set-up costs could apply, for example, for staff recruitment; these have not been taken into account here.

The cost estimations are based on several **sources**:

- A variety of stakeholders were consulted in order to further operationalise the factors for change and establish the assumptions presented below. They included representatives of DG CONNECT, ENISA, industry and Member States.
- A number of reports and documents have been consulted, as listed in the table below.

##### Secondary sources

ENISA Annual Activity Report 2015.

Europaid (2017): Current per diem rates. Available at: [https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17\\_en.pdf](https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17_en.pdf). Accessed **16.06.2017**.  
 Proposal for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and **Council Decision 2005/267/EC, COM(2015) 671 final**.

Statista – The Statistics Portal (2016): Rental prices of prime office properties in selected European cities as of 4th quarter 2016 (in euros per square meter per year).

Available at: <https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/>. Accessed **16.07.2017**

ENISA (2017): Statement of estimates (budget 2017). Available at: <https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-2017-annual-budget>. Accessed **16.07.2017**

ENISA (2017): Programming document 2017-2019. Available at: <https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019>. Accessed **19.06.2017**

The cost estimations for each of the four options are presented below. The table presents the costs for year 1 of the introduction of the options, including specific set-up costs where relevant (notably in Option 3). The costs of each option in the following four years are also presented, considering the costs arising once an option is fully implemented. Please note that no standard inflation rate has been applied.

Two scenarios are presented. The first one considers the minimum changes that need to be implemented under each option. Costs thus represent the minimum number of staff and additional meetings that will be needed. The second scenario presents a more ideal situation, where costs represent the staff that need to be hired and meetings to be held for a smoother implementation of the options. Under Option 1 the minimum scenario assumes that ENISA will be able to take on all new tasks assigned to it as per recent legislative changes by reallocating responsibilities and tasks, as it has been done in the 2016 and 2017 Work Programme. The second scenario assumes that ENISA will get another eight staff members (two for each of the key sectors finance, health, transport and energy) to respond to its new responsibilities.

The costs are presented differentiating between staff costs (costs due to additional human resources) and “other” costs for additional office space, meetings or operational activities. These are further explained and specified in Table 28.

Under Option 2 and 3, three sub-options are presented (a, b and c) because there are three different factors of change to strengthen ENISA’s position relative to research and innovation which exclude one another due to issues of conflict of interest. Sub-option a) represents the costs for the factor of change under which ENISA will take part in programme implementation of the Framework Programme for R&I; a lump sum of EUR 3.5 m has been estimated for this factor of change based on a similar function foreseen for Frontex<sup>106</sup> (including additional staff) which is added under “other” costs. Sub-option b) includes the costs of ENISA taking part in programming through playing an advisory role in EU R&D funding. Sub-option c) includes the costs of ENISA befitting from EU R&I funding (which are nil).

**Table 27: Cost estimations for the options –overview**

	Year 1			Year 2 to 5		
	Scenario 1 – Minimum changes	Scenario 2 - Ideal changes	Scenario 1 – Minimum changes	Scenario 2 - Ideal changes	Scenario 1 – Minimum changes	Scenario 2 - Ideal changes
	Costs in EUR per year	Costs in EUR per year	Costs in EUR per year	Costs in EUR per year	Costs in EUR per year	Costs in EUR per year
	Number of staff/ specification of other costs	Number of staff/ specification of other costs	Number of staff/ specification of other costs	Number of staff/ specification of other costs	Number of staff/ specification of other costs	Number of staff/ specification of other costs
<b>Option 0: Baseline, maintain the status quo:</b> This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation and Telecoms Framework Directive would need to be taken into account.						
Current budget	11,244,679.00	11,244,679.00	84	11,244,679.00	84	11,244,679.00
Revise ENISA’s mandate to make its new tasks per	0	676,416	8 (8 senior experts)	0	0	676,416
						8 (8 senior experts)

<sup>106</sup> Based on: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC, COM(2015) 671 final. See SPECIFIC OBJECTIVE NO 6 “Management of Pooled resources and R&D. [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation\\_on\\_the\\_european\\_border\\_and\\_coast\\_guard\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation_on_the_european_border_and_coast_guard_en.pdf)

recent/upcoming legislation more specific	Year 1			Year 2 to 5				
	11,244,679.00	84 (48 TAs, 31 CAS, 5 SNEs) <sup>107</sup>	11,921,095.00	92 (56 TAs, 31 CAS, 5 SNEs)	11,244,679.00	84 (48 TAs, 31 CAS, 5 SNEs)	11,921,095.00	92 (56 TAs, 31 CAS, 5 SNEs)
<b>Total budget under the option</b>	<b>11,244,679.00</b>	<b>84</b> (48 TAs, 31 CAS, 5 SNEs) <sup>107</sup>	<b>11,921,095.00</b>	<b>92</b> (56 TAs, 31 CAS, 5 SNEs)	<b>11,244,679.00</b>	<b>84</b> (48 TAs, 31 CAS, 5 SNEs)	<b>11,921,095.00</b>	<b>92</b> (56 TAs, 31 CAS, 5 SNEs)
<b>Option 1: Expiry of ENISA's mandate (terminating ENISA):</b> This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive and bilateral or regional ties at Member State level.								
Current budget	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84
<b>Costs savings for the EU budget<sup>108</sup></b>	<b>10,322,000.00</b>	<b>84</b>	<b>10,322,000.00</b>	<b>84</b>	<b>10,322,000.00</b>	<b>84</b>	<b>10,322,000.00</b>	<b>84</b>
<b>Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate):</b> This option concerns making significant revisions to ENISA's mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.								
Current budget	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84
Strengthen ENISA's operational role	531,000.00	6 (1 HoU, 5 senior experts)	700,104.00	8 (1 HoU, 7 senior experts)	531,000.00	6 (1 HoU, 5 senior experts)	700,104.00	8 (1 HoU, 7 senior experts)
Strengthen ENISA's role in policy development and implementation	926,142.00	Exercises	926,142.00	Exercises	926,142.00	Exercises	926,142.00	Exercises
	1,140,235.75	13 (3 HoU, 10 senior experts)	1,251,077.00	15 (3 HoU, 12 senior experts)	1,140,235.75	13 (3 HoU, 10 senior experts)	1,251,077.00	15 (3 HoU, 12 senior experts)
	175,320.00	Meetings	175,320.00	Meetings	175,320.00	Meetings	175,320.00	Meetings
Make ENISA's mandate permanent	7,500.00	Office space	7,500.00	Office space	7,500.00	Office space	7,500.00	Office space
Strengthen ENISA's governance structure	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Include a role for ENISA in EU-level standardisation and certification	361,896.00	4 (1 HoU, 3 senior experts)	531,000.00	6 (1 HoU, 5 senior experts)	361,896.00	4 (1 HoU, 3 senior experts)	531,000.00	6 (1 HoU, 5 senior experts)
Strengthen ENISA's position relative to research and innovation sub-option a)	28,002.00	Events/ meetings	58,440.00	Events/ meetings	28,002.00	Events/ meetings	58,440.00	Events/ meetings
	3,500,000	Total costs based on similar function in Frontex	3,500,000	Total costs based on similar function in Frontex	3,500,000	Total costs based on similar function in Frontex	3,500,000	Total costs based on similar function in Frontex
Strengthen ENISA's	192,792.00	2 (1 HoU, 1	277,344.00	3 (1 HoU, 2	192,792.00	2 (1 HoU, 1	277,344.00	3 (1 HoU, 2

<sup>107</sup> Based on: Multi-annual staff policy plan year 2017-2019, Establishment plan in Draft EU budget 2017, in ENISA Programming document 2017-2019; Annex III

<sup>108</sup> Excluding the budget contribution by Greece and other income of the Agency

	Year 1			Year 2 to 5			
	23,373.00	senior expert) Meetings	35,064.00	senior expert) Meetings	23,373.00	senior expert) Meetings	35,064.00
position relative to research and innovation sub-option b)	23,373.00	senior expert) Meetings	35,064.00	senior expert) Meetings	23,373.00	senior expert) Meetings	35,064.00
Strengthen ENISA's position relative to research and innovation sub-option c)	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Additional staff costs sub-option a)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00	29 (5HoU, 22 senior, 2 junior experts)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00
Additional staff costs sub-option b)	2,225,923.75	25 (6 HoU, 18 senior, 1 junior expert)	2,759,525.00	32 (6 HoU, 24 senior, 2 junior experts)	2,225,923.75	25 (6 HoU, 18 senior, 1 junior expert)	2,759,525.00
Additional staff costs sub-option c)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00	29 (5HoU, 22 senior, 2 junior experts)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00
Additional other costs sub-option a)	4,636,964.00		4,667,402.00		4,636,964.00		4,667,402.00
Additional other costs sub-option b)	1,160,337.00		1,202,466.00		1,160,337.00		1,202,466.00
Additional other costs sub-option c)	1,136,964.00		1,167,402.00		1,136,964.00		1,167,402.00
<b>Total budget under the sub-option a)</b>	<b>17,914,774.75</b>	<b>107</b>	<b>18,394,262.00</b>	<b>113</b>	<b>17,914,774.75</b>	<b>107</b>	<b>18,394,262.00</b>
<b>Total budget under the sub-option b)</b>	<b>14,630,939.75</b>	<b>109</b>	<b>15,206,670.00</b>	<b>116</b>	<b>14,630,939.75</b>	<b>109</b>	<b>15,206,670.00</b>
<b>Total budget under the sub-option c)</b>	<b>14,414,774.75</b>	<b>107</b>	<b>14,894,262.00</b>	<b>113</b>	<b>14,414,774.75</b>	<b>107</b>	<b>14,894,262.00</b>



	Year 1				Year 2 to 5			
<b>Option 3: European Agency with full operational capabilities (Establish a European Centre of Cybersecurity):</b> This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.								
Current budget	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84
Create an EU level cybersecurity umbrella	243,125.75	2 (1 HoU, 1 senior expert) Office space	349,753.00	3 (1 HoU, 2 senior experts) Office space	243,125.75	2 (1 HoU, 1 senior expert) Office space	349,753.00	3 (1 HoU, 2 senior experts) Office space
Create a virtual European CSIRT	2,531,104.00	29 (3 HoU, 26 senior experts)	7,500.00	40 (3 HoU, 37 senior experts)	7,500.00	39 (3 HoU, 36 senior experts)	7,500.00	91 (3 HoU, 88 senior experts)
Additional staff costs	2,774,229.75	31 (4 HoU, 27 senior experts)	3,796,201.00	43 (4 HoU, 39 senior experts)	3,651,469.75	41 (4 HoU, 37 senior experts)	8,127,201.00	94 (4 HoU, 90 senior experts)
Additional other costs	7,500.00		7,500.00		7,500.00		7,500.00	
<b>Total budget under the option</b>	<b>14,026,408.75</b>	<b>115</b>	<b>15,048,380.00</b>	<b>127</b>	<b>14,903,648.75</b>	<b>125</b>	<b>19,379,380.00</b>	<b>178</b>
<b>Combined costs of Option 2 a) and 3<sup>109</sup></b>	<b>31,690,557.75</b>	<b>136</b>	<b>33,085,389.00</b>	<b>153</b>	<b>32,567,797.75</b>	<b>146</b>	<b>37,416,389.00</b>	<b>204</b>
<b>Combined costs of Option 2 b) and 3<sup>110</sup></b>	<b>28,406,722.75</b>	<b>138</b>	<b>29,897,797.00</b>	<b>156</b>	<b>29,283,962.75</b>	<b>148</b>	<b>34,228,797.00</b>	<b>207</b>
<b>Combined costs of Option 2 c) and 3<sup>111</sup></b>	<b>28,190,557.75</b>	<b>136</b>	<b>29,585,389.00</b>	<b>153</b>	<b>29,067,797.75</b>	<b>146</b>	<b>33,916,389.00</b>	<b>204</b>

This second table provides more detailed information on the costs of the options. It presents the specific assumptions taken into account to calculate the costs of the factors for change. Please note that where synergies are expected (as detailed in the assumption column) the estimated costs are only taken into account once. Therefore, the costs indicated in the last column of this table cannot be added up to reach the total costs.

**Table 28: Cost estimations for the options – detailed including assumptions**

Options	Factors of change	Assumptions	Estimated costs/year
<b>Option 0: Baseline, maintain the status quo:</b> This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation and Telecoms Framework Directive would need to be taken into account.			
<b>Revise ENISA's mandate to make its new tasks as per recent/upcoming</b>	<ul style="list-style-type: none"> <li><b>Involvement in Cooperation Group:</b> Support MS cooperation on drafting and maintaining over time voluntary guidelines on security measures for Operators of Essential</li> </ul>	<ul style="list-style-type: none"> <li>It is assumed that ENISA will be able to take on all new tasks assigned to it as per recent legislative changes by reallocating responsibilities and tasks, as it has been done in the 2016 and 2017 Work</li> </ul>	Human resource costs: Status quo to EUR 676,416

<sup>109</sup> Taking into account that the costs for a liaison office in Brussels would only have to be added once.

<sup>110</sup> Taking into account that the costs for a liaison office in Brussels would only have to be added once.

<sup>111</sup> Taking into account that the costs for a liaison office in Brussels would only have to be added once.

Options	Factors of change	Assumptions	Estimated costs/year
<p><b>legislation more specific</b></p>	<p>Services, Incident Reporting, Identification of Essential Operators and Essential Service</p> <ul style="list-style-type: none"> <li> <p><b>CSIRT Network Secretariat:</b> Provide technical support for back-end services that enable CSIRTs to exchange information on best practices and actual incidents and threats, as well as support voluntary cooperation in case of incidents</p> </li> <li> <p><b>Electronic communications code, recital 92:</b> Contribute to an enhanced level of security of electronic communications by, amongst other things, providing expertise and advice, and promoting the exchange of best practices</p> </li> <li> <p><b>eIDAS:</b> (1) Recital 39 - Enable the EC and MSs to assess the effectiveness of the breach notification mechanism introduced by this Regulation by, for example, aggregating the national reports provided by supervisory bodies into an annual Report on EU Breaches in Trust Service Providers. (2) Support supervisory authorities in the drafting and supervision of security measures of Trust Services through, for example, supporting national regulators in the drafting and maintenance of guidelines on security measures and incident notification formats and procedures on Trust Services</p> </li> </ul>	<p>Programme.</p> <ul style="list-style-type: none"> <li>Should this not be possible, ENISA could get another eight staff members (two for each of the key sectors finance, health, transport and energy) to respond to its new responsibilities. This represents eight FTEs at senior expert/analyst level (AD 7 to 12 grade).</li> </ul>	
<p><b>TOTAL COST OF OPTION 0</b></p>		<p>Assuming that all factors of change are being implemented</p>	<p>Current budget: EUR 11,244,679                      Additional human resources costs: EUR 0 to EUR 676,416                      Other additional costs: EUR 0                      TOTAL: EUR 11,244,679 to 11,921,095</p>

Options	Factors of change	Assumptions	Estimated costs/year
<p><b>Option 1: Expiry of ENISA’s mandate (terminating ENISA): This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive and bilateral or regional ties at Member State level.</b></p>	<p>N/A</p>	<p>N/A</p>	<p><b>Cost savings:</b> The direct costs for the EU budget of not extending the mandate of ENISA in 2020 would be EUR 0, which implies thus a cost saving for the European institutions<sup>112</sup> of approximately EUR 10,332,000<sup>113</sup> yearly, plus a 2% standard increase per year.</p> <p><i>Note that abstraction is made of any possible cost of e.g. re-allocating staff and the removal of infrastructure and all miscellaneous administrative requirements for ending ENISA’s activities.</i></p>
<p><b>Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate):</b> This option concerns making significant revisions to ENISA’s mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.</p>	<p><b>Provide periodic threat intelligence and ad hoc alerts:</b> ENISA would develop and maintain its own threat intelligence capacity in order to monitor the threat landscape and provide MSs fast alerts/warnings on emerging threats and risks and monitor security incidents, including those affecting specific MSs. This would involve: (1) producing regular threat intelligence reports including high-level strategic analyses on threats, incidents and trends (e.g. key technological developments) and (2) collecting and analysing public communications on an event and compiling EU-level flash reports and guidance to</p>	<p>• Would need analysis capability and need to source the information which would require a kind of security operation centre (SOC) receiving feed or threat data which could come through individual CSIRTs. Would have automated tools to interpret what that data is saying and then a team of analysts to transcribe what the tools are saying into something that makes sense.</p> <p>• ENISA have the staff necessary to conduct the preparatory analysis, but do not have anyone to conduct the technical, short-term, quick analysis</p> <p>• For the periodic threat intelligence: 6 to 8 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to engage and interpret the data and provide high level situational reports and a mix of</p>	<p><b>Human resource costs:</b> EUR 531,000 to EUR 700,104 / year</p>
<p><b>Strengthen ENISA’s operational role</b></p>	<p>• <b>Provide periodic threat intelligence and ad hoc alerts:</b> ENISA would develop and maintain its own threat intelligence capacity in order to monitor the threat landscape and provide MSs fast alerts/warnings on emerging threats and risks and monitor security incidents, including those affecting specific MSs. This would involve: (1) producing regular threat intelligence reports including high-level strategic analyses on threats, incidents and trends (e.g. key technological developments) and (2) collecting and analysing public communications on an event and compiling EU-level flash reports and guidance to</p>	<p>• Would need analysis capability and need to source the information which would require a kind of security operation centre (SOC) receiving feed or threat data which could come through individual CSIRTs. Would have automated tools to interpret what that data is saying and then a team of analysts to transcribe what the tools are saying into something that makes sense.</p> <p>• ENISA have the staff necessary to conduct the preparatory analysis, but do not have anyone to conduct the technical, short-term, quick analysis</p> <p>• For the periodic threat intelligence: 6 to 8 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to engage and interpret the data and provide high level situational reports and a mix of</p>	<p><b>Human resource costs:</b> EUR 531,000 to EUR 700,104 / year</p>

<sup>112</sup> The financing provided by the Government of the Hellenic Republic (which constitutes between 6 and 7% each year), as well as contributions from third countries participating in the work of the Agency (around 1%) has been deducted from this estimate.

<sup>113</sup> Share of ENISA’s budget in 2017 representing a subsidy from the EU budget.

Options	Factors of change	Assumptions	Estimated costs/year
	<p>businesses and citizens.</p>	<p>IT players that understand the tools, senior subject experts/analysts (AD 7 to 12 grade) to interpret the data and with a multi-stakeholder experience (i.e. relations and links to industry, CSIRTs, EC3 etc.)</p> <ul style="list-style-type: none"> <li>For the ad hoc alerts: 0.5 FTEs among the 6 to 8 FTEs (TAs) senior subject experts/analysts (AD 7 to 12 grade) above to focus on this and be able to scale when an incident takes place as will be on demand</li> <li><i>Note: An additional cost that could be incurred is derived from ENISA acquiring feed or threat data for a fee, but here it has been assumed that data would be channelled to it by CSIRTs</i></li> </ul>	
	<ul style="list-style-type: none"> <li><b>Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level:</b> ENISA would: (1) organise cybersecurity exercises to test the Blueprint at all levels – operational, tactical and strategic) with all stakeholders; (2) collect and aggregate reports from national sources (CSIRTs) to establish a common situation awareness report for decision makers in the event of an incident; (3) support technical handling of the incident, including facilitating sharing of technical solutions between MSs; (4) handle public communication around the incident; (5) in case of a major crisis, propose the activation of the political decision making (IPCR) by alerting all or one of the EU institutions; (6) publish flash report or alerts in the event of significant events or incidents based on publicly available information OR information made available through the CSIRT Network</li> </ul>	<ul style="list-style-type: none"> <li>Would go hand in hand with the “Provide periodic threat intelligence and ad hoc alerts” change above for points 2 and 6 in particular, so synergies in the team could be exploited if both changes are implemented</li> <li>Synergies could be exploited here with the communications team should this change be implemented</li> <li>The organisation of cyber exercises would be scaled up by 50%: Would look at incident from beginning to end, involve a variety of stakeholders and would be carried out yearly (rather than every 2 years)</li> <li>6 to 8 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to engage and interpret the data and provide high level situational reports, as well as bridging the operational and strategic levels, being responsible for escalation and facilitation in a crisis situation; a communications professional with an understanding of cybersecurity to manage the press and support the Head of Unit; and a mix of IT players that understand the tools, senior subject experts/analysts (AD 7 to 12 grade) to interpret the data and with a multi-stakeholder experience (i.e. relations and links to industry, CSIRTs, EC3 etc.)</li> <li>0.5 FTEs among the 6 to 8 FTEs (TAs) senior subject experts/analysts (AD 7 to 12 grade) above</li> </ul>	<p>Human resource costs: EUR 531,000 to EUR 700,104 / year</p> <p><u>Organisation of exercise costs<sup>114</sup>:</u> EUR 926,142 / year</p>

<sup>114</sup> Based on the cost of the 2016 exercise which amounted to EUR 617,428. See ENISA Annual Activity Report 2015. <https://www.enisa.europa.eu/publications/corporate/enisa-annual-activity-report-2015>

Options	Factors of change	Assumptions	Estimated costs/year
	<ul style="list-style-type: none"> <li><b>Provide emergency cybersecurity response:</b> ENISA would provide on-demand technical assistance to MS bodies and institutions by creating and maintaining a team of experienced senior cybersecurity incident advisors who may be sent to MSs upon their request to assist and contribute to cybersecurity incident response and recovery</li> </ul>	<p>to be able to scale up and support the technical handling of an incident when an incident takes place as will be on demand</p> <ul style="list-style-type: none"> <li><i>Note: An additional cost that could be considered and for which external funding could be sought is the updating of the platform used for these exercises – here it has been assumed that the existing platform will be employed</i></li> <li>Would be on-demand, so difficult to estimate the exact need, but synergies in the team “supporting the Blueprint for response to large scale cybersecurity incidents and crises at EU level” and the before and after incident response capability to be developed as part of this could be exploited</li> <li>15% of 4 FTEs (TAs) among the 6 to 8 FTEs (TAs) senior subject experts/analysts (AD 7 to 12 grade) above working on “Providing periodic threat intelligence and ad hoc alerts” and “Supporting the Blueprint for response to large scale cybersecurity incidents and crises at EU level” with experience in dealing with events in real time and advising, as well as contacts in the CERTs who could be called upon in the event of an incident</li> </ul>	<p>Human resource costs: EUR 50,731 / year</p>
<p><b>Strengthen ENISA’s role in policy development and implementation</b></p>	<ul style="list-style-type: none"> <li>Establish ENISA as an agency that has to be involved by other EU bodies, including the Commission, when cybersecurity matters are being considered</li> <li>Formally involve ENISA in the implementation of the Connecting Europe Facility on Telecoms as an advisory body</li> <li>Establish semi-formal governance structures with regular meetings between ENISA and other agencies/international organisations (e.g. on given common themes such as training) to increase cooperation at EU institutional level</li> <li>Set-up a liaison office in Brussels with two to three permanent employees</li> </ul>	<ul style="list-style-type: none"> <li>Would involve ENISA taking a more proactive approach where it would actively follow policy and play the role of a strong coordination body in this respect</li> <li>Ideally, would need to have 2 FTEs per sector (i.e. energy, transport (aviation/vehicles), health, finance) to avoid a single point of failure</li> <li>9 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior sector-specific experts/analysts (AD 7 to 12 grade)</li> <li>Estimated 15 meetings per month with travel and per diems for 1.5 staff/meeting on average – (where other than Brussels-based staff)</li> <li>2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to talk to MEPs, senior officials and go to meetings at short notice and senior experts/analysts (AD 7 to 12 grade) to follow through and execute what has been decided</li> <li>Office space rental in Brussels at a cost of EUR 300</li> </ul>	<p>Human resource costs: EUR 784,656 / year</p> <p>Meeting costs<sup>115</sup>: EUR 175, 320 / year</p> <p>Human resource costs: EUR 243,125.75 to 349,753 EUR / year</p> <p>Office space rental: EUR 7,500 / year</p>

<sup>115</sup> Return trip estimated at EUR 500 and per diems at EUR 224 on the basis of an average of EuropeAid per diem rates for Europe – see [https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17\\_en.pdf](https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17_en.pdf)

Options	Factors of change	Assumptions	Estimated costs/year
	<ul style="list-style-type: none"> <li>Create a dedicated communications team within ENISA</li> </ul>	<ul style="list-style-type: none"> <li>/square meter<sup>116</sup> and a need for an estimated office space of 25 square meters for 2 to 3 people</li> <li>2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) with experience in communications at different levels and understanding of cyber security and junior communications experts/analysts (AD 5 to 6 grade) to assist the Head of Unit</li> <li>Would simply involve a revision of the mandate</li> </ul>	<p><u>Human resource costs:</u> EUR 112,454 to 116,668 / year</p>
<b>Make ENISA’s mandate permanent</b>	<ul style="list-style-type: none"> <li>This would involve ENISA having a permanent mandate, but still allow for the periodic evaluation of the performance of the Agency</li> </ul>	<ul style="list-style-type: none"> <li>Would simply involve a revision of the mandate</li> </ul>	N/A
<b>Strengthen ENISA’s governance structure</b>	<ul style="list-style-type: none"> <li>Formally involve other stakeholders in the governance of ENISA by increasing the weight of the PSG in playing an advisory role on ENISA’s Work Programme</li> <li>Allow more flexibility for ENISA to determine its own work priorities at Executive Board level</li> </ul>	<ul style="list-style-type: none"> <li>Would simply involve a revision of the mandate</li> <li>Would simply involve a revision of the mandate</li> </ul>	N/A
<b>Include a role for ENISA in EU-level standardisation and certification</b>	<ul style="list-style-type: none"> <li><b>Support the EU ICT Security Certification Framework:</b> Put in place an EU ICT security certification framework whereby ENISA would play a supporting role by (1) assisting the Commission in carrying out secretarial tasks and actively supporting the work undertaken (e.g. convene meetings of the framework’s governance structures and meetings and engagements with industry stakeholders);(2) providing technical expertise to Member States (e.g. MS taking part in the framework on issues related to security testing and vulnerabilities in ICT products); and (3) compiling and publishing guidelines concerning the security requirements of ICT products and services in cooperation with national authorities and industry, thereby communicating the work of the framework to industry, consumers at EU and international level</li> <li><b>Support ICT security standardisation:</b></li> </ul>	<ul style="list-style-type: none"> <li>Synergies could be exploited here with the team set-up to strengthen ENISA’s role in policy development and implementation should this change be implemented</li> <li>4 to 6 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) including a mix of sector-specific experts and experts in certification (preferably with experience of industry or a good understanding of it), as well as multi-stakeholder expertise and an understanding of policy</li> <li>Estimated 3 to 5 meetings/events per month with travel and per diems for 1.5 staff/meeting on average – (where other than Brussels-based staff)</li> </ul>	<p><u>Human resource costs:</u> EUR 361,896 to 531,000 EUR / year</p> <p><u>Attendance at event/ meeting costs<sup>117</sup>:</u> EUR 28,002 to 58,440 / year</p>

<sup>116</sup> Source: Rental prices of prime office properties in selected European cities as of 4th quarter 2016 (in euros per square meter per year). The Statistics Portal. <https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/>

<sup>117</sup> Return trip estimated at EUR 500 and per diems at EUR 224 on the basis of an average of EuropeAid per diem rates for Europe – see [https://ec.europa.eu/europeaid/sites/devco/files/devco-files/perdiems-2017-03-17\\_en.pdf](https://ec.europa.eu/europeaid/sites/devco/files/devco-files/perdiems-2017-03-17_en.pdf)

Options	Factors of change	Assumptions	Estimated costs/year
<p><b>Strengthen ENISA's position relative to research and innovation</b></p>	<p>ENISA would provide a supportive role in facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services, including by cooperating with Member States on technical areas concerning the security requirements for operators of essential services and digital service providers. This could involve supporting the work of the EU ICT Security Certification Framework in EU and international standard organisations; taking part in and contributing to the work of cybersecurity working groups of the European Standardisation Organisations (ESCs); performing reviews and assessments of cybersecurity related standards when associated with regulatory and legal requirements (e.g. eIDAS)</p> <ul style="list-style-type: none"> <li>• <b>Take part in programming implementation:</b> ENISA would implement parts of the Framework Programme for R&amp;I which relates to cybersecurity whereby the EC delegates the relevant powers by performing the following tasks: (1) managing some stages of then programme implementation and some phases in the lifetime of specific projects on the basis of WPs adopted by the EC; (2) adopting the instruments of budget execution for revenue and expenditure and carrying out all the operations necessary for the management of the programme; and (3) providing support in programme implementation. Examples of the activities ENISA could perform include implementing calls on Public Procurement of Innovation (PPI) in close collaboration with MS authorities, and support MS public procurers in identifying common research and innovation requirements.</li> </ul>	<p>ICT Security Certification Framework“ change above as the issues are related and there would be a need to avoid silos, so synergies in the team could be exploited if both changes are implemented in order to avoid single points of failure</p> <ul style="list-style-type: none"> <li>• 4 to 6 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) including a mix of sector-specific experts and experts in standardisation/certification (preferably with experience of industry or a good understanding of it), as well as multi-stakeholder expertise and an understanding of policy</li> <li>• 0.5 FTEs among the 4 to 6 FTEs (TAs) above to be used for the stock taking, compiling and reviewing of standards</li> </ul>	<p>EUR 361,896 to 531,000 EUR / year</p>
		<ul style="list-style-type: none"> <li>• ENISA would perform a similar function with respect to R&amp;I to that foreseen as part of the new Frontex Regulation<sup>118</sup></li> </ul>	<p>Estimated costs based on similar function foreseen for Frontex: EUR 3.5m / year</p>

<sup>118</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC, COM(2015) 671 final. See SPECIFIC OBJECTIVE NO 6 "Management of Pooled resources and R&D. [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation\\_on\\_the\\_european\\_border\\_and\\_coast\\_guard\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation_on_the_european_border_and_coast_guard_en.pdf)

Options	Factors of change	Assumptions	Estimated costs/year
	<ul style="list-style-type: none"> <li><b>Take part in programming through playing an advisory role:</b> ENISA would play an expert advisory role in the cyber security-related elements of EU R&amp;D funding programmes (H2020, CEF) by sitting on an advisory committee, providing independent advice and input and feeding into ideas for research.</li> </ul>	<ul style="list-style-type: none"> <li>Synergies could be exploited here with the team set-up to strengthen ENISA's role in policy development and implementation should this change be implemented</li> <li>Advisors would need to draw on the knowledge of sector experts/analysts for input</li> <li>2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade)</li> <li>Estimated 2 to 3 meetings per month with travel and per diems for 1.5 staff/meeting on average – (where other than Brussels-based staff)</li> </ul>	<p><u>Human resource costs:</u> EUR 192,792 to 277,344 EUR / year</p> <p><u>Meeting costs:</u> EUR 23,373 to 35,064 /year</p>
	<ul style="list-style-type: none"> <li><b>Benefit from EU R&amp;I funding:</b> Open ENISA's mandate to take part in EU R&amp;D funding programmes (H2020, CEF) as a recipient of funding by changing the provisions on source of revenue but not adding it as a task. ENISA can provide added value to industry and academia in R&amp;I by leveraging its practical expertise in areas such as cooperation, information sharing and regulatory requirements.</li> </ul>	<ul style="list-style-type: none"> <li>Would simply involve a revision of the mandate</li> </ul>	<p>N/A</p>
<b>TOTAL COST OF OPTION 2</b>			
<p>Assuming that all factors of change are being implemented</p> <p>There are different factors of change to strengthen ENISA's position relative to research and innovation which exclude one another due to issues of conflict of interest. Sub-option a) represents the costs for the factor of change under which ENISA will take part in programme implementation of the Framework Programme for R&amp;I. Sub-option b) includes the costs of ENISA taking part in programming through playing an advisory role in EU R&amp;D funding. Sub-option c) includes the costs of ENISA benefitting from EU R&amp;I funding (which are nil).</p>			
<p>Current budget: EUR 11,244,679</p> <p>Additional human resources costs:</p> <p>a) EUR 2,033,131.75 to EUR 2,482,181</p> <p>b) EUR 2,225,923.75 to EUR 2,759,525</p> <p>c) EUR 2,033,131.75 to EUR 2,482,181</p> <p>Other additional costs:</p> <p>a) EUR 4,636,964 to EUR 4,667,402</p> <p>b) EUR 1,160,337 to EUR 1,202,466</p> <p>c) EUR 1,136,964 to EUR 1,167,402</p> <p>TOTAL:</p> <p>a) EUR 17,914,774.75 to EUR</p>			



Options	Factors of change	Assumptions	Estimated costs/year
<p><b>Option 3: European Agency with full operational capabilities (establish a European Centre of Cybersecurity ):</b> This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.</p> <p><b>Create an EU level cyber security umbrella</b></p>	<ul style="list-style-type: none"> <li>Develop an umbrella organisation covering ENISA and CERT-EU, thereby bringing together three main functions, namely policy advice, centre for information and Computer Emergency Response Team. The operational role of CERT-EU in responding to cyber incidents in the EU institutions would therefore be combined with ENISA's role of ensuring cooperation in the event of an incident. The new organisation would act as an EU contact point for cybersecurity related issues in close coordination with the EEAS.</li> <li>Options include merging ENISA and CERT-EU and having a governance structure that would allow different reporting lines and oversight for the team dealing with the EU institutions, or integrating CERT-EU within ENISA as one of the Agency's departments.</li> </ul>	<ul style="list-style-type: none"> <li>If this option is adopted, ENISA would be in the position to "Provide periodic threat intelligence and ad hoc alerts" and "Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level" (see above – Option 2) by using a combination of ENISA and CERT EU staff.</li> <li>Most of the changes referred to above in relation to "Providing periodic threat intelligence and ad hoc alerts" and "Supporting the Blueprint for response to large scale cybersecurity incidents and crises at EU level" (see above – Option 2) would come for free (i.e. anything related to response side, e.g. flash notes, following up on incidents etc.) as CERT-EU have the capacity internally to deal with this</li> <li>Relocation of ENISA to Brussels would not be necessary, but the establishment of a liaison office would</li> </ul> <p><u>Costs linked to the establishment of a liaison office (as above):</u></p> <ul style="list-style-type: none"> <li>Synergies could be exploited here with the team set-up to strengthen ENISA's role in policy development and implementation should this change be implemented</li> <li>2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to talk to MEPs, senior officials and go to meetings at short notice and senior experts/analysts (AD 7 to 12 grade) to follow through and execute what has been decided</li> <li>Office space rental in Brussels at a cost of EUR 300 /square meter<sup>119</sup> and a need for an estimated office space of 25 square meters for 2 to 3 people</li> </ul>	<p>18,394,262</p> <p>b) EUR 14,630,939.75 to EUR 15,206,670</p> <p>c) EUR 14,414,774.75 to EUR 14,894,262</p>

<sup>119</sup> Source: Rental prices of prime office properties in selected European cities as of 4th quarter 2016 (in euros per square meter per year). The Statistics Portal. <https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/>

Options	Factors of change	Assumptions	Estimated costs/year
<p><b>Create a virtual European CSIRT</b></p>	<ul style="list-style-type: none"> <li><b>Coordinate CSIRT Network operations:</b> Enable the Agency to coordinate the operations of MS CSIRTs, collecting information and pooling national resources on analysing threats and responding to incidents</li> </ul>	<ul style="list-style-type: none"> <li><i>Note: Change management costs would be incurred but it is outside of the scope of this study to assess these</i></li> <li>ENISA would act as a facilitator as the expertise would come from the Member States themselves</li> <li>Could second people to/draft people in from Member State CSIRTs to build a virtual European CSIRT and then have an aggregation of information so what is sensitive to Member States is taken out without losing the contextual picture</li> <li>4 to 5 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) to put the infrastructure in place, and carry out the outreach with industry in Member States, through the ISACs at sectoral, with CSIRTs etc.</li> </ul>	<p>Human resource costs: EUR 361,896 to EUR 446,448 EUR / year</p>
<ul style="list-style-type: none"> <li><b>Produce real time situational awareness and dynamic (live) threat intelligence feeds:</b> Enable ENISA to act as a broker, sharing information on incidents between Member States in the form of real-time situational awareness and dynamic (live) threat intelligence feeds on the basis of information exchanged on the CSIRT Network</li> </ul>	<ul style="list-style-type: none"> <li>Would be an observatory in real time</li> <li>First there will be a need to set-up the necessary infrastructure, including the communication links across Europe with a variety of players (industry, ISACs). This would result in the establishment of a security operation centre (SOC) that would process and share the data, report to the press and conduct briefings at political level.</li> <li>Initial set-up: 10 to 15 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) to put the infrastructure in place.</li> <li>Once up and running: 5 to 6 FTEs (TAs) - including 1 Head of Unit (AD9 to AD14 grade) to engage at the right levels and across sectors, and senior (ICT) experts/analysts (AD 7 to 12 grade) to process and analyse the data real time through a roster (24/7) and in order to avoid single points of failure</li> </ul>	<ul style="list-style-type: none"> <li>Human resource costs: (1) Initial set-up: EUR 869,208 to 1.3m / year (2) Once up and running: EUR 446,448 to 531,000 EUR / year</li> </ul>	
<ul style="list-style-type: none"> <li><b>Maintain and provide own cybersecurity incident response capacity to public and private sector:</b> ENISA would create and maintain the capacity to provide on-demand technical operational assistance to MS CSIRTs, operators of essential services, EU</li> </ul>	<ul style="list-style-type: none"> <li>The scope and scale of this task could vary extensively depending on the breadth of “clients” of the service, e.g. whether SMEs or not etc.</li> <li>Initial set-up: 15 to 20 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) to put the</li> </ul>	<ul style="list-style-type: none"> <li>Human resource costs: (1) Initial set-up: EUR 1.3m to 1.7m / year (2) Once up and running:</li> </ul>	

Options	Factors of change	Assumptions	Estimated costs/year
	<p>bodies and institutions for the prevention, detection and response to incidents</p>	<p>infrastructure in place.</p> <ul style="list-style-type: none"> <li>Once up and running: 30 to 80 FTEs<sup>120</sup> (TAs) - including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade)</li> </ul>	<p>EUR 2.6m to 6.8m / year</p> <p><i>Note as a means of comparison (and while keeping in mind the differing aims of these centres) that Frontex runs a 24/7 situation centre at an average cost of EUR 3.0m / year, as per the new Frontex Regulation<sup>121</sup>.</i></p>
<b>TOTAL COST OF OPTION 3</b>		<p>Assuming that all factors of change are being implemented</p>	<p>Current budget: EUR 11,244,679</p> <p>YEAR 1</p> <p>Additional human resources costs: EUR 2,774,229.75 to EUR 3,796,201</p> <p>Other additional costs: EUR 7,500</p> <p>TOTAL: EUR 14,026,408.75 to EUR 15,048,380</p> <p>YEAR 2-5</p> <p>Additional human resources costs: EUR 3,651,469.75 to EUR 8,127,201</p> <p>Other additional costs: EUR 7,500</p> <p>TOTAL: EUR 14,903,648.75 to EUR 19,379,380</p>
<b>TOTAL COST OF OPTION 2 AND OPTION 3 COMBINED</b>		<p>Assuming that all factors of change are being implemented</p> <p>Taking into account that the costs for a liaison office in Brussels would only have to be added once</p>	<p>YEAR 1</p> <p>Option 2a and 3: EUR 31,690,557.75 to EUR 33,085,389</p> <p>Option 2b and 3: EUR 28,406,722.75 to EUR 29,897,797</p> <p>Option 2c and 3: EUR 28,190,557.75 to EUR</p>

<sup>120</sup> Based on an average of the number of FTEs employed in CERT-EU (30 FTEs) and in the larger Member State CERTs

<sup>121</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC, COM(2015) 671 final. See SPECIFIC OBJECTIVE NO 7 "EUROSUR and situational picture" [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation\\_on\\_the\\_european\\_border\\_and\\_coast\\_guard\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation_on_the_european_border_and_coast_guard_en.pdf)

Options	Factors of change	Assumptions	Estimated costs/year
			29,585,389  YEAR 2-5 Option 2a and 3: EUR 32,567,797.75 to EUR 37,416,389 Option 2b and 3: EUR 29,283,962.75 to EUR 34,228,797 Option 2c and 3: EUR 29,067,797.75 to EUR 33,916,389



**APPENDIX 1**  
**EVALUATION QUESTION MATRIX**

Table 29: Evaluation questions matrix

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
<b>EFFECTIVENESS</b>				
<b>EQ1 To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate?</b>	<p><b>Retrospective</b></p> <p>EQ2: What have been the benefits of acting at Agency level both from the operational and strategic perspective?</p> <p>EQ3: To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe? What more could be done?</p> <p>EQ4: How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders?</p> <p>*EQ5: To what extent has ENISA become an EU-wide centre of expertise and a reference point for stakeholders<sup>122</sup> in providing guidance, advice and assistance on issues related to network and information security?<sup>123</sup></p> <p>EQ6: How effectively has the Agency managed to set its work priorities?</p> <p>EQ7: How effectively does the Agency tackle important upcoming, unplanned issues deriving by demands of its constituencies and/or EU policy priorities?</p>	<p><u>Activity level indicators:</u> Number of training courses, exercises, publications (e.g. training material, toolkits, BP guides, reports, roadmaps), methodologies, workshops, conferences.</p> <p><u>Output level indicators:</u></p> <ul style="list-style-type: none"> <li>- Number of responses to Article 14 requests 2013-2016</li> <li>- Number of guidelines issued and disseminated 2013-2016</li> <li>- Number of recommendations issued and disseminated 2013-2016</li> <li>- Number and type of participants in trainings, workshops, exercises 2013-2016</li> <li>- Number of downloads of different types of publications (e.g. training material, BP guides etc.)</li> <li>- Number and type of standards established</li> </ul> <p><u>Result level indicators:</u></p> <ul style="list-style-type: none"> <li>- Stakeholders' views on the extent to which ENISA has achieved its objectives as per its mandate.</li> <li>- Degree to which stakeholders' have made use of material, followed recommendations and guidelines, copied BPs</li> <li>- Degree to which stakeholders have disseminated material, guidelines, BPs more widely</li> <li>- Overall degree of achievements of objectives – as per specific M&amp;E framework (Yearly adapted to core</li> </ul>	<p>Products (e.g. publications/papers) and services are delivered as planned.</p> <p>The activities carried out by the Agencies are shown to support the achievement of the objectives.</p> <p>70% of objectives and intended results were reached and where objectives or results were not reached this is accounted for (cross-checking KPIs and stakeholder's assessments).</p> <p>Users are satisfied with the products and services (no issue is mentioned)<sup>127</sup></p> <p>Mechanisms are in place to ensure that the</p>	<p>Data sources: Desk research – annual reports, in particular reporting on the KIIs<sup>128</sup></p> <p>Results of ENISA's follow-up activities relating to exercises, trainings, workshops, events</p> <p>Results of the evaluations of ENISA's activities of 2014 and 2015</p> <p>In-depth interviews</p> <p>Public consultation (excluding EQ11)</p>

<sup>122</sup> The stakeholders include EU institutions, Members States and the wider stakeholders community

<sup>123</sup> This question has been reformulated to ensure that it is open. The original question was: "To what extent ENISA became an EU-wide centre of expertise and a reference point for EU institutions, Members States and the wider stakeholders community, in providing guidance, advice and assistance on issues related to network and information security?"

<sup>127</sup> This judgement criterion is also expected to rely on the assessments made in relation to evaluation question related to the evaluation criterion relevance.

<sup>128</sup> Please note that, as concluded in the evaluation of ENISA's 2015 core operational activities, while some KIIs are situated at the impact level and data has been collected in relation to them, it was found that it was too early to report on many of the indicators. An additional challenge is that the KIIs change on an annual basis, making it difficult to monitor results on a year-on-year basis as there is no requirement to do so. Some of the indicators are situated at the output/result levels and will be used to report in relation to the indicators set out in this matrix.

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	<p>EQ8: Does the Agency consistently perform the same tasks with the same quality level over time?</p> <p>EQ9: How does ENISA compare to the other EU and national bodies offering similar services in relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency?</p> <p>*EQ11: How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to effectiveness in the work of the agency?<sup>124</sup></p> <p>EQ12: How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate?</p> <p>EQ13: What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives?</p> <p>*EQ19: To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc.)?<sup>125</sup></p> <p>*EQ20: To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?<sup>126</sup></p>	<p>operational activities)</p> <p><b>Impact level indicators:</b></p> <ul style="list-style-type: none"> <li>- Stakeholders' perceptions on the extent to which ENISA contributed to the overall EU goal of increasing network and information security in Europe, and what more could be done.</li> </ul> <p>Degree to which there are internal/external factors to ENISA which influence / restrict progress</p> <p><b>Other indicators:</b></p> <ul style="list-style-type: none"> <li>Mapping of the Agencies' structured quality management processes (gathering and analysing feedback from users).</li> <li>Mapping the process of developing multi-annual work programmes.</li> <li>Evidence of adjustments to annual work programmes, justified by policy, political or economic changes.</li> <li>Stakeholders' assessment of the Agencies' ability to adapt to policy, political or economic changes.</li> <li>Expert assessment of whether evaluation/monitoring requirements and practices are adequate compared to the Better Regulation Guidelines.</li> <li>A comparison of make or buy between similar agencies, e.g. procurement/operational budget.</li> <li>Mapping of how make or buy (or a hybrid form) decisions have been made.</li> </ul>	<p>products (e.g. publications/papers) and services developed continuously meet the needs of the users.</p> <p>It can be documented that ENISA's products and services are used by a wide range of national and European stakeholders.</p>	<p>Survey of ENISA staff (only for EQ11)</p>

<sup>124</sup> This question has been reformulated by removing a reference to "efficiency", which will be covered by EQ14 and its sub-questions. The original question was: "How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to efficiencies and effectiveness in the work of the agency?"

<sup>125</sup> This question was originally (in the Roadmap) included under efficiency, but is better suited under effectiveness.

<sup>126</sup> This question was originally (in the Roadmap) included under efficiency, but is better suited under effectiveness.



Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
<p><b>Prospective</b></p> <p>*EQ37: How does the new policy and regulatory landscape, having regard to the recently adopted Network and Information Security Directive and COM(2016) 410, and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?<sup>129</sup></p> <p>*EQ38: What are the main strengths and weaknesses of ENISA in taking up new challenges, considering its current mandate and organisational set-up and capacity?<sup>130</sup></p> <p>*EQ39: If ENISA should take on any new challenges and tasks, would a fixed-term mandate be suitable?<sup>131</sup></p> <p>EQ41: Which are the concrete needs and opportunities for cooperation and synergies with international bodies working in adjacent fields, like the NATO Cooperative Cyber Defence Centre of Excellence?</p>	<p>Findings from the research done for EQ1-9, EQ11-13, EQ19 and EQ20.</p> <p>Stakeholders' assessment of the Agency's mandate main strength(s) and weakness(es) in view of taking up new challenges.</p> <p>Stakeholders' assessment of the Agency's organisational set-up and capacity main strength(s) and weakness(es) in view of taking up new challenges.</p> <p>Stakeholders' assessment of the optimal type of mandate.</p> <p>Expert assessment of the optimal type of mandate.</p>	<p>Since the prospective EQs are explorative it is not recommendable to define judgement criteria (as there is no justified basis).</p>	<p>Data sources: Public consultation and in-depth interviews</p>	
<b>EFFECIENCY</b>				
<p><b>EQ14: To what extent has ENISA been efficient in implementing the mandate as laid down in its Regulation? To assess this</b></p>	<p><b>Retrospective</b></p> <p>*EQ15: Were the annual budgets of the Agency implemented in an efficient way considering the results achieved?<sup>132</sup></p> <p>EQ16: Have the resources allocated to the Agency been sufficient for the pursuit of its tasks (input/output analysis)?</p>	<p>Tracking of cost/resources used per deliverable Cost per download for reports</p> <p>Cost saving measures are in place</p> <p>% of staff positions filled (on an annual basis)</p> <p>% of staff members working on core operations.</p>	<p>Stable costs, and decreases/increases can be justified</p> <p>Continuous work/processes in place to save costs in the operations</p>	<p>Data sources: AARs, Governing Boards analysis and assessment of the AARs, in-depth interviews</p>

<sup>129</sup> This question has been revised based on comments from the Commission. It was originally (in the Roadmap) "How does the new policy and regulatory landscape, having regard to the recently adopted Network and Information Security Directive, in COM(2016) 410, and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?"

<sup>130</sup> This question has been re-worded to improve clarity. The original question was: "What are the main strengths and weaknesses of ENISA, within its current mandate and organisational set-up and capacity, in taking up new challenges?"

<sup>131</sup> This question has been re-worded to improve clarity. The original question was: "Is a fixed-term mandate coherent with the new challenges and tasks ENISA will have to take on?"

<sup>132</sup> This question has been re-worded to improve clarity. The original question was "Were the annual budgets of the Agency implemented in an efficient way with a view on achieved results?"

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
<p><b>question, elements relating to internal structure, operation, programming of activities and resources, accountability and controls, etc. will be analysed.</b></p>	<p>*EQ17: To what extent are the organisational solutions and procedures of ENISA adapted to the work entrusted to it and to the actual workload?<sup>133</sup></p> <p>Is the planning cycle of the agency (work programme and budget) in line with the objective of achieving efficient results?</p> <p>EQ18: To what extent have ENISA's governance, organisational structure, locations and operations as set in its Regulation and the arrangements related to the location of its offices been conducive to efficiency and to achieving economies of scale?</p> <p>EQ21: To what extent and how have external factors influenced the efficiency of ENISA?</p> <p><i>*Please note that EQ19 and EQ20 were originally (in the Roadmap) included under efficiency, but have here been organised under effectiveness as this is more appropriate.</i></p>	<p>Agencies' managerial staff assessment of flexibility in adjusting staff composition</p> <p>Share of budget allocated to administrative tasks</p> <p>Existence of own implementation rules (approved by the Commission)</p> <p>Prevalence of use of external expertise</p> <p>% of publications and similar deliverables where dissemination/ communication was successful</p> <p>Number of studies procured vs. number of studies produced in-house", including relative to other comparable organisations</p> <p>Typologies of what triggers procurement decisions (need for expertise, resource constraints or other) , including relative to other comparable organisations</p> <p>Drivers and inhibitors in the budgeting process.</p> <p>Usage of permanent stakeholder groups/bureaus or similar<sup>134</sup> and use of advisory committees/working groups or similar.</p> <p>Development in location costs during the period (compared to a 2009 baseline).</p> <p>% of agency staff and management which assess that the Headquarters Agreement is fulfilled.</p> <p>Host member states assessment of the extent to which the Headquarters Agreement is fulfilled</p> <p>Positive/negative assessments from the respective Governing Boards of the AARs.</p>	<p>Follow-up measures in place</p> <p>Evidence of efficient management of the resources available with improvements in the balance between operational budgets and administrative budgets achieved where necessary (based on previous evaluations, audits or similar).</p> <p>Evidence can be provided on how current organisation allows for optimal use of capabilities and resources:</p> <ul style="list-style-type: none"> <li>•Division of work and resources are appropriate</li> <li>•Shared resources are available</li> <li>•Cooperation is encouraged facilitated</li> </ul> <p>No organisational obstacles are encountered in the delivery of products and services</p> <p>The internal organisational structure for the delivery of products and services allow for the most</p>	

<sup>133</sup> This question has been re-worded to improve clarity. The original question was "To what extent are the organisational solutions and procedures of ENISA adequate to the work entrusted to it and to the actual workload?"

<sup>134</sup> Several EU decentralised Agencies have established such groups in order to consult/engage/involve stakeholders in the Agencies work, for example annual work programme's priorities.

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	<p><b>Prospective</b></p> <p>*EQ42: Could ENISA’s mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape or would another EU initiative be more efficient?<sup>135</sup></p> <p>EQ43: What would be the financial implications associated with each of the possible options for modifying ENISA’s mandate as they emerge from the evaluation?</p>	<p>Findings from EQ14-18, and EQ21 as well as EQ 36.</p>	<p>optimal use of capabilities and resources:</p> <ul style="list-style-type: none"> <li>• no gap is identified</li> <li>• no redundancy is found</li> </ul> <p>Since the prospective EQs are explorative it is not recommendable to define judgement criteria (as there is no justified basis).</p>	<p>Data sources:</p> <p>Public consultation (only for EQ42)</p>
<b>RELEVANCE</b>				
<p><b>EQ33: Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework and needs?</b></p>	<p><b>Retrospective</b></p> <p>EQ29: How far are the Agency’s tasks and resources aligned with key EU political priorities?</p> <p>EQ30: Which Agency tasks are absolutely essential to deliver on these priorities?</p> <p>EQ31: Which Agency tasks are necessary to continue implementing existing and evolving obligations under the Treaties and EU legislative framework?</p> <p>EQ32: Are there some Agency tasks that have become redundant / negative priorities? If so, which are they?</p> <p>EQ34: Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?</p>	<p>Mapping of structured quality management processes (gathering and analysing feedback from users).</p> <p>% of KPIs related to uptake of the Agencies expertise in policy documents or by industry.</p> <p>% of KPIs related to the Agencies contribution to policy development through events.</p> <p>Users’ assessment of the extent to which the agency fulfils current needs.</p> <p>Estimate of media-coverage of the Agency (which reaches a broader audience)</p> <p>New stakeholders are engaged when appropriate (e.g. new sign-ups for newsletters, new consultations or similar).</p>	<p>Mechanisms are in place to ensure that the products and services developed continuously meet the needs of the users.</p> <p>All existing products and services provided by the Agencies’ correspond to current needs (no issues are mentioned)</p> <p>All current needs are fulfilled (no gaps are identified)</p>	<p>Data sources:</p> <p>Public Consultation, in-depth interviews, staff survey (only for EQ34)</p>
<p><b>Prospective</b></p>		<p>Findings from EQ29-EQ34.</p>	<p>Since the prospective EQs are explorative it is</p>	<p>Data sources:</p> <p>Public</p>

<sup>135</sup> This question has been revised based on comments from the Commission to the inception report. The original question (from the Roadmap) was: “How could ENISA’s mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape?”

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	<p>*EQ36: Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent is ENISA best placed to respond to these needs? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?<sup>136</sup></p> <p>EQ40: Which are the concrete needs and opportunities for further increased practical cooperation with Member States and EU bodies?</p>	<p>Stakeholders assessment of needs which are not addressed, weighed against the relevance of ENISA providing them.</p>	<p><i>not recommendable to define judgement criteria (as there is no justified basis).</i></p>	<p>consultation</p>
<b>COHERENCE</b>				
<p><b>*EQ24: To what extent are ENISA activities coherent with the policies, strategy documents and activities of other stakeholders?</b><sup>137</sup></p>	<p><b>Retrospective</b></p> <p>EQ22: To what extent is ENISA acting in cooperation with the <i>European Commission and other EU bodies</i>, to ensure complementarity and avoid duplication of efforts?</p> <p>EQ23: To what extent is ENISA acting in cooperation with the <i>Member States</i> to ensure complementarity and avoid duplication of efforts?</p> <p>EQ25: Are the procedures put in place effective to ensure that ENISA's cooperation activities are coherent with the policies and activities of its stakeholders?</p> <p>EQ26: What are the risks/sources of overlaps/conflict of interests?</p> <p><b>Prospective</b></p> <p>*EQ45: Taking into account the new tasks (identified during the evaluation), will there be any risk of ENISA's tasks and activities overlapping with those of other national, European or international bodies working?</p>	<p>Comparison of the ENISA's mandate, objectives and activities to comparable organisations/bodies, including potential overlap between stakeholders/users</p> <p>Number of joint workshops and deliverables between ENISA and cooperation partners.</p> <p>Identification of areas in which ENISA cooperates closely with other EU, national or international bodies.</p> <p>Mapping of coordination mechanisms in place between the Agencies.</p> <p>Stakeholders' assessment of whether there is coherence between ENISA and other policies and activities of its stakeholders.</p> <p>Findings from EQ22-26, and EQ29-34, and EQ36</p>	<p>The mandates, objectives and activities of the ENISA are:</p> <ul style="list-style-type: none"> <li>complementary to the work carried out by national/European/international stakeholders (do not duplicate)</li> </ul> <p>Sources of complementarity and synergy are systematically utilised</p>	<p>Data sources: Public Consultation, in-depth interviews</p>

<sup>136</sup> This question has been reformulated based on comments from the Commission. The original question was: "Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?" Please note that the evaluator considers this question key in assessing upcoming and future needs.

<sup>137</sup> This question has been reformulated for clarity and comprehensiveness. The original question was: "To what extent are ENISA activities coherent with the strategy documents adopted in this policy field?"

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
<p><b>EU ADDED VALUE</b>  <b>EQ27: What would be the most likely consequences at the EU level of stopping ENISA?</b></p>	<p><i>Please note that findings related to EQ29-34 will also be relevant to answer this question (EQ41).</i></p> <p><b>Retrospective</b>                      *EQ10: To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements?<sup>138</sup>                      EQ45: What has been the added value of having an EU cybersecurity agency such as ENISA over the period 2013-2016?<sup>139</sup></p>	<p>Extent to which stakeholders' assess that the Agency has strengthened existing EU or national initiatives (volume effects)</p> <p>Extent to which stakeholders' assess that the Agency has carried out new initiatives (initiatives not part of existing EU or national initiatives, such as new areas of research or training) (scope effects)</p> <p>Share of stakeholders/Member States which consider that actions could not have been carried out without the support of the Agencies (including examples of innovative actions) (potential scope or role effect).</p> <p>Share of stakeholders/Member States which report additional benefits derived from the products or services (comparison with baselines from previous evaluations where possible) (potential role or process effects).</p> <p>Comparison of the Agencies ability to deliver results (derived from EQ1 above) to the upcoming multi-annual programmes.</p> <p>Stakeholders assessment of other similar organisations ability to deliver the needed results.</p>	<p>EU added value is identified and acknowledged</p>	<p>Data sources:                      Desk research, in-depth interview</p>
<p><b>Prospective</b>                      EQ28: How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place?                      EQ35: What would be the most likely consequences at the EU level of stopping ENISA's activities?</p>		<p>Cross-checking of whether the new challenges and tasks fit within the EU added value identified or not identified in the findings for EQ10, EQ27-28, and EQ35.</p>	<p>Since the prospective EQs are explorative it is not recommendable to define judgement criteria (as there is no justified basis).</p>	<p>Data sources:                      Interviews and Public consultation</p>

<sup>138</sup> This question has been added by the evaluator.

<sup>139</sup> This question has been added by the evaluator based on comments received from the Commission to the Interim Report. It was not presented in the Roadmap for the evaluation of ENISA.

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	<p>*EQ44: If any new tasks for ENISA are identified (e.g. through EQ4 and EQ37), do these represent EU added value?<sup>140</sup></p>			

---

<sup>140</sup> This question has been added by the evaluator.

## **APPENDIX 2**

### **BIBLIOGRAPHY**

## 1. LEGAL SOURCES

Directive 2009/136/EC of the European Parliament and of the Council, of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation(EC) No 460/2004

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

## 2. POLICY DOCUMENTS

Commission Staff Working Document. Executive Summary of the Impact Assessment accompanying the document 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union'; SWD (2013) 31 final

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for A European Policy Approach; COM/2001/0298 final

Communication from the Commission: Europe 2020: A strategy for smart, sustainable and inclusive growth; COM (2010) 2020 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions regarding 'A Digital Single Market Strategy for Europe'; COM (2015) 192 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry; COM (2016) 410 final

Council of the European Union (2014): Information note - Recommendations by the inter-institutional Steering Board of the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) on the future mandate, governance, organisational setup, staffing and funding of CERT-EU. Brussels, 9 September 2014 – document number 12992/14

Council of the European Union (2015): Information note - CERT-EU mandate, service catalogue and information sharing and exchange framework. 3 March 2015 – document number 6738/15



European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA); SEC(2010) 1126

European Commission, DG CNECT – H1, Evaluation Roadmap for the Evaluation of the European Union Agency for Network and Information Security (ENISA), 25/07/2016. Available at: [https://ec.europa.eu/info/law/law-making-process/better-regulation-why-and-how\\_en](https://ec.europa.eu/info/law/law-making-process/better-regulation-why-and-how_en). Accessed 16 May 2017

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'; JOIN (2013) 1 final

Study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: 'Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses'. Study for the LIBE Committee. September 2015. Available at: [www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL\\_STU\(2015\)536470\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf). Accessed 16 May 2017

### 3. ENISA'S PUBLICATIONS, PROGRAMMING AND REPORTING DOCUMENTS

ENISA (2013): National-level Risk Assessments – An analysis report. ISBN: 978-92-9204-073-4; DOI: 10.2824/2633.

ENISA (2014): Annual Report 2013; ISBN: 978-92-9204-08; DOI: 10.2824/31416

ENISA (2015): Annual Activity Report 2014; ISBN: 978-92-9204-124-3; DOI: 10.2824/521040.

ENISA (2015): CYBER 7: Seven messages to the edge of Cyber-Space; ISBN: 978-92-9204-133-5; DOI: 10.2824/850678.

ENISA (2015): Threat Landscape and Good Practice Guide for Software Defines Networks/ 5G; ISBN: 978-92-9204-161-8; DOI: 10.2824/67261.

ENISA (2016): Annual Activity Report 2015; ISBN: 978-92-9204-167-0; DOI: 10.2824/698162

ENISA (2016): ENISA Strategy 2016-2020; ISBN: 978-92-9204-170-0; DOI: 10.2824/17857.

ENISA (2016): Events - 5<sup>th</sup> ENISA/EC3 Workshop. Available at: <https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop>. Accessed 30 May 2017

ENISA (2017): Privacy and Security in Personal Data Clouds – Final Report. ISBN: 978-92-9204-182-3; DOI: 10.2824/24216

Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings. Available at: [https://europa.eu/european-union/sites/europa.eu/files/docs/body/agency\\_level\\_findings\\_en.pdf](https://europa.eu/european-union/sites/europa.eu/files/docs/body/agency_level_findings_en.pdf). Accessed 30 May 2017

Ramboll Management Consulting (2015) External Evaluation of ENISA, focussing on ENISA's 2014 activities.

Ramboll Management Consulting (2016) External Evaluation of ENISA, focussing on ENISA’s 2015 activities.

## 4. ACADEMIC LITERATURE

Bendiek, A. (2012). ‘European Cyber Security Policy’, SWP Research Paper No13. Available at: [www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html). Accessed 16 May 2017

Carrapico, H., and Barrinha, A. (2017). ‘The EU as a Coherent (Cyber)Security Actor?’, JCMS: Journal of Common Market Studies, DOI: 10.1111/jcms.12575. Available at: <http://onlinelibrary.wiley.com/doi/10.1111/jcms.12575/epdf>. Accessed 16 May 2017

Christou, G. (2014): The EU’s Approach to Cyber Security. EUSC EU China Security Cooperation: performance and prospects. Policy paper series. Available at: <http://privatewww.essex.ac.uk/~susyd/EUSC/documents/EUSC%20Cyber%20Security%20EU%20Christou.pdf>. Accessed 16 May 2017

Fahey, E. (2014): EU’S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security. European Journal of Risk Regulation, Vol. 5, No. 1, pp. 46-60. Available at: [https://papers.ssrn.com/sol3/Delivery.cfm/SSRN\\_ID2384491\\_code1636539.pdf?abstractid=2384491&mirid=1](https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2384491_code1636539.pdf?abstractid=2384491&mirid=1). Accessed 16 May 2017

## 5. NATIONAL AND EU CYBERSECURITY BODIES

Agencia Estatal Boletín Oficial del Estado (2017): Legislación – Código de Derecho de la Ciberseguridad. Available at: [http://www.boe.es/legislacion/codigos/codigo.php?id=173\\_Codigo\\_de\\_Derecho\\_\\_de\\_la\\_Ciberseguridad](http://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Ciberseguridad). Accessed 30 May 2017

ANSSI (2016): ANSSI, ready for the 2016 European Cybersecurity Month (ESCM). Available at: <https://www.ssi.gouv.fr/en/actualite/anssi-ready-for-the-2016-european-cybersecurity-month-escm/>. Accessed 30 May 2017

ANSSI (2016) : Rapport d’activité 2015. Available at: [https://www.ssi.gouv.fr/uploads/2016/09/rapport\\_annuel\\_2015\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf). Accessed 30 May 2017

ANSSI (2016): “Stronger together” – ANSSI successfully took part in pan-European Exercise Cyber Europe 16. Available at: <https://www.ssi.gouv.fr/en/actualite/stronger-together-anssi-successfully-took-part-in-pan-european-exercice-cyber-europe-16/>. Accessed 30 May 2017

ANSSI (2017): Administration – bonnes pratiques. Available at: <https://www.ssi.gouv.fr/administration/bonnes-pratiques/>. Accessed 30 May 2017.

ANSSI (2017): Crypto – Le webdoc’. Available at: <https://www.ssi.gouv.fr/entreprise/actualite/crypto-le-webdoc/>. Accessed 30 May 2017

ANSSI (2017): Entreprise – bonnes pratiques. Available at: <https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>. Accessed 30 May 2017

ANSSI (2017): Entreprise – Certification. Available at: <https://www.ssi.gouv.fr/entreprise/produits-certifies/>. Accessed 30 May 2017

ANSSI (2017): Entreprise – principales menaces. Available at: <https://www.ssi.gouv.fr/entreprise/principales-menaces/>. Accessed 30 May 2017

ANSSI (2017): Particuliers – bonnes pratiques. Available at: <https://www.ssi.gouv.fr/particulier/bonnes-pratiques/>. Accessed 30 May 2017

Certsi (2017): Alerta Temprana – Avisos SCI. Available at: <https://www.certsi.es/alerta-temprana/avisos-sci>. Accessed 30 May 2017

Certsi (2017): Servicios operadores – Detector de incidentes. Available at: <https://www.certsi.es/servicios-operadores/detector-de-incidentes>. Accessed 30 May 2017

Certsi (2017): Servicios operadores – Notificaciones y análisis ad hoc. Available at: <https://www.certsi.es/servicios-operadores/notificaciones-y-analisis-adhoc>. Accessed 30 May 2017

CERT-EU (2011): RFC 2350. Available at: [http://cert.europa.eu/static/RFC2350/RFC2350\\_CERT-EU\\_v1\\_0.pdf](http://cert.europa.eu/static/RFC2350/RFC2350_CERT-EU_v1_0.pdf). Accessed 30 May 2017

CERT-EU (2016): About us. Available at: [https://cert.europa.eu/cert/plainedition/en/cert\\_about.html](https://cert.europa.eu/cert/plainedition/en/cert_about.html). Accessed 30 May 2017

Cyber Camp (2017): Summer boot camp. Available at: <https://cybercamp.es/summer-bootcamp>. Accessed 30 May 2017

DG JRC (2012): Will the cloud make the citizen more vulnerable? Risk and vulnerability assessment in times of cloud computing. Available at: <https://ec.europa.eu/jrc/en/publication/contributions-conferences/will-cloud-make-citizen-more-vulnerable-risk-and-vulnerability-assessment-times-cloud-computing>. Accessed 30 May 2017

DG JRC (2015): Risk assessment methodologies for critical infrastructure protection. Available at: <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf>. Accessed 30 May 2017

Europol (2017): European Cybercrime Centre – EC3. Available at: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-2>. Accessed 30 May 2017

Europol (2017): Training and capacity building. Available at: <https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building>. Accessed 30 May 2017

INCIBE (2015): Gestión de riesgos – Una guía de aproximación para el empresario. Available at: [https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia\\_gestion\\_riesgos/guiagestionriesgos.pdf](https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf). Accessed 30 May 2017

INCIBE (2015): INCIBE presenta la plataforma de NIS, como herramienta de la Estrategia Europea de Ciberseguridad, en el Infoday Horizonte 2020. Available at: <https://www.incibe.es/sala-prensa/notas-prensa/nw-infoday-raul-riesco>. Accessed 30 May 2017

INCIBE (2015): Taxonomía de ciberejercicios. Available at: [https://www.certsi.es/sites/default/files/contenidos/estudios/doc/incibe\\_taxonomia\\_ciberejercicios.pdf](https://www.certsi.es/sites/default/files/contenidos/estudios/doc/incibe_taxonomia_ciberejercicios.pdf). Accessed 30 May 2017

INCIBE (2016): 10 Encuentro internacional de seguridad de la información. Available at: <https://www.incibe.es/en/enise>. Accessed 30 May 2017

INCIBE (2016): El Instituto Nacional de Ciberseguridad representa los intereses nacionales en el European Cyber Security Organisation (ECSO). Available at: <https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-representa-los-intereses-nacionales-el>. Accessed 30 May 2017

INCIBE (2017): Formación especializada. Available at: <https://www.incibe.es/formacion>. Accessed 30 May 2017

INCIBE (2017): Protege tu empresa – Guías. Available at: <https://www.incibe.es/protege-tu-empresa/guias>. Accessed 30 May 2017

INCIBE (2017): Welcome to INCIBE. Available at: <https://www.incibe.es/en>. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2012): Factsheet Beveilig apparaten gekoppeld aan internet. Available at: <https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-apparaten-gekoppeld-aan-internet.html>. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2015): Checklist beveiliging van ICS/SCADA systemen. Available at: <https://www.ncsc.nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen.html>. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2017): Cybersecuritybeeld Nederland. Available at: <https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland>. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2017): International One Conference 2017 – We are all connected. Available at: <https://www.ncsc.nl/english/conference>. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2017): Whitepapers. Available at: <https://www.ncsc.nl/actueel/whitepapers>. Accessed 30 May 2017

## 6. OTHER SOURCES

Accenture and HfS Research (2016): The State of Cybersecurity and Digital Trust 2016 - Identifying Cybersecurity Gaps to Rethink State of the Art. Available at: <https://www.accenture.com/us-en/new-applied-now>. Accessed 16 May 2017

European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No3 – Agencies’ seat and role of the host country. Available at: [http://europa.eu/european-union/sites/europa.eu/files/docs/body/fiche\\_3\\_sent\\_to\\_ep\\_cons\\_2010-12-15\\_en.pdf](http://europa.eu/european-union/sites/europa.eu/files/docs/body/fiche_3_sent_to_ep_cons_2010-12-15_en.pdf). Accessed 30 May 2017

Court of Auditors (2015): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2014 together with the Agency’s reply. Available at: [http://www.eca.europa.eu/Lists/ECADocuments/ENISA\\_2014/ENISA\\_2014\\_EN.pdf](http://www.eca.europa.eu/Lists/ECADocuments/ENISA_2014/ENISA_2014_EN.pdf). Accessed 30 May 2017

Court of Auditors (2016): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2015 together with the Agency’s reply; 2016/C 449/25

Court of Auditors (2016): Summary of results from the Court's annual audits of the European Agencies and other bodies for the financial year 2015; 2016/C 449/01

European Commission (2015): Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

European Commission (2015): Draft General Budget of the European Union for the financial year 2016 - Working Document Part III; COM(2015) 300

European Commission (2016): Digital Single Market, Pillar III: Trust & Security. Available at: <https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security>. Accessed 30 May 2017

European Commission (2016): The EU Single Market – Copyright and Neighbouring Rights - The EU legal framework ("acquis"). Available at: [http://ec.europa.eu/internal\\_market/copyright/acquis/index\\_en.htm](http://ec.europa.eu/internal_market/copyright/acquis/index_en.htm). Accessed 30 May 2017

European Cyber Security Organisation (2016): European Cyber Security cPPP Strategic Research & Innovation Agenda. Available at: <https://ecs-org.eu/documents/ecs-cppp-sria.pdf>. Accessed 30 May 2017

EY (2015): Cybersecurity and the Internet of Things. Available at: [www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/\\$FILE/EY-cybersecurity-and-the-internet-of-things.pdf](http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf). Accessed 16 May 2017

Georgian Institute of Technology (2016): 2016 Emerging Cyber Threats Report. Available at: [www.iisp.gatech.edu/sites/default/files/documents/2016\\_georgiatech\\_cyberthreatsreport\\_onlinescroll.pdf](http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf). Accessed 16 May 2017

Government of the Netherlands and Netherlands Organisation for Scientific Research (2013): National cybersecurity research agenda II. Available at: <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/expertise--advies/onderzoek-innovatie-en-onderwijs/1/NCRSA%2BII.pdf>. Accessed 30 May 2017

PoliceMediaBlog (2016): Social Media Handbook for Law Enforcement – Europol EC3. Available at: <https://policemediablog.com/2016/01/27/social-media-handbook-for-law-enforcement-europol-ec3/>. Accessed 30 May 2017

The Kosciuszko Institute (2015): Strategic Perspectives on Cybersecurity Management and Public Policies. European CyberSecurity Journal (2015), Volume 1, Issue 1. Available at: <https://app.box.com/s/hmvkjazr1jxppjgj3skkm31dl0k6lyxw>. Accessed 16 May 2017

**APPENDIX 3**  
**SURVEY QUESTIONNAIRES**

## QUESTIONNAIRE ON ENISA'S GOVERNANCE, ORGANISATIONAL STRUCTURE AND WORKING PRACTICES

Thank you for taking the time to respond to this survey which will take approximately 15 to 20 minutes to complete.

### What is this about?


This survey is carried out by Ramboll Management Consulting and Carsa in the context of the "Evaluation of ENISA 2013-2016" commissioned by DG CONNECT.

### Who should answer?

The survey invites all ENISA staff and representatives to provide their assessments. Please note that this survey is strictly confidential - your identity will not be disclosed and the survey will be anonymous.

### How will this survey make a difference?

The survey data will contribute to the evaluation of ENISA over the 2013-2016 period and the identification of recommendations for the future. We would therefore highly appreciate your feedback.

Should you wish to read through the questionnaire prior to answering it, you may generate a printable version by clicking on this icon. You must, however, still **respond to the survey online.** 

## BACKGROUND QUESTIONS

### Please describe your main relationship with ENISA?

- (2)  ENISA Staff (including management)
- (3)  ENISA Management Board
- (4)  ENISA Executive Board
- (5)  National Liaison Officer
- (6)  Permanent Stakeholder Group

### Which department do you work for within ENISA? (optional)

- (1)  Stakeholder relations and administration
- (2)  Core Operations
- (3)  Other

### Which entity do you represent? (optional)

- (1)  The European Commission
- (2)  An EU Member State

- (3)  An EFTA Country
- (4)  Other

**From which location do you work? (optional)**

- (1)  Heraklion
- (2)  Athens

**How long have you been working for ENISA? (optional)**

- (1)  <1 year
- (2)  1-3 years
- (3)  4-5 years
- (4)  6-10 years
- (5)  > 10 years

## ENISA'S ORGANISATIONAL SET-UP

**To what extent do you agree/disagree with the statements below regarding ENISA?**

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
<p>The size of the agency is appropriate for the work entrusted to ENISA and adequate for the actual workload.</p>	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
<p>The organisational solutions and procedures of ENISA are well adapted to the work entrusted to it and to the actual workload.</p>	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
<p>The staff composition is appropriate for the work</p>	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>



Not at all                      To a limited extent                      To some extent    To a high extent    Do not know

entrusted to ENISA and  
adequate for the actual  
workload.

The recruitment and training  
procedures are appropriate  
for the work entrusted to  
ENISA and adequate for the  
actual workload.

(1)                       (2)                       (3)                       (4)                       (5)

**Please elaborate on your assessment of the statement "The size of the agency is appropriate for the work entrusted to ENISA and adequate for the actual workload."**

\_\_\_\_\_

**Please elaborate on your assessment of the statement "The organisational solutions and procedures of ENISA are well adapted to the work entrusted to it and to the actual workload."**

\_\_\_\_\_

**Please elaborate on your assessment of the statement "The staff composition is appropriate for the work entrusted to ENISA and adequate for the actual workload."**

\_\_\_\_\_

**Please elaborate on your assessment of the statement "The recruitment and training procedures are appropriate for the work entrusted to ENISA and adequate for the actual workload."**

\_\_\_\_\_

**To what extent do you agree/disagree with the statements below regarding the efficiency and/or effectiveness of ENISA's governance and management?**

Not at all                      To a limited extent                      To some extent    To a high extent    Do not know

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
<p>The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives).</p>	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>

<p>The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the efficient functioning of the Agency (i.e. in terms of value for money).</p>	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
---	------------------------------	------------------------------	------------------------------	------------------------------	------------------------------

<p>The establishment of an Executive Board has led to a more efficient functioning of the Management Board.</p>	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
---	------------------------------	------------------------------	------------------------------	------------------------------	------------------------------

<p>ENISA’s management practices are conducive to creating an effective organisation (i.e. in terms of</p>	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
---	------------------------------	------------------------------	------------------------------	------------------------------	------------------------------

Not at all
To a limited extent
To some extent
To a high extent
Do not know

meeting its objectives).

ENISA’s management

practices are conducive to

creating an efficient

(1) 
(2) 
(3) 
(4) 
(5)

organisation (i.e. in terms of

value for money).

ENISA’s location enables it to

effectively conduct its work

(1) 
(2) 
(3) 
(4) 
(5)

(i.e. in terms of meeting its

objectives).

ENISA’s location enables it to

conduct its work efficiently

(1) 
(2) 
(3) 
(4) 
(5)

(i.e. in terms of value for

money).

**Please elaborate on your assessment of the statement "The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives)."**

\_\_\_\_\_

**Please elaborate on your assessment of the statement "The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the efficient functioning of the Agency (i.e. in terms of value for money)."**

\_\_\_\_\_

**Please elaborate on your assessment of the statement "The establishment of an Executive Board has led to a more efficient functioning of the Management Board."**

\_\_\_\_\_

Please elaborate on your assessment of the statement "ENISA's management practices are conducive to creating an effective organisation (i.e. in terms of meeting its objectives)."

\_\_\_\_\_

Please elaborate on your assessment of the statement "ENISA's management practices are conducive to creating an efficient organisation (i.e. in terms of value for money)."

\_\_\_\_\_

Please elaborate on your assessment of the statement "ENISA's location enables it to effectively conduct its work (i.e. in terms of meeting its objectives)."

\_\_\_\_\_

Please elaborate on your assessment of the statement "ENISA's location enables it to conduct its work efficiently (i.e. in terms of value for money)."

\_\_\_\_\_

## ENISA'S EFFECTIVENESS AND EFFICIENCY

To what extent do you agree/disagree with the statements below regarding ENISA?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
ENISA's working practices are efficient and make best use of available resources.	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
The internal capacity and capabilities of staff are well utilised in ENISA.	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Internal management systems for planning, follow-up and monitoring are	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
effective (i.e. in terms of meeting its objectives).					
Internal management systems for planning, follow-up and monitoring are efficient (i.e. in terms of value for money).	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Knowledge and information sharing within ENISA are supported and encouraged.	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
The administrative systems in place to support ENISA’s operations are adequate and appropriate.	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
The quality control mechanisms in place ensure a high and consistent quality in ENISA’s work and publications.	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>

**Please elaborate on your assessment of the statement "ENISA’s working practices are efficient and make best use of available resources."**

\_\_\_\_\_

**Please elaborate on your assessment of the statement "The internal capacity and capabilities of staff are well utilised in ENISA."**

\_\_\_\_\_

Please elaborate on your assessment of the statement "Internal management systems for planning, follow-up and monitoring are effective (i.e. in terms of meeting its objectives)."

\_\_\_\_\_

Please elaborate on your assessment of the statement "Internal management systems for planning, follow-up and monitoring are efficient (i.e. in terms of value for money)."

\_\_\_\_\_

Please elaborate on your assessment of the statement "Knowledge and information sharing within ENISA are supported and encouraged."

\_\_\_\_\_

Please elaborate on your assessment of the statement "The administrative systems in place to support ENISA’s operations are adequate and appropriate."

\_\_\_\_\_

Please elaborate on your assessment of the statement "The quality control mechanisms in place ensure a high and consistent quality in ENISA’s work and publications."

\_\_\_\_\_

## COOPERATION WITH STAKEHOLDERS

To what extent do you agree/disagree with the statements below regarding ENISA’s cooperation with stakeholders?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
ENISA's activities are coherent with the policies and activities of its stakeholders.	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
ENISA has built strong and trustful relationships with its stakeholders when executing	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>

Not at all      To a limited extent      To some extent      To a high extent      Do not know

its mandate.

The collaboration between the Permanent Stakeholder Group and ENISA has functioned well.

(1)       (2)       (3)       (4)       (5)

The collaboration between the Permanent Stakeholder Group and ENISA has allowed for greater efficiency.

(1)       (2)       (3)       (4)       (5)

ENISA is open to cooperating with a variety of stakeholders, across different levels and sectors, to ensure best results.

(1)       (2)       (3)       (4)       (5)

ENISA has good systems and procedures in place for stakeholder consultation and management.

(1)       (2)       (3)       (4)       (5)

**Is there anything else that you would like to add in relation to ENISA's governance, organisational structure and working practices?**

---

Thank you very much for your contribution!

Click Finish to close the consultation.

Your answers have been saved. If you would like a printed copy of your answers, please click

the print button.





## QUESTIONNAIRE ON ENISA'S RELATIONSHIP WITH CERTS/CSIRTS

Thank you for taking the time to respond to this survey which will take approximately 10 minutes to complete.

### What is this about?

This survey is carried out by Ramboll Management Consulting and Carsa in the context of the project "Evaluation of ENISA" commissioned by DG CONNECT.

### Who should answer?

The survey invites CERTs / CSIRTS staff who have been sent a link to the survey to provide their assessments.

Please note that this is a strictly confidential survey - your identity will not be disclosed and the survey will remain anonymous.

### How will this survey make a difference?

The survey data will contribute to the evaluation of ENISA over the 2013-2016 period and the identification of recommendations for improvement. We would therefore highly appreciate your feedback.

Should you wish to read through the questionnaire prior to answering it, you may generate a printable version by clicking on this icon. You must, however, still **respond to the survey online**.



## BACKGROUND QUESTIONS

### Can you briefly describe your main responsibilities?

- (1)  Preventative Measures (e.g. Penetration Testing)
- (2)  Incident Response Team
- (3)  Post Incident Management (e.g. Disaster Recovery)
- (4)  Customer Relationship Management
- (5)  Policy Development
- (6)  Public Awareness
- (7)  Administration and Management
- (8)  Other

Please describe which other responsibilities you are referring to:

---

## COHERENCE

To what extent did ENISA proactively support cooperation among CERTs / CSIRTs during the 2013-2016 period?

- (1)  Not at all
- (2)  To a limited extent
- (3)  To some extent
- (4)  To a high extent
- (5)  Do not know

What else do you think could be done by ENISA to improve cooperation among CERTs / CSIRTs?

---

To what extent did ENISA cover CERTs / CSIRTs' needs over the 2013-2016 period?

- (1)  Not at all
- (2)  To a limited extent
- (3)  To some extent
- (4)  To a high extent
- (5)  Do not know

In your opinion, how important were ENISA's capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) in 2013-2016 for CERTs / CSIRTs' development?

- (1)  Not at all
- (2)  Of limited importance
- (3)  Important
- (4)  Very important
- (5)  Do not know

**To what extent will the new role foreseen for ENISA in relation to CERTs / CSIRTs as part of the NIS Directive enable ENISA to better cover CERTs / CSIRTs' needs?**

- (1)  Not at all
- (2)  To a limited extent
- (3)  To some extent
- (4)  To a high extent
- (5)  Do not know

**In concrete terms, what do you foresee ENISA doing as part of its new role as secretariat for the CSIRTs Network, as foreseen in the NIS Directive?**

\_\_\_\_\_

**What else do you think could be done by ENISA to better cover CERTs / CSIRTs' needs?**

\_\_\_\_\_

## DEGREE OF COHERENCE AND COMPLEMENTARITY

The activities below were activities conducted by ENISA to support CERTs/CSIRTs over the 2013-2016 period. In your opinion, to what extent were these activities coherent with and complementary to (i.e. not overlapping or duplicating) what CERTs/CSIRTs were doing?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
Organising and managing large-scale cyber security exercises	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Creating tools and best practices	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Providing training courses	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Developing training methodologies	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
Creating training and exercise material	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Developing publications	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Working towards cyber security cooperation	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Providing guidance based on best practice in the area of operational community efforts (operational cooperation, information exchange, etc.)	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Creating reports and roadmaps	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Organising workshops and conferences	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Supporting cooperation among CERTs/CSIRTs, within the CERTs/CSIRTs network	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>
Contributing to the dialogue between CERTs / CSIRTs and law enforcement and data privacy communities, in order to support consistent a EU-wide approach to NIS	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
Supporting the collaboration between CERTs / CSIRTs and law enforcement communities, in responding to recent policy and technical developments in this area	(1) <input type="checkbox"/>	(2) <input type="checkbox"/>	(3) <input type="checkbox"/>	(4) <input type="checkbox"/>	(5) <input type="checkbox"/>

**Is there anything else that you would like to add?**

---

Thank you very much for your contribution!

Click Finish to close the questionnaire. Your answers have been saved. If you would like a printed copy of your answers, please click the print button. ■

**APPENDIX 4  
POSITIONING EXERCISE**

This appendix presents the detailed assessment of activities of ENISA and other national and EU bodies prepared for the positioning exercise. These tables have been prepared based on findings from desk-based research and interviews with the concerned organisations. They provide an assessment on whether activities implemented by ENISA are also implemented by other EU or national bodies and if so, whether this represents a complementarity or an overlap.

The following EU bodies/organisations have been covered in the positioning exercise:

- CERT-EU (information confirmed by the organisation)
- Europol – EC3 (based on desk research)
- DG JRC (information confirmed by the organisation)

At national level, three organisations were covered:

- INCIBE – Spain (based on desk research)
- National Cyber Security Centre – Netherlands (information confirmed by the organisation)
- ANSSI – France (based on desk research)

### Note on methodology

ENISA’s activities were mapped for the positioning exercise as presented in the table below.

**Table 30: Overview of positioning analysis framework**

Overarching theme	ENISA’s activities	Sub-activity
<b>To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security</b>	Creation of good practices and recommendations on the security and resilience of	Critical Infrastructures
		Transportation
	Regular threat analysis reports	Health
		Energy (incl. Smart grids)
		Homes
		Finance
		Big Data
		Recommendations on aligning research programme(s) with policy in the specialised area of NIS
		Covering the themes described above (critical infrastructures, transportation, etc.)
		Annual overall threat analysis/landscape report
Knowledge and methodology enhancement	Threat analysis reports specific for governments	
	Threat analysis reports specific for SMEs	
<b>To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security</b>	Good practices, reports and standardisation for legal and policy areas	Threat analysis reports specific on NIS issues
		Increase in cryptographic knowledge
	Provide an overview of the threat landscape for the legal framework	Identifying critical communication networks, links, and components
		Provide best practices for data protection legal framework
		Provide best practices for incident handling legal framework
		Contribute to the development and implementation of the NIS directive
		Provide good practices for cryptographic protection measures
		Provide guidance for harmonisation of legal framework and standards for the private sector
		Support policy discussion in thematic areas:
		-smart grids
-IT security certification		
<b>To assist the Member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union</b>	Good practices, white papers and guidelines	-finance
		-electronic communications
		on how to conduct risk assessment and handle incident tracking
		on how to conduct training and exercises directed towards vulnerable infrastructures related to NIS Directive needs
		for fostering cybersecurity culture in the private sector
for national cybersecurity strategies		

	Trainings	Trainings and exercises for CERTs On-request training for Member States and EU bodies Workshops to Assist and advise Member States on the secure use of cloud computing for e-government applications and services On-request support for Member States decision-making in the areas of privacy and trust
	Standardisation	Harmonised Minimum Security Measures for Internet Service Providers Provide minimum Security Measures for Cloud Computing
	Direct support and assistance	Provide guidance and support for the European Cyber Security Month Support the working groups of the NIS platform Direct support for CERTs strategic direction Assisting member states in building capabilities on national Private-Public-Partnerships (PPPs) Support and advise member states on the establishment and evaluation of national cybersecurity strategies
	Incident analysis	Annual incident reports and recommendations on how to mitigate threats
	<b>To enhance cooperation both between the Member States of the European Union and between related network and information security communities</b>	Cross Member States cooperation building Workshops with 2 or more Member States Fostering discussion among 2 or more Member States through events Cybersecurity exercises with 2 or more Member States

to the aim of this exercise was to compare ENISA’s services with those of CERT-EU, EC3, DG JRC, the Dutch National Cyber Security Centre, the French National Cybersecurity Agency and the Spanish National Institute for Cybersecurity. In order to do so a desk research was conducted and individuals in the concerned organisations were contacted to gather the missing information. A full assessment of overlaps and complementarities was provided by CERT-EU and a partial contribution was received from the DG JRC, Netherlands National Cyber Security Centre and the Spanish National Institute for Cybersecurity (providing detailed information on activities but with no assessment of overlaps or complementarities). For the remaining organisations (EC3 and the French ANSSI) best judgments were made regarding possible overlaps or complementarities given the limited information available online.

Organisations were compared at the activity level based on an overall assessment of the differences or similarity observed between organisations. Finally, desk research findings were cross-checked with information obtained from the interviews. Based on this research complementarities and overlaps were identified.

It is to be noted that even if no clear overlap was identified, the issue might remain that ENISA does not build on the existing competencies and activities of other organisations. For example, even if reports produced by ENISA do not cover exactly the same topics as reports produced by other organisations, it might be the case that there is room for more efficiency gains in ENISA not basing its work on the existing work done in other organisations on the topic.

**1. CERT-EU**

All information provided in the comments concerning CERT-EU’s activities was provided directly by CERT-EU through the positioning exercise and the interviews.



Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
<b>To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security</b>	Good practices and recommendations	Complementarity	<p>CERT-EU contributes to ISACs related to critical infrastructure, transportation, health and other topics relevant to the thematic areas of focus of ENISA. They provide information about the technical developments in the threat landscape and offer informal security advice. They service therefore complements that of ENISA.</p> <p>As pointed out during an interview, there is a risk that CERT-EU and ENISA publish statements on issues already covered by one another but this risk does not represent an actual overlapping issue.</p>
	Regular Threat Analysis Reports	Complementarity	<p>CERT-EU provides highly technical reports aimed at its constituents and peers and include non-public information which is distributed on a need-to-know basis. ENISA's reports contain only public information and are written for the public at large. They therefore complement each other.</p> <p>In addition, CERT-EU uses the reports produced by ENISA for their own monthly reports and feed into ENISA's annual report.</p> <p>They try to have an operational cooperation and avoid any duplication of work.</p>
	Knowledge and Methodology Enhancements	Complementarity	<p>CERT-EU provides limited advice to its constituents on how to identify critical communication networks, links and components. ENISA works for the public at large. They therefore complement each other.</p> <p>One interview pointed at the danger for overlap in the work CERT-EU and ENISA conduct on cryptography and vulnerabilities.<sup>141</sup></p>
<b>To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security</b>	Good practices, reports and standardisation for legal and policy areas	Complementarity	<p>CERT-EU brought out guidelines for notifications of cyber-security incident response processes to Data Protection Officers, aimed at EU institutions, bodies and agencies but published as a white paper. They therefore aim at a different scope and audience than ENISA.</p>
<b>To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union</b>	Good practices, white papers and guidelines for the government	None	<p>CERT-EU publishes white papers on selected security issues of current interest on their website, which are publicly available.</p>
	Trainings	Complementarity	<p>CERT-EU provides very technical trainings and workshops to its constituency. The audience differs from that of the trainings delivered by ENISA.</p>
	Standardisation	None	N/A
	Direct Support and Assistance	Overlap	<p>While CERT-EU discusses best practices with other CERTs, they do not provide direct support and assistance.</p> <p>It appeared however that those who want to build a CERT go to CERT-EU for practical advice rather than to ENISA. There is a risk of overlap in the advice and expertise that both organisations provide them with.</p>
	Incident Analysis	Complementarity	<p>CERT-EU provides incident analysis reports to its constituency. These reports are however highly technical, confidential</p>

<sup>141</sup> We were not able to identify clear evidence for such overlaps in publicly accessible reports and have therefore not taken into account the evidence coming from this one interview.

			and exclusive to these constituents and peers. ENISA's incident analysis reports are public.
<b>To enhance cooperation both between the Member States of the European Union and between related network and information security communities</b>	Cross Member States cooperation building	Overlap	CERT-EU organised workshops on Malware Information Sharing Platforms in which national and governmental CERTs participated.  Nine interviews pointed at the fact that CERT-EU tends to act outside of its mandate on cooperation building, potentially overlapping with what ENISA is or should be doing. For example, CERT-EU should not be directly getting in touch with commercial organisations in Member States but does so through national CERTs.

## 2. Europol – EC3

Little information is accessible on EC3's website. The assessment below was made by the evaluators but was not confirmed by EC3.

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
<b>To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security</b>	Good practices and recommendations	None	N/A
	Regular Threat Analysis Reports	None	N/A
	Knowledge and Methodology Enhancements	None	N/A
<b>To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security</b>	Good practices, reports and standardisation for legal and policy areas	Complementarity	EC3 works together with ENISA to provide workshops which aim at defining a common taxonomy between CSIRTs and Law Enforcement and facilitate information sharing between the two communities. <sup>142</sup> EC3 developed a Handbook for Law Enforcement on the use of social media for prevention/awareness purposes. <sup>143</sup>
	Good practices, white papers and guidelines for the government	None	N/A
<b>To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union</b>	Trainings	Complementarity	EC3 supports training for the relevant authorities in Member States. <sup>144</sup> It however provides trainings that are very focused on reacting to cybercrime by involving the national law enforcement authorities, therefore differing from what ENISA does.
	Standardisation	None	N/A
	Direct Support and Assistance	Complementarity	EC3 provides direct support in reducing cybercrime through its operational powers (e.g. arresting cyber criminals or taking down cybercrime forums). <sup>145</sup>
	Incident Analysis	Complementarity	EC3 does not provide publicly available incident analysis reports but has some publicly available tools to understand the different types of cyber threats and how individuals can avoid becoming victims to them. <sup>146</sup>
<b>To enhance cooperation both between the Member States of the European Union and between</b>	Cross member states cooperation building	Complementarity	As noted previously, EC3 works together with ENISA to provide workshops which aim at defining a common taxonomy between CSIRTs and Law Enforcement

<sup>142</sup> <https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop>

<sup>143</sup> <https://policemediablog.com/2016/01/27/social-media-handbook-for-law-enforcement-europol-ec3/>

<sup>144</sup> <https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building>

<sup>145</sup> <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-2>

<sup>146</sup> <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-2>

<b>related network and information security communities</b>			and facilitate information sharing between the two communities. <sup>147</sup>
---	--	--	--

### 3. DG JRC

All information provided in the comments concerning the DG JRC's activities was provided directly by the DG JRC through the positioning exercise and the interviews.

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
<b>To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security</b>	Good practices and recommendations	General complementarity but some risk for duplication	<p>The DG JRC provides good practices and recommendations on critical infrastructures, transportation, energy and homes. These activities primarily come in form of a contribution to the Commission's work and are in this sense complementary to ENISA's work targeting Member States and a broader stakeholder group.</p> <p>E.g. contribution to Commission work on Cooperative Intelligent Transport System (C-ITS), in particular with respect to security and privacy: participation in the C-ITS platform, contribution to its final report, to the preparation of the "European Strategy for C-ITS" Com(2016)-766, to the C-ITS common certificate and security policy, Interaction as Commission representative with the Technology subgroup of the Article 29 working party</p> <p>Preparation of a BREF (Best Available Techniques Reference Document) for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems. Co-chairing with DG ENER of the WG2 (on cybersecurity and privacy) of the Smart Grid Task Force</p>
	Regular Threat Analysis Reports	Complementarity	Through the ITIS project, DG JRC provides news bulletins on vulnerabilities and threats in the EU for the energy sector and also half year reports on foresight for emerging threats
	Knowledge and Methodology Enhancements	Risk of duplication	The DG JRC has developed risk assessment methodologies reports that are available to the MS for implementation
<b>To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security</b>	Good practices, reports and standardisation for legal and policy areas	Complementarity	<p>The DG JRC provides direct support to the European Commission in the development of good practices and standardisation for legal and policy areas.</p> <p>E.g. contribution to the recent review of the ePrivacy Directive and preparation of a proposed Regulation</p> <p>Starting, supporting DG CNECT with methodology and best practices insights, in the NIS Cooperation Group, for Essential Services identification and the criteria to use.</p> <p>Work on the preparation of a roadmap for the security certification and labelling of ICT goods and services (part of COM(2016) 410 - Strengthening Europe's Cyber Resilience System) Request for DG CNECT to support the identification of essential services by MS.</p>
	Good practices, white papers and guidelines for the government	Complementarity	The DG JRC has developed risk assessment methodologies reports that are available to the MS for implementation
<b>To assist the member States and the European Union institutions and bodies in enhancing</b>	Trainings	Complementarity	The DG JRC does not provide training to

<sup>147</sup> <https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop>

<b>capacity building throughout the European Union</b>			CERTs. Three training activities until now for MS and for operators of critical infrastructures in the EU. These are done on requests
	Standardisation	None	N/A
	Direct Support and Assistance	None	N/A
	Incident Analysis	None	N/A
<b>To enhance cooperation both between the Member States of the European Union and between related network and information security communities</b>	Cross member states cooperation building	Complementarity	Workshops on: zero-day vulnerability EU governance, Transborder personal data-breach exercise, data portability, encryption/decryption  The DG JRC is supporting the EU Critical Information Infrastructure Protection (CIIP) Action Plan by contributing to the organisation of pan-European cyber-security exercises. This is organised in cooperation with ENISA.

#### 4. INCIBE – Spain

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
<b>To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security</b>	Good practices and recommendations	Complementarity	INCIBE produces some guides aimed at public and private actors. <sup>148</sup> These guides and the guides produced by ENISA do not have obvious overlaps and can be used in a complementary fashion by end-users.
	Regular Threat Analysis Reports	Overlap	INCIBE compiles incidents notice and provides a number of incident analysis reports. <sup>149</sup> While these might be in Spanish and with a particular national focus, it is unclear whether the actors looking at these analyses benefit from the additional analysis reports provided by ENISA.
	Knowledge and Methodology Enhancements	Overlap	INCIBE helps companies in critical infrastructures to identify critical weaknesses. <sup>150</sup> It is unclear what additional value ENISA is bringing to these companies when they provide help on identifying critical communication networks, links and components.  There were no clear overlaps identified concerning other areas of knowledge and methodology enhancements.
<b>To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security</b>	Good practices, reports and standardisation for legal and policy areas	Complementarity	INCIBE cooperates with the Spanish government to produce standardised best practices which aim at contributing to the development and implementation of the NIS Directive. They have for example compiled all of the Spanish legislation which affects the area of cybersecurity. <sup>151</sup> ENISA brings in the EU aspect and helps INCIBE and the Spanish government by providing what they see as being the best practices based on experience across Member States.
<b>To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union</b>	Good practices, white papers and guidelines for the government	Complementarity	INCIBE produces a number of reports which aim at providing best practices, for example on how to conduct trainings and exercises <sup>152</sup> , how businesses should manage risks <sup>153</sup> . In addition, they work alongside the Spanish government on establishing national strategies related to the NIS Directive. <sup>154</sup> ENISA's complementary role here is to

<sup>148</sup> <https://www.incibe.es/protege-tu-empresa/guias>

<sup>149</sup> <https://www.certs.es/servicios-operadores/notificaciones-y-analisis-adhoc>

<sup>150</sup> <https://www.certs.es/servicios-operadores/detector-de-incidentes>

<sup>151</sup> [http://www.boe.es/legislacion/codigos/codigo.php?id=173\\_Codigo\\_de\\_Derecho\\_de\\_la\\_Ciberseguridad](http://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad)

<sup>152</sup> <https://www.certs.es/guias-y-estudios/estudios/taxonomia-ciberejercicios>

<sup>153</sup> [https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia\\_gestion\\_riesgos/guiageestionriesgos.pdf](https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiageestionriesgos.pdf)

<sup>154</sup> <https://www.incibe.es/sala-prensa/notas-prensa/nw-infoday-raul-riesco>

			link this effort with the good practices observed at the European level.
	Trainings	Complementarity	INCIBE provides trainings and exercises, including to CERTS and security forces <sup>155156</sup> . It seems that ENISA focuses more on capacity building trainings for CERTs and that INCIBE provides specific trainings (e.g. on fraud detection using machine learning and deep learning). <sup>157</sup>
	Standardisation	None	INCIBE does not seem to provide minimum security measures to internet service providers or for cloud computing in the same way ENISA does.
	Direct Support and Assistance	Complementarity	INCIBE provides some support to the state on establishing and evaluating its National Cyber Security Strategy and contributes to the establishment of private-public partnerships in cybersecurity. <sup>158</sup> It is however unclear how much of what they do is complementary or overlapping with ENISA's activities. We did not identify any clear overlaps.
	Incident Analysis	Overlap	INCIBE repertories and analyses incidents happening in Spain. <sup>159</sup> They also provide advice to companies on how to mitigate threats and identify their own weaknesses. <sup>160</sup> It is therefore unclear what ENISA's added value is in that regards.
<b>To enhance cooperation both between the Member States of the European Union and between related network and information security communities</b>	Cross member states cooperation building	Complementarity	INCIBE organises workshops <sup>161</sup> and helps foster discussion among member states <sup>162</sup> with the help and in coordination with ENISA.

## 5. NCSC - Netherlands

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
<b>To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security</b>	Good practices and recommendations	Overlap	The Dutch Cybersecurity Centre produces good practices for critical infrastructures and for the protection of home internet devices. <sup>163</sup> It is not clear what the added value of good practices produced in these areas by ENISA would have in the Netherlands.
	Regular Threat Analysis Reports	Overlap	The Dutch Cybersecurity Centre compiles incidents and provides regular threat analysis reports. These reports are in Dutch and seem to focus on the national level. <sup>164</sup> It is however not clear what the added value of the reports provided by ENISA is for the Dutch actors.
	Knowledge and Methodology Enhancements	Complementarity	The Dutch Cybersecurity Centre conducts research in cryptography. <sup>165</sup> No clear overlap was spotted between the reports produced by the Dutch Cybersecurity Centre and the ones produced by ENISA.
<b>To assist the Member States and the European Union institutions and</b>	Good practices, reports and standardisation for legal and policy areas	Overlap	The Dutch Cybersecurity Centre produces a number of reports and white papers <sup>166</sup> to support the government of the

<sup>155</sup> <https://cybercamp.es/summer-bootcamp>

<sup>156</sup> <https://www.incibe.es/formacion>

<sup>157</sup> <https://cybercamp.es/programa/agenda>

<sup>158</sup> <https://ecs-org.eu/documents/ecs-cppp-sria.pdf>

<sup>159</sup> <https://www.certs.es/alerta-temprana/aviso-sci>

<sup>160</sup> <https://www.certs.es/servicios-operadores/detector-de-incidentes>

<sup>161</sup> <https://www.incibe.es/en/enise>

<sup>162</sup> <https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-representa-los-intereses-nacionales-el>

<sup>163</sup> <https://www.ncsc.nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen.html>

<sup>164</sup> <https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-apparaten-gekoppeld-aan-internet.html>

<sup>165</sup> <https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland>

<sup>166</sup> <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/expertise--advies/onderzoek-innovatie-en-onderwijs/1/NCRSA%2BII.pdf>

<sup>166</sup> <https://www.ncsc.nl/actueel/whitepapers>

<b>bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security</b>			Netherlands on the topic of the cybersecurity legal framework. It is unclear how much ENISA is bringing in addition to the work already happening.
<b>To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union</b>	Good practices, white papers and guidelines for the government	No	The Dutch Cybersecurity Centre did not report any activity in this category.
	Trainings	Overlap	The Dutch Cybersecurity Centre provides trainings and exercises such as the ISIDOOR exercise. Their audience includes some CERTs. There is therefore a risk of overlap here depending on the content of each training.
	Standardisation	No	The Dutch Cybersecurity Centre did not report any activity in this category.
	Direct Support and Assistance	No	The Dutch Cybersecurity Centre did not report any activity in this category.
	Incident Analysis	Overlap	The Dutch Cybersecurity Centre produces an annual cybersecurity report for the Netherlands <sup>167</sup> . It is unclear how useful the annual cybersecurity landscape report by ENISA is useful to the Netherlands. It might be good for cross-referencing and providing additional details.
<b>To enhance cooperation both between the Member States of the European Union and between related network and information security communities</b>	Cross member states cooperation building	Complementarity	The Dutch Cybersecurity Centre organises yearly conferences called the International One Conference <sup>168</sup> . They also organise cyber exercises with neighbouring countries. As such, they participate in the same effort as ENISA towards cooperation building without duplicating what ENISA does.

## 6. ANSSI - France

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
<b>To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security</b>	Good practices and recommendations	Overlap	There might be some overlaps in that ANSSI provides good practices for individuals <sup>169</sup> , industries <sup>170</sup> and administrations <sup>171</sup> . While these good practices might be in French or focused on the French national context, there is a risk of duplication of work if ENISA produces similar good practices.
	Regular Threat Analysis Reports	Overlap	ANSSI regularly provides threat analysis to inform individuals, governments and enterprises of the threat landscape. <sup>172</sup> It produces reports on the different techniques used by cyber criminals. <sup>173</sup> While these reports might be in French, if they are made publicly available, there is therefore a risk of overlap with what ENISA is doing.
	Knowledge and Methodology Enhancements	Overlap	ANSSI does quite a lot of work on cryptography. <sup>174</sup> There is therefore a risk of overlap with what ENISA does in that regard.
<b>To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network</b>	Good practices, reports and standardisation for legal and policy areas	Complementarity	ANSSI provides advice to the French government on strategies to take and best practices to observe in order to foster cybersecurity in France. <sup>175</sup> ENISA is however complementary to that work in that they support the development of EU policies and represent the interest of ANSSI and other CS agencies in dialogues

<sup>167</sup> <https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland>

<sup>168</sup> <https://www.ncsc.nl/english/conference>

<sup>169</sup> <https://www.ssi.gouv.fr/particulier/bonnes-pratiques/>

<sup>170</sup> <https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>

<sup>171</sup> <https://www.ssi.gouv.fr/administration/bonnes-pratiques/>

<sup>172</sup> <https://www.ssi.gouv.fr/entreprise/principales-menaces/>

<sup>173</sup> [https://www.ssi.gouv.fr/uploads/2016/09/rapport\\_annuel\\_2015\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf)

<sup>174</sup> <https://www.ssi.gouv.fr/entreprise/actualite/crypto-le-webdoc/>

<sup>175</sup> [https://www.ssi.gouv.fr/uploads/2016/09/rapport\\_annuel\\_2015\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf)

<b>and information security</b>			among the EU institutions in supporting the implementation of EU legislation. This was noted during the interview with ANSSI as a new need identified by the French agency.
<b>To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union</b>	Good practices, white papers and guidelines for the government	Overlap	ANSSI has a number of good practices aimed at the public <sup>176</sup> and the private sectors. <sup>177</sup> They also work with the government to define strategies related to the NIS Directive needs. <sup>178</sup> There is therefore a risk of overlap with what ENISA is doing.
	Trainings	None	N/A
	Standardisation	Overlap	ANSSI aims at enforcing standards through the creations of qualifications and certifications in France. <sup>179</sup> There is therefore a risk of overlap with what ENISA does.
	Direct Support and Assistance	Complementarity	ANSSI is a campaign coordinator for the European Cyber Security Month. <sup>180</sup> It also provides direct support and assistance to the French government. <sup>181</sup> As such, it is complementary with what ENISA does.
<b>To enhance cooperation both between the Member States of the European Union and between related network and information security communities</b>	Incident Analysis	None	N/A
	Cross member states cooperation building	Complementarity	ANSSI works in collaboration with ENISA on organising and attending events which aim at increasing cooperation among member states. <sup>182</sup>

<sup>176</sup> <https://www.ssi.gouv.fr/particulier/bonnes-pratiques/>

<sup>177</sup> <https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>

<sup>178</sup> [https://www.ssi.gouv.fr/uploads/2016/09/rapport\\_annuel\\_2015\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf)

<sup>179</sup> <https://www.ssi.gouv.fr/entreprise/produits-certifies/>

<sup>180</sup> <https://www.ssi.gouv.fr/en/actualite/anssi-ready-for-the-2016-european-cybersecurity-month-escm/>

<sup>181</sup> [https://www.ssi.gouv.fr/uploads/2016/09/rapport\\_annuel\\_2015\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf)

<sup>182</sup> <https://www.ssi.gouv.fr/en/actualite/stronger-together-anssi-successfully-took-part-in-pan-european-exercice-cyber-europe-16/>

**APPENDIX 5  
COMPREHENSIVE SWOT TABLE**



STRENGTHS	WEAKNESSES
<p><b>Independence / neutrality.</b> ENISA is an independent agency without political or commercial bias. Its independence is supported by its location in Heraklion and Athens giving it less involvement in the everyday politics in cybersecurity in Brussels.<sup>183</sup></p>	<p><b>Lack of a more strategic, long-term vision.</b> ENISA has difficulties in executing a long-term vision due to regulatory constraints and overlapping mandates (other agencies/bodies claiming to have expertise and ownership in cybersecurity).<sup>184</sup> ENISA's work programme is influenced by the interests of Member States, although its flexibility has been broadened by Art.14, it's not enough.<sup>185</sup> <sup>186</sup></p>
<p><b>Capacity building assistance.</b> ENISA has a good track record / experience organizing trainings, cybersecurity exercises, development of manuals, studies trying to reach a broad sector (Member States, private actors, European Union institutions and agencies<sup>187</sup>). The aim of this capacity building activity is to develop the capabilities of the agents, providing them with the necessary tools to prevent, detect and handle incidents.<sup>188</sup> Agencies reporting best practices on the cyber domain could be encouraged.<sup>189</sup></p>	<p><b>Limited visibility of ENISA.</b> As a result of weak communication, marketing and/or branding, ENISA is not very present, i.e. it has not managed to carve out its own space within the cybersecurity policy landscape.<sup>190</sup></p>
<p><b>Maintaining the network / coordination role</b><sup>191</sup>. ENISA is involved in addressing existing fragmentation at national, European and international level<sup>192</sup>. It acts as a pole to gather and exchange information and best practices among Member States, EU and international players. ENISA is also involved in fostering cooperation with the private sector and encourages the setup of PPP as a way to increase the operational capabilities in the sector. It also bolsters the establishment of cyber threat reporting channels as a way to</p>	<p><b>Office location in Heraklion and Athens.</b> ENISA's location impacts its capabilities / capacities in terms of recruiting high-level experts (difficulties for spouses to integrate and limited international schooling options) and connectedness to influence cybersecurity policy in Brussels due to the distance to decision makers in the EU institutions. An option would be to have a liaison office.<sup>195</sup></p>

<sup>183</sup> See interviews

<sup>184</sup> See interviews

<sup>185</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

<sup>186</sup> See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<sup>187</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

<sup>188</sup> See European Parliament and Council Regulation (EU) No 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

<sup>189</sup> Experts discussions

<sup>190</sup> See interviews

<sup>191</sup> See European Parliament and Council Regulation (EU) No 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

<sup>192</sup> See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

<p>gather information and disseminate expertise.<sup>193</sup></p> <p>Furthermore, being part of the EC3 board assures ENISA involvement in other NIS related issues of cybercrime.<sup>194</sup></p>	
<p><b>Member States support:</b> ENISA has cyber resilience capability and supports the fostering of Member States' effectiveness in this area.<sup>196</sup></p> <p><sup>197, 198</sup></p> <p>It also, plays a role assisting the national CERTs (from their set-up to their daily activities)<sup>199</sup>. Its role as CERT coordination should be enhanced.<sup>200</sup></p>	<p><b>Inadequate staff composition and human resources policies.</b><sup>201</sup> ENISA's staff lacks the technical expertise to act as a reference in cybersecurity in policy. Next to a lack of computing specialists, there is a lack of career opportunities within the Agency. More junior staff members tend to move on causing capability loss of the Agency.</p>
<p><b>Horizontal policy expertise.</b> ENISA has expertise and experience in strengthening detection and prevention of cybersecurity threats in different country contexts giving it more horizontal expertise. One of its main activities is to assist the development and implementation of NIS related policies and laws, trying to strengthen the importance of cybersecurity as an EU policy priority.<sup>202</sup></p>	<p><b>Limited size and low financial resources.</b><sup>203</sup></p> <p>The budget allocated for cybersecurity is low if compared with other areas or with the resources spent in other countries on this issue.<sup>204</sup></p>
<p><b>Recognised relationships with its stakeholders.</b> ENISA's stakeholders judge their relationship with ENISA to be trustful and effective.</p>	<p><b>Recruitment and training procedures.</b></p> <p>Recruitment and training procedures of ENISA are considered not appropriate or only appropriate to a limited extent to manage ENISA's workload. Additional comments revealed that the recruitment process is considered too slow and therefore not being adapted to the cybersecurity domain.<sup>205</sup></p>

<sup>195</sup> See interviews

<sup>193</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

<sup>194</sup> See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee

<sup>196</sup> See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

<sup>197</sup> See ENISA (2016) Evaluation Roadmap 25/07/2016.

<sup>198</sup> See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<sup>199</sup> See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

<sup>200</sup> See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee

<sup>201</sup> See interviews

<sup>202</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

<sup>203</sup> Ibid.

<sup>204</sup> See Fahey, E. (2014) 'EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security'. European Journal of Risk Regulation, Vol. 5, No. 1, pp. 46-60.

<sup>205</sup> See ENISA survey

OPPORTUNITIES	THREATS
<p><b>Synergies &amp; risk management culture<sup>206</sup>.</b> There is a growing need to explore and ensure synergies between operators as to assure concerted and collaborative NIS policy actions<sup>207</sup>. Cooperation is also important in the public-private dimension. Improvement regarding information sharing could help the creation of a coherent risk management culture aligned with existing crisis mechanisms. ENISA could work to ensure effective cooperation and prompt information sharing between EU institutions and different agencies, national government and the private sector. Without the involvement of the private sector it will be difficult to identify the relevant threats.<sup>208</sup></p>	<p><b>Insufficient sharing of information - lack of data.</b> Stakeholders in the private sector are reluctant to share information regarding NIS incidents<sup>209</sup>. The fact that reporting is not mandatory for public authorities does not encourage the private sector to do so on a voluntary basis. In addition, some private companies lack training in cybersecurity issues<sup>210</sup>. Incentives for information disclosure are not attractive. Some sectors are more eager to cooperate than others (financial vs telecommunications). Member States are also averse to disclose relevant information to ENISA, in particular, where national security is concerned. Furthermore, there is a lack of consensus among Member States' understanding of the cyber domain<sup>211 212</sup></p>
<p><b>ICT standardization, certification and harmonisation.</b> ENISA should encourage harmonisation regarding threat assessments (threats, threat tools and vulnerabilities). In order to create digital trust, ENISA should seek to introduce a European ICT labelling for cybersecurity products. This would help foster the integration of the Single Market, create trust and protect credentials. Harmonisation of different national legislation should be sought at EU level in order to have an effective cybersecurity protection.<sup>213</sup></p>	<p><b>Fragmentation and coordination.</b> Fragmentation is an issue regarding operational capabilities<sup>214</sup> (e.g. ENISA has no operational power and therefore cannot intervene to fix NIS issues)<sup>215</sup>. In addition, there is a diverse set of agencies dealing with different issues in the cyber incident landscape. Coordination amongst different agencies is sometimes not only difficult, but also distorts the visibility and hinders accessibility of the European response to threats and demands of</p>

<sup>206</sup> See European Commission (2013). SWD (2013) 31 final; COM (2013) 48 final: Commission Staff Working Document-Executive Summary of the Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union.

<sup>207</sup> See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

<sup>208</sup> See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<sup>209</sup> See European Commission (2013). SWD (2013) 31 final; COM (2013) 48 final: Commission Staff Working Document-Executive Summary of the Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union.

<sup>210</sup> See European Commission (2013). JOIN (2013) 1 final: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

<sup>211</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

<sup>212</sup> See Carrapico, H., Barrinha, A. (2017). The EU as a coherent (cyber)security actor?

<sup>213</sup> See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee

<sup>214</sup> See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

	<p>stakeholders. For instance, one Member State representative claimed that “his organisation did not work together with ENISA and that if they came across ENISA’s work, it was by coincidence”<sup>216</sup>. There is a need to disseminate ENISA’s work. Furthermore, a clear distribution of competences within the different agencies could help to strengthen EU capacity to react.<sup>217</sup> Some experts suggest that if similar functions are identified at ENISA, EC3 or CERT-EU they should be merged.<sup>218</sup></p>
<p><b>Awareness raising and capacity building.</b> Public awareness on cyber threats should be enhanced. ENISA could enhance its discourse and awareness strategy and provide additional guidance, training regarding management of cyber threats.<sup>219</sup> ENISA could also use its expertise in cyber resilience to strengthen pan-European cyber incident exercises and examine computer security incident response teams.<sup>220</sup> There is a need to assist and develop national cyber resilience capability and ENISA should continue its works in the domain, helping for instance the development of national contingency plans and organizing regular emergency exercises and setting alarms to detect attacks on critical infrastructures.<sup>221</sup></p>	<p><b>Cooperation with Member States - capability gaps.</b> The priorities set by national governments in cybersecurity vary significantly among Member States. Member States’ cyber capacities and capabilities are uneven<sup>222</sup> <sup>223</sup> not only at preparedness level, but also at policy. Divergent legislation, priorities and coordination problems can lead towards Single Market fragmentation, lack of effectiveness of the European response and interoperability problems when incidents spread across borders.<sup>224</sup> The new Cooperation Group set up by NIS Directive, aims to overcome this weakness aiming to strengthen cooperation among Member States and offering advice on security issues.<sup>225</sup></p>

<sup>215</sup> See European Commission (2013). JOIN (2013) 1 final: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

<sup>216</sup> See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

<sup>217</sup> See ENISA (2016) Evaluation Roadmap 25/07/2016.

<sup>218</sup> See Fahey, E. (2014) ‘EU’S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security’. European Journal of Risk Regulation, Vol. 5, No. 1, pp. 46-60.

<sup>219</sup> See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

<sup>220</sup> Ibid.

<sup>221</sup> See Bendiek, A. (2012) ‘European Cyber Security Policy’, SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<sup>222</sup> See European Commission (2013). JOIN (2013) 1 final: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

<sup>223</sup> See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe’s Cyber Resilience System and Innovative Cybersecurity Industry.

<sup>224</sup> See European Commission (2013). SWD (2013) 31 final; COM (2013) 48 final: Commission Staff Working Document-Executive Summary of the Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union.

<sup>225</sup> See Bendiek, A. (2012) ‘European Cyber Security Policy’, SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<p><b>Stakeholder engagement.</b>                  Reinforce links with industry stakeholders<sup>226</sup>.                  Broader cybersecurity ecosystem.                  Sharing of information, practices among operators → instrumental role of ENISA.<sup>227</sup>                  EU agencies are one of the principal channels to engage with the private sector.<sup>228</sup></p>	<p><b>Lacking capacities to respond to changing technological landscape and corresponding new vulnerabilities<sup>229</sup>, such as:</b></p> <ul style="list-style-type: none"> <li>• Data theft of corporate information: emergence of “corporate insider”</li> <li>• Economic espionage and state sponsored activities</li> <li>• Overall data loss or destruction</li> <li>• Malicious apps (malware)</li> <li>• Hijacking-interception of information</li> <li>• Nefarious activity: identity fraud, denial of service, malicious code, rouge certificates, failure of business process</li> <li>• Online fraud-point</li> </ul> <p>Cyber-attack methods have become more pervasive<sup>230</sup> → low-end, low to medium tech. Furthermore, cyber-attackers’ profile, methods, and aims are diverse. It is not possible do draw an accurate portrait.</p> <p>In addition, states are not only subject to cyber-attacks but are also performing them. The EU is lacking a method to detect and disseminate information about threats and attacks.<sup>231</sup></p>
<p><b>Multi-perspective and holistic approach.</b>                  There is a need for comprehensive security policies. Broader engagement from industry and the community should be envisaged, as well as the use of dual capabilities (e.g. civil-military cooperation)<sup>232</sup>. Civil society perspective should also be taken into account.<sup>233</sup></p> <p>If incident report becomes mandatory for other sectors, there can be new opportunities for ENISA to support Member States in building</p>	<p><b>Internet of Things (IoT).</b> Interconnectivity between devices implies that there is a larger vulnerable surface.<sup>235</sup> The boundary of the companies is disappearing as everything is connected, and thus finding loopholes to enter is easier. Securing the supply chain is still challenging.<sup>236</sup></p>

<sup>226</sup> See European Commission (2013). JOIN (2013) 1 final: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

<sup>227</sup> See ENISA (2015). Threat Landscape and Good Practice Guide for Software Defines Networks/ 5G: ISBN: 978-92-9204-161-8, DOI: 10.2824/67261.

<sup>228</sup> See Bendiek, A. (2012) ‘European Cyber Security Policy’, SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<sup>229</sup> See European Commission (2013). JOIN (2013) 1 final: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

<sup>230</sup> See ENISA (2015). CYBER 7: Seven messages to the edge of Cyber-Space; Catalogue Number: TP-04-15-745-EN-C; ISB: 978-92-9204-133-5.

<sup>231</sup> See Bendiek, A. (2012) ‘European Cyber Security Policy’, SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<sup>232</sup> See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe’s Cyber Resilience System and Innovative Cybersecurity Industry.

<sup>233</sup> The Kosciuszko Institute- European CyberSecurity Journal (2015), Volume 1, Issue 1. Strategic Perspectives on Cybersecurity Management and Public Policies

<p>more resilience against cyber-attacks. Without carefully defined and orchestrated security rules and procedures, it is impossible to imagine a functional and reliable software-defined networking infrastructure.<sup>234</sup></p>	
<p><b>Consumer protection.</b> Safeguard online environment providing highest possible freedom and security (fundamental rights, freedom of expression, personal data and privacy).</p>	<p><b>Talent Gap.</b> There are not enough cybersecurity skilled workers → There is a need to broaden the pool of talent. <sup>237, 238</sup></p>
<p><b>Cross-border coordination.</b> As most of the incidents arise from cross border activity, ENISA could strengthen its coordination role at EU level.<sup>239 240</sup> The EU level is best placed to supervise and respond to cyber-attacks, in order to help close the capability gaps that are identified at national level.<sup>241</sup></p>	<p><b>Lack of funding and prioritisation of cybersecurity at enterprise level.</b> There is not enough available funding for private companies to secure their infrastructure<sup>242, 243</sup> Private companies also often do not set cybersecurity as a clear priority (statement from experts) – lack of interest to invest in cybersecurity.<sup>244</sup></p>
<p>The <b>NIS Directive</b> has helped to develop a coherent and less fragmented vision of cybersecurity at EU level.<sup>245</sup></p>	<p><b>NIS Directive - additional tasks, but no extra funding.</b><sup>246</sup> The NIS Directive imposes many additional tasks on the Agency without cuts on responsibilities assigned before the NIS Directive. At the same time, no increase in the resources occurred. There is a risk that ENISA will not be able to deliver high quality outputs on all the tasks entrusted to it.</p>

<sup>235</sup> See ENISA (2015). **CYBER 7: Seven messages to the edge of Cyber-Space**; Catalogue Number: TP-04-15-745-EN-C; ISB: 978-92-9204-133-5.

<sup>236</sup> Georgian Institute of Technology (2016). 2016 Emerging Cyber Threats Report.

<sup>234</sup> European Commission (2015). **COM (2015) 192 final**, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions regarding "A Digital Single Market Strategy for Europe" 6/05/2015.

<sup>237</sup> European Commission (2015). **COM (2015) 192 final**, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions regarding "A Digital Single Market Strategy for Europe" 6/05/2015.

<sup>238</sup> The Kosciuszko Institute- European CyberSecurity Journal (2015), Volume 1, Issue 1. Strategic Perspectives on Cybersecurity Management and Public Policies

<sup>239</sup> See European Commission (2013). **JOIN (2013) 1 final**: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

<sup>240</sup> See European Commission (2016). **COM (2016) 410 final**, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry

<sup>241</sup> See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

<sup>242</sup> See Accenture and HfS Research (2016). The State of Cybersecurity and Digital Trust 2016.

<sup>243</sup> See European Commission (2016). **COM (2016) 410 final**, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry

<sup>244</sup> See Carrapico, H., Barrinha, A. (2017). The EU as a coherent (cyber)security actor?

<sup>245</sup> See Christou, G. (2014). The EU's Approach to Cyber Security. EUSC EU China Security Cooperation: performance and prospects. Policy paper series. Available at

<http://privatewww.essex.ac.uk/~susyd/EUSC/documents/EUSC%20Cyber%20Security%20EU%20Christou.pdf>

<sup>246</sup> See interviews

	<p><b>Data processing and analysis.</b> Difficulties arise to identify consequences and lessons learned once an incident has occurred. This is due to the fact that normalisation of data and processes is problematic, as impacts cannot be measured or identified easily. Thus, comparability becomes arduous. Moreover, testing cannot offer guarantee of success.<sup>247</sup></p> <p><b>Lack of data</b> is also an issue as a large number of cyber incidents in the EU go unnoticed due to unwillingness to disclose information.<sup>248</sup></p>
--	---

---

<sup>247</sup> See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at [http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european\\_cyber\\_security\\_policy.html](http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html) Accessed 28 February 2017.

<sup>248</sup> The Kosciuszko Institute- European CyberSecurity Journal (2015), Volume 1, Issue 1. Strategic Perspectives on Cybersecurity Management and Public Policies

European Commission

**Evaluation of ENISA**

Luxembourg, Publications Office of the European Union

**2017** – number pages

ISBN number  
doi:number





doi:number

ISBN number



Brussels, 13.9.2017  
SWD(2017) 500 final

PART 3/6

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF  
THE COUNCIL**

**on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013,  
and on Information and Communication Technology cybersecurity certification  
("Cybersecurity Act")**

{COM(2017) 477 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

## Annex 6: Economic estimates of the policy options for ENISA

This document provides an estimation of the costs related to each of the four options for the future of ENISA. The costs are based on a series of **assumptions** presented below:

- It has been assumed that the Greek government will continue to provide its current financial contribution (of EUR 640,000 per year) for the offices in Greece and that this budget would be sufficient to accommodate extended offices if needed. This assumption concerns Options 1, 2 and 3.
- It has been assumed that the new staff would reinforce the implementation of the current mandate and implement the new tasks foreseen. The calculation was based on the average cost as per category of an employee. For the staff based in Greece a corrective coefficient (79.3%) was applied. For staff based in Brussels, no coefficient applies.

Category of personnel	Standard rate without corrective coefficient
Temporary agent	138.000 €/year
Seconded National Expert	78.000 €/year
Contractual agent	70.000 €/year

- The gradual increase of staff (Option 2 and 3) has been also reflected (e.g. calculation takes into consideration the potential employment date).
- For the calculation of overall costs per option, efforts have been made to take potential synergies with other EU bodies (especially CERT-EU).
- Additional set-up costs might apply, for example, for staff recruitment. This was taken into consideration in relevant options (Option 2 and 3) or additional office costs (Option 3).
- A standard inflation rate of 2% was also applied.

The cost estimations are based on several **sources**:

<ul style="list-style-type: none"> <li>• <b>ENISA evaluation report</b></li> </ul>
<ul style="list-style-type: none"> <li>• ENISA Annual Activity Report 2015.</li> </ul>
<ul style="list-style-type: none"> <li>• Europaid (2017): Current per diem rates. Available at: <a href="https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17_en.pdf">https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17_en.pdf</a>. Accessed 16.06.2017.</li> </ul>
<ul style="list-style-type: none"> <li>• Statista – The Statistics Portal (2016): Rental prices of prime office properties in selected European cities as of 4th quarter 2016 (in euros per square meter per year). Available at: <a href="https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/">https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/</a>. Accessed 16.07.2017</li> </ul>
<ul style="list-style-type: none"> <li>• ENISA (2017): Statement of estimates (budget 2017). Available at: <a href="https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-2017-annual-budget">https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-2017-annual-budget</a>. Accessed 16.07.2017</li> </ul>

The costs estimations for each of the four options are presented below.

### Option 0:

**Baseline, maintain the status quo:** This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation and Telecoms Framework Directive would need to be taken into account. Under Option 0 the minimum scenario assumes that ENISA will be able to take on all new tasks assigned to it as per recent legislative changes (NIS Directive) by reallocating responsibilities and tasks, as it has been done in the 2016 and 2017 Work Programme. The below calculation, however, assumes that ENISA will get another eight staff members (two for each of the key sectors finance, health, transport and energy) to respond to its new responsibilities.

	YEAR 1		YEAR 2 ONWARDS	
	Number of staff/ specification of other costs	Costs in EUR per year	Number of staff/ specification of other costs	Costs in EUR per year
Current budget	84	11,244,679	84	11,244,679
Revise ENISA's mandate to make its new tasks per recent/upcoming legislation more specific	0	676,416	8	676,416
<b>Total budget under the option</b>	<b>84</b> (48 TAs, 31 CAs, 5 SNEs) <sup>1</sup>	<b>11,921,095</b>	<b>92</b> (56 TAs, 31 CAs, 5 SNEs)	<b>11,921,095</b>

### Option 1:

**Expiry of ENISA's mandate** (terminating ENISA): it would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive and bilateral or regional ties at Member State level. The direct costs for the EU budget of not extending the mandate of ENISA in 2020 would be EUR 0, which implies thus a cost saving for the European institutions of approximately EUR 10,332,000 yearly, plus a 2% standard increase per year.

The financing provided by the Government of the Hellenic Republic (which constitutes between 6 and 7% each year), as well as contributions from third countries participating in the work of the Agency (around 1%) were deducted from this estimate.

Please note, however, that some one-off costs related to e.g. re-allocating staff and the removal of infrastructure and all miscellaneous administrative requirements for ending ENISA's activities might need to be incurred in the year following the decision to close down ENISA.

<sup>1</sup> Based on: Multi-annual staff policy plan year 2017-2019, Establishment plan in Draft EU budget 2017, in ENISA Programming document 2017-2019; Annex III

## Option 2

**'Reformed ENISA':** This option would build on the current mandate of ENISA with a view of adopting selective changes which take the evolution of the cybersecurity landscape into account. The Agency would gain a permanent mandate, based on the following key building blocks: support to EU policy development and implementation; capacity building; knowledge and information; market related tasks; research and innovation; and operational cooperation and crisis management.

This option assumes substantial increase of ENISA's resources to reinforce the execution of the current tasks and to implement new tasks. The table below presents the needs of new staff as per the category of tasks.

Tasks	AD	AST	CA	SNE	Total
Policy and capacity building	10	2			12
Operational cooperation	9	2		7	18
Certification (market related tasks)	6	1	7		14
Knowledge, information and awareness	1	2			3
Research and Innovation	2	1			3
<b>TOTAL</b>	<b>28</b>	<b>8</b>	<b>7</b>	<b>7</b>	<b>50</b>

Based on the above needs, the table presents the costs for year 1 and 2 of the introduction of the option 2. The costs are presented differentiating between staff costs (costs due to additional human resources) and “other” costs e.g. infrastructure & operating expenditure as well as for operational expenditure.

ENISA	Baseline 2017 (31/12/2016)	2019	2020	TOTAL
<b>Staff Expenditure</b> <i>(including also e.g. expenditure related to staff recruitment, training, socio-medical infrastructure)</i>	6.387	12.143	14.973	<b>27.117</b>
<b>Infrastructure &amp; operating expenditure</b>	1.770	2.188	2.645	<b>4.833</b>
<b>Operational Expenditure</b>	3.086	5.764	6.078	<b>11.842</b>
<b>TOTAL for ENISA</b>	<b>11.244</b>	<b>20.095</b>	<b>23.696</b>	<b>43.792</b>

## Option 3

**EU cybersecurity agency with full operational capabilities.** This option implies reforming ENISA by bringing together three main functions: 1. A policy/advisory function; 2. A centre of information and expertise, and 3. A Computer Emergency Response Team (CERT). To a large extent this option would imply the same change in the scope of the mandate as option 2. However, additional tasks would be added in the area of incident response and crisis management, so that the Agency would cover the entire cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.

This option assumes substantial increase of ENISA's resources to reinforce the execution of the current tasks and to implement new tasks. It also assumes that a substantial number of new staff would be based in Brussels.

The table below presents the needs of new staff as per the category of tasks.

Tasks	AD	AST	CA	SNE	Total
Policy and capacity building	10	2			12
Operational cooperation (NIS, exercises)	9	2		7	18
Operational support (CERT function)	6	2	6	6	20
Certification (market related tasks)	6	1	7		14
Knowledge, information and awareness	1	2			3
Research and Innovation	2	1			3
<b>TOTAL</b>	<b>34</b>	<b>10</b>	<b>13</b>	<b>13</b>	<b>70</b>

Based on the above needs, the table presents the costs for year 1 and 2 of the introduction of the option 3. The costs are presented differentiating between staff costs (costs due to additional human resources) and “other” costs e.g. infrastructure & operating expenditure as well as for operational expenditure.

ENISA	Baseline 2017 (31/12/2016)	2019	2020	TOTAL
<b>Staff Expenditure</b> <i>(including also e.g. expenditure related to staff recruitment, training, socio-medical infrastructure)</i>	6.387	13.027	17.382	30.409
<b>Infrastructure &amp; operating expenditure</b>	1.770	3.938	4.966	8.904
<b>Operational Expenditure</b>	3.086	5.764	6.078	11.842
<b>TOTAL for ENISA</b>	<b>11.244</b>	<b>22.729</b>	<b>28.426</b>	<b>51.155</b>



Brussels, 13.9.2017  
SWD(2017) 500 final

PART 4/6

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF  
THE COUNCIL**

**on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013,  
and on Information and Communication Technology cybersecurity certification  
("Cybersecurity Act")**

{COM(2017) 477 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

# Table of contents:

---

<b>1. Introduction</b> .....	3
<i>1.1 Methodological approach</i> .....	5
<i>1.2. Data bottlenecks and methodological limitations</i> .....	7
<hr/>	
<b>2. What is the problem</b> .....	8
<i>2.1 Selective evidence on size and costs</i> .....	8
<i>2.2 Root causes</i> .....	10
<i>2.3. Information Asymmetry</i> .....	14
<i>2.3 The Labelling Concept</i> .....	18
<i>2.4. The problem of Fragmentation</i> .....	29
<hr/>	
<b>3. The ICT security certification landscape</b> .....	31
<i>3.1 International schemes and other initiatives</i> .....	31
<i>3.2. National initiatives</i> .....	39
<i>3.3. Main challenges and the need for a EU approach</i> .....	44
<hr/>	
<b>4. Policy objective and intervention logic</b> .....	47
<i>4.1. Policy options</i> .....	48
<b>Option 0</b> .....	<b>48</b>
<b>Option 1</b> .....	<b>50</b>
<b>Option 2</b> .....	<b>50</b>
<b>Option 3</b> .....	<b>50</b>



---

# 1. Introduction

Every day, cybersecurity incidents cause major economic damages to European businesses and the economy at large. Such incidents undermine the trust of citizens and enterprises in the digital society. Theft of commercial trade secrets, business information and personal data, disruption of services - including essential ones - and of infrastructures result in economic losses of hundreds of billions of euros each year.

Cyberattacks are increasing at an alarming pace. The latest ransomware campaign, in May 2017, shows the potentially massive impact of cyber-attack across sectors and countries: more than 150 countries and over 190,000 systems were affected, including those related to essential services such as hospitals. This example is just the last of a series: more than 4,000 ransomware attacks have occurred every day since the beginning of 2016, a 300% increase over 2015. 50 % of businesses in the EU have suffered a cyber-attack and the projected growth of cybercrime is now higher than that of the internet. A recent survey<sup>1</sup> from 2016 revealed that number of security incidents across all industries rose by 38% in 2015, i.e. the biggest increase in 12 years.

Against this background, in its 2016 Cybersecurity Communication, the European Commission announced that, in view of the cybersecurity challenges and the overall effort to step up cooperation and knowledge sharing landscape, it would have advanced the evaluation of ENISA, due by June 2018, and present a proposal for a new mandate, as soon as possible. In particular, the Commission noted that the review of ENISA would provide an opportunity for a possible enhancement of the agency's capabilities and capacities to support Member States in a sustainable manner in achieving cybersecurity resilience by taking into account the agency's new responsibilities under the NIS Directive, new policy objectives to support cybersecurity industry, evolving needs in securing critical sectors, and new challenges linked to cross-border incidents, including coordinated response to cyber crises.

At the same time, the Commission noted that national initiatives are emerging to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Albeit important, these initiatives bear the risk of creating single market fragmentation and interoperability issues. Accordingly, the Commission announced that it would work, among others, on a possible European ICT security certification framework proposal, to be presented by end-2017, and to assess the feasibility and impact of a European lightweight cybersecurity labelling framework.

In the Communication on the Digital Single Market Strategy Mid-term Review, the Commission has further clarified that, by September 2017, it will review the mandate of ENISA to define its role in the changed cybersecurity ecosystem and develop measures on cyber security standards, certification and labelling, to make ICT-based systems, including connected objects, more cyber-secure.

Building on the findings<sup>2</sup> of the public consultation on the contractual Public Private Partnership on cybersecurity and possible accompanying measures, that took place from 18 December 2015 to 11 March 2016, and other technical studies, the following two main problems have been identified with regard to ICT security certification and labelling:

- Citizens' and companies do not have sufficient information concerning the security properties of ICT products and services they purchase
- The emergence of multiple national and sectorial certification schemes causes market fragmentation and barriers to the internal market

To evaluate the needs for policy action in the field of cybersecurity certification and labelling and carry out an impact assessment in light of the Commission's "Better Regulation" guidelines, the Commission needs a study to provide the evidence base needed.

Following a stakeholder consultation held in April 2017 by DG CNECT, the following policy options have been considered and discussed:

- Option 0) *No action*
- Option 1) *Soft law tools*
- Option 2) *SOG-IS agreement mandatory for all EU Member States and extend its membership.*

---

<sup>1</sup> <http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/>

<sup>2</sup> <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-contractual-ppp-cybersecurity-and-staff-working-document>

---

- Option 3) *ICT Security Certification Framework*

In the following chapters of this Interim Report, the results of Task 1 are presented, after a quick recall of the adopted methodological approach. Within this Interim Report will be also summarized the results obtained from the desk research, the interviews with selected and impacted stakeholders and the online questionnaire properly structured by the Consortium. All data gathered will be used for Task 2 in order to duly evaluate and compare the policy options considered by the Commission.

In order to respond to the pressing time-line of the client we have modified the work plan originally presented within the proposal. This Interim Report is developed in accordance with all indications and agreements provided by the Commission during the project development, during the Inception Meeting of May 17th 2017 and in accordance with the Inception Report submitted on 19<sup>th</sup> May 2017. All activities were carried out in close cooperation between the Commission and the Consortium.

The final version of this Interim Report will take into account observations and comments raised by the Commission at the First Interim Meeting and will be made available to the Commission one week after the meeting.

## 1.1 Methodological approach

The European Commission - DG CNECT asked to the Consortium to gather evidence on ICT Security Certification and Labelling in order to assist the development of an Impact Assessment accompanying the foreseen regulation on certification and labelling. The Impact Assessment developed by the European Commission – DG CNECT has been substantiated empirically by the Consortium mainly through additional secondary sources, the use of more granular statistics (by country, sectors, affected groups), and a limited amount of field work. In particular, we have been fleshed out the IA by:

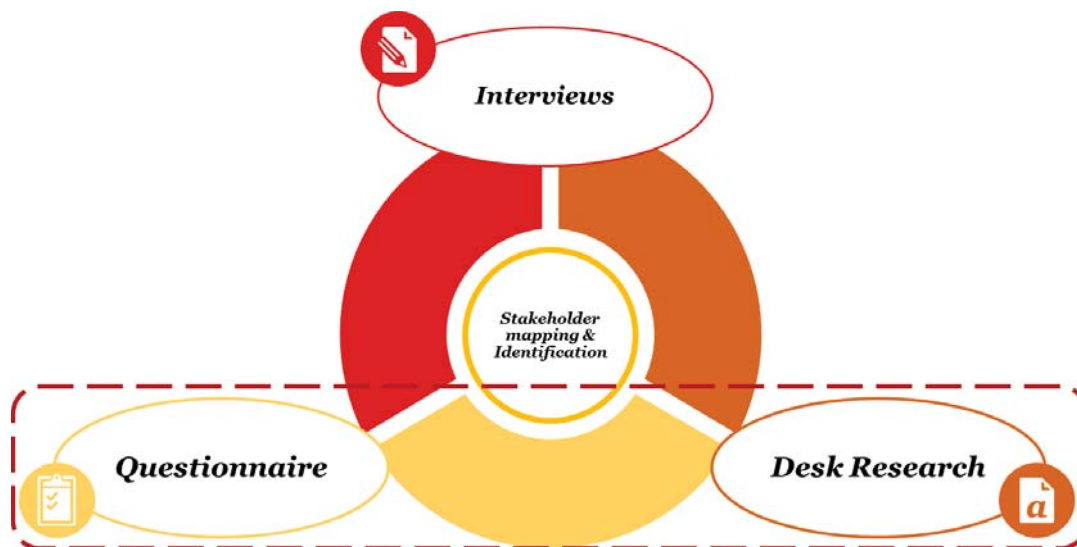
- Mapping all certification and labelling scheme, which enables to further substantiate the definition of the problem, the EU right to act, and the baseline and no action scenarios;
- Further describing and operationalising the policy options and their implications;
- Substantiate the market failures, fragmentation and their costs, including exemplifications and specific cases;
- Attempting to come up with some educated guesses on the different costs and benefits of certification;
- Further developing, commenting, and substantiating the options comparison and ranking

In close cooperation with the Commission, the Consortium will continue to flash out the Impact Assessment developed by the Commission in the same way explained above.

### Methodological triangulation

The methodological triangulation refers to a fully structured and consolidated methodology for triangulating sources and methods, so that this will be a mixed methods study integrating quantitative and qualitative sources and methods.

**Figure 1 Sources and methods triangulation**



Source: own elaboration

---

## Desk Research

Initial overall **desk research** was key for understanding the state of the art, for highlighting the complexities to be addressed and for laying the ground for **a solid methodology which builds over, but does not replicate, existing literature findings**. For this reason, PwC and FUB have been aligned with the EC Team concerning the study, which are currently being undertaken in closely related topics as to avoid overlap in research output. During the desk research activities, the Consortium has analysed all the documents provided by Commission including:

- European Commission Communications and studies
- JRC studies
- ENISA workshops
- Stakeholders consultations and workshops
- Results of ENISA Surveys

In addition to the documentation provided by the Commission, the Consortium has analysed other related and relevant documents from internal or secondary sources as:

- European Commission studies
- ENISA studies
- JRC studies
- Publications
- Stakeholders communications and studies
- Workshops

Moreover, in order to create synergies and not replicate parallel studies that are still ongoing, the Consortium has taken into account all the documentation including:

- IoT and Cybersecurity studies
- PwC studies
- IoT Market Studies
- Cloud Computing study

Other relevant information, evidences and data cost have been extracted through the interviews with selected stakeholders, that will be summarized in **chapter 5**. The desk research activities were also aim to find additional impacted stakeholder. A stakeholder mapping, taking in consideration all the inputs provided by the Commission, resulted fundamental to select the main stakeholder to be interviewed.

## Interviews

Another step of the triangulation methodology was working with DG CONNECT to identify and validate the list of the stakeholders who are directly or indirectly impacted by the project. During the first preliminary meeting, on the 8th of May 2017, has been highlighted by the DG CONNECT Team that surveys have been conducted by **JRC**; this means that a mapping of stakeholders has already been developed. The stakeholders **mapping** has been integrated with the identification of **new selected stakeholder** included in specific and most impacted industrial sectors, taking in consideration the JRC surveys data received and analysed by the Consortium. A detailed stakeholder map has been necessary for identifying experts and participants for the **interviews** organized. The Map was constantly updated and improved during the project running and it is attached within the **Annex 7.3**.

More in particular, the Commission asked to contact National Certification Authorities and some representatives from smart-metering and semi-conductors industries. The Consortium has collected contacts to be interviewed from European Commission – DG CNECT, from internal sources and from online websites of companies and other impacted organisations.

In order to contact directly the selected stakeholders, many phone calls were made to have an appointment, asking also to spread the Questionnaire within the representatives of the Organization. Before any interviews, the Consortium sent by e-mail an interview template to inform the representative interviewed about the topics and the questions that would be later posed during the interview. Many organizations were also contacted only by e-mail with attached the interview template structured by the Consortium.

Once the appointment was scheduled, the interviews were conducted through a conference call with representatives from the organizations involved, representatives from PwC and representatives from FUB.

To this day, **18 representatives** have been interviewed from impacted sectors and national Certification Authorities. More in detail, the stakeholders interviewed are:

Type	Representatives interviewed
National Certification Authority	6
Conformity Assessment Bodies	2
Semi-Conductors Industry	1
Smart-Metering Industry	5
Critical Infrastructures	4

All the Minutes of the Interviews conducted by the Consortium are included within the **Annex 7.1** and all the contributes from stakeholder are also structured in Chapter 5 to convey the different views gathered on different aspects.

### *Questionnaire*

The Consortium has structured an online questionnaire in order to gather additional evidence on ICT security certification and labelling across Europe. The Questionnaire has been put online on 6<sup>th</sup> June 2017 and will remain open until 19<sup>th</sup> June 2017.

The invitation to the Questionnaire has been sent by e-mail to all collected contacts. A detailed map of the stakeholders contacted is presented within the Annex 7.2 "Questionnaire". Within the same Annex, preliminary descriptive statistics of the type of organisations that have completed the questionnaire is presented. More detailed results and analysis of the answers provided will be presented within the next deliverables, after the expiration date of the Questionnaire on 19<sup>th</sup> June 2017. The results of the online questionnaire will also contribute to the data cost analysis. The Questionnaire results will be partly complemented also by **surveys' answers provided by JRC and DG CONNECT**.

## ***1.2. Data bottlenecks and methodological limitations***

A few considerations on data bottlenecks and methodological limitations that apply especially to the products, that will be delivered in five weeks but also more generally to the final products at the end of the five months' project duration.

There are clear bottlenecks in terms of gathering reliable data on certification costs and benefits that have a wide EU 28 coverage. Through secondary sources only some scattered, fragmented, and at times inconsistent figures are available. Some interviews with relevant stakeholders and experts (or a workshop) have been possible to be conducted but the quality of the data obtained will not warrant a full objective quantification. Even within the five months' period, though some more data and qualitative information will be obtained, we will never have a fully robust and representative dataset.

For the above reasons it is important to stress again that: a) the triangulation of sources and methods remains a key pillar of our approach; and b) the assessment of impacts and the comparison and ranking of policy options will have by necessity a mixed quantitative-qualitative nature and will be supported by narrative explanations and justifications.

## 2. What is the problem

### 1.1 Selective evidence on size and costs

As stated in the European Commission (henceforth EC) Communication on Resilience, despite previous initiatives and achievements *'the EU remains vulnerable to cyber incidents. This could undermine the digital single market and economic and social life as a whole'* (European Commission, 2016a, p. 2). The box below reports some selective evidence on cyber incidents dimensions and associated problems and costs.

#### **Box 1 Exemplificative evidence**

##### **Total breaches 2014-2016 (Symantec, 2017)**

- 2014: 1523 (with more than 10 million identities exposed: 11; total identifies exposed: 1.2B);
- 2015: 1211 (with more than 10 million identities exposed: 13; total identifies exposed: 564M);
- 2016: 1209 (with more than 10 million identities exposed: 15; total identifies exposed: 1.1B);
- In the last 8 years more than 7.1 billion identities have been exposed in data breaches;
- It takes two minutes for a IoT device to be attacked.

##### **Global estimates (CSIS, 2014)**

- The likely annual cost to the global economy from cybercrime are estimated in more than \$400 billion;
- Hundreds of millions of people having their personal information stolen cost as much as \$160 billion per year;
- As cybercrime have impacts on export related jobs, Europe could lose as many as 150,000 jobs due to cybercrime or about 0.6% of the total unemployed

##### **Costs to firms (PwC, 2015)**

- The 2015 Information Security Breaches Survey conducted in the United Kingdom showed that 90% of large organisations and 74% of small and medium-sized businesses reported they had suffered from an information security breach;
- For companies with more than 500 employees the average cost of the most severe breach was between €1.86 million and €4.01 million
- For SMEs it oscillated between €95,840 and €397,1675

##### **Hindrances to online activity, (Eurostat data reported in European Commission 2016b)**

- The proportion of internet users having experienced certain common security issues over the internet – such as viruses affecting devices, abuse of personal information, financial losses or children accessing inappropriate websites – stood at 25% in 2015
- Security concerns prevented some internet users in the EU from doing certain activities over the internet: almost 1 in 5 did not shop online (19%) or did not carry out banking activities (18%) in 2015, and 13% of them did not use the internet with a mobile device via wireless connection from places other than home.
- Notably, more than 1 internet user out of 5 did not buy or order goods or services on-line for private use due to security concerns

##### **Skill shortage and risk of know-how out flow (Friedman 2015; ISACA, 2015; Optimity Advisors, 2015)**

- The Global Cybersecurity Status Report indicates an alarming shortage of skilled cybersecurity professionals around the world
- According to different estimates the demand for the cybersecurity workforce will rise to 6 million globally by 2019, with a projected shortfall of 1 - 1.5 million
- The situation is similar in Europe where, although academic organisations are educating highly qualified and trained cybersecurity professionals, this talent is many a time not absorbed by the European cybersecurity market;
- Given barriers to growth of European cybersecurity companies, this could result into an outflow of knowhow from Europe

##### **Hindrances to Open and Big Data Economy**

- The potential for data-driven innovation, provided cybersecurity is achieved, is a two-fold source of economic growth (OECD, 2013). First, directly as a new market with great economic potential of generating revenues by itself; Second, as a way of increasing efficiency and reducing administrative bottleneck;
- In the EU, if all framework conditions were in place, the EU data economy could increase up to EUR 643 billion by 2020 to EUR 272 billion in 2015 ;

---

Even the smallest estimates of cybercrime costs to the global economy are larger than the national economy of some countries, while governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow. The most important cost of cybercrime<sup>3</sup>, however, comes from its damage to company performance and to national economies.

Cybercrime hinders trade, competitiveness, innovation, and global economic growth. The first largest source of direct loss from cybercrime is the theft of intellectual property. In fact, companies invest substantial amount of money in research and development (R&D) to create new intellectual property (IP). One UK Company told British officials that it incurred revenue losses of \$1.3 billion through the loss of intellectual property and disadvantages in commercial activities. Anecdotal evidence about IP theft come from every major economy (CSIS 2014).

According to the OECD Digital Economy Outlook 2015 (2015), 'ransomware' is rising as a prominent challenge among digital security issues. Experts estimate that "CryptoLocker infected some 234 000 computers during its first two months alone, before being disrupted by a multinational law enforcement effort, involving Canada, Germany, Luxembourg, the Netherlands, Ukraine, the United Kingdom and the United States"

The 'threat landscape' continues to evolve, sustained by often profitable business models. For example, one of such models is based on 'ransomware, which is a type of file-encrypting malware increasingly deployed by cybercriminals to encrypt the computer files of an organisation or individual, who must then make a payment (i.e. the "ransom") in exchange for decryption of their files.

The most prominent strain of ransomware is "CryptoLocker", which is spread via email attachments. Experts estimate that "CryptoLocker infected some 234 000 computers during its first two months alone, before being disrupted by a multinational law enforcement effort, involving Canada, Germany, Luxembourg, the Netherlands, Ukraine, the United Kingdom and the United States". In addition, cyberattacks leading to data breaches where the personal data of millions of European individuals in the EU get compromised have become more and more common in the recent years.

Similarly, to the business model behind ransomware, the breached company could be requested to pay a sum of money to the attackers in exchange for not publishing the data online. This type of incidents can have a direct impact on citizens in the form of e.g. identity theft or financial fraud (stolen credit cards) directly impacting the trust in the Digital Single Market (DSM).

ISACA (2015) conducted a global survey<sup>4</sup> of 3,439 business and IT professionals in 129 countries to capture their real-time insights on cybersecurity attacks, skills shortages finding that 86% of respondents see a global cybersecurity skills gap—and 92% of those planning to hire more cybersecurity professionals this year say they expect to have difficulty finding a skilled candidate. The survey also found that 83% of respondents say cyberattacks are among the top three threats facing organizations today, and only 38% say they are prepared to confront such threats. Moreover, 86% of respondents believe there is a shortage of skilled cybersecurity professionals. 48% of respondents are equally concerned about physical attack (e.g., terrorist attack or act of war) and cyberattacks.

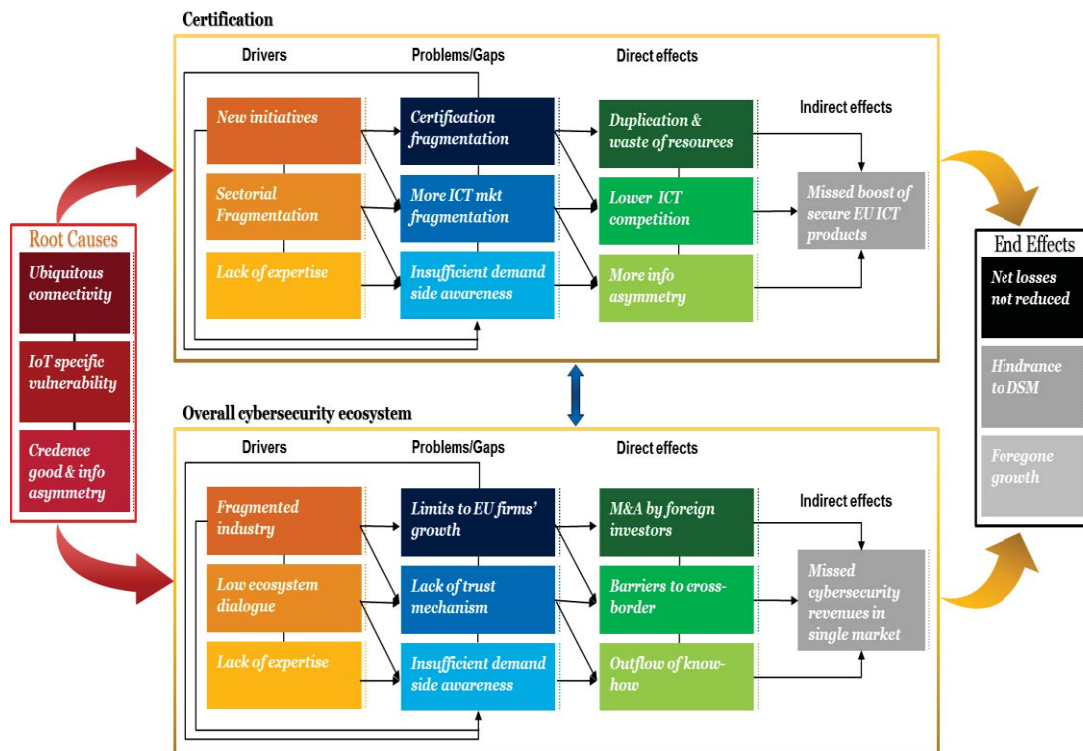
---

<sup>3</sup> Symantec. (2017). Internet Security Threat Report: Volume 22, Symantec.

<sup>4</sup> ISACA. (2015). 2015 Global Cybersecurity Status Report: ISACA

In the picture below, we present a problem tree where effects are framed as foregone opportunities.

**Figure 2 Problem tree**



Sources: own elaboration based on EC sources (European Commission, 2016a, 2016b, 2016c, 2016d), and on various studies (Baldini et al., 2017; ECORYS, 2011; ERNCIP, 2014; IDC, 2009; Optimity Advisors, 2015)

## 1.2 Root causes

**Universal ICT usage increase ‘surface attacks’.** Among the root causes or the increasing risk for, and occurrence of, cyber incidents there is the simple fact that the Internet and the cyberspace have become ever more important and are the backbone of our digital economies and societies. ICTs have become widely available to the general public, both in terms of accessibility as well as cost<sup>5</sup>. A boundary was crossed in 2007, when a majority (55 %) of households in the EU-28 had internet access. This proportion continued to increase, passing three quarters in 2012 and four fifths in 2014. In 2016, the share of EU-28 households with internet access rose by two additional percentage points compared with 2015 to reach 85 %, 30 percentage points higher than in 2007. Widespread and affordable broadband access is one of the means of promoting a knowledge-based and informed society. Broadband was by far the most common form of internet access in all EU Member States: it was used by 83 % of the households in the EU-28 in 2016, approximately double the share recorded in 2007 (42 %).

<sup>5</sup> [http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital\\_economy\\_and\\_society\\_statistics\\_-\\_households\\_and\\_individuals](http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals)

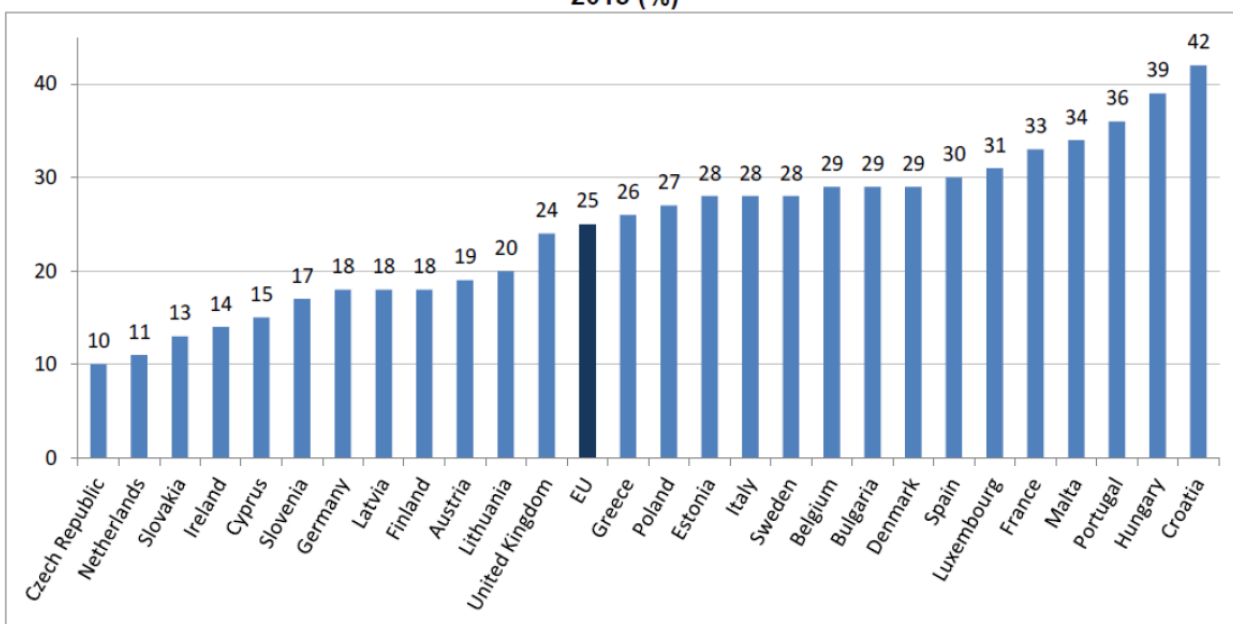


**Figure 3 Cyberspace as backbone of digital economy and society**



Source: European Commission (2016b, p. 3)

**Share of internet users who experienced security related problems in the EU Member States, 2015 (%)**



Romania: data not available

Source: Eurostat

Security concerns prevented some internet users in the EU from doing certain activities over the internet: almost 1 in 5 did not shop online (19%) or did not carry out banking activities (18%) in 2015, and 13% of them did not use the internet with a mobile device via wireless connection from places other than home. Notably, more than 1 internet user out of 5 did not buy or order goods or services on-line for private use due to security concerns in Romania (35%), Sweden (34%), Portugal (30%), France (29%), Spain and Latvia (both 28%), Finland (27%), Italy and Malta (both 25%), Slovenia (24%), Denmark (22%) and the Netherlands (21%). Just as consumers, who take advantage of digital opportunities, businesses across Europe also largely depend on smoothly running information systems. This concerns not only the organisations, whose business model is based on online activity such as e.g. e-commerce platforms, but practically all types of businesses as the use of information and communication technologies influences the way that enterprises are run, information shared with partners and customers. Increasingly public and private sector business entities have the core business, operational critical data and "digital assets of their operations" in digital form, implemented by various ICT systems customer relation management, applications, services and operations (e.g. customer relationship management, supply chain management or enterprise resource planning). According to the survey on information and communication technology (ICT) usage in enterprises, only 3% of enterprises in the EU 28 do not have access to Internet. According to the **2015 Eurostat survey on ICT** usage in enterprises, the awareness among European enterprises related to cyber threats and the need to have a proper ICT security policy is growing, though there is still much room for improvement. In 2015, almost one out of three enterprises in the EU 28 had a formally defined ICT

security policy. The share of large enterprises with such a policy was almost three times the share of small ones.

**Surface attack increased and vulnerability amplified by IoT.** The vulnerability is amplified by the fact that various sectors and industries heavily depends on ICT components and by the interdependence between current and future infrastructures (e.g. in smart cities environments, connected cars, energy smart grids). According to a recent report based on a Global IoT Executive Survey<sup>6</sup> on the impact of the IoT on companies around the world (Business Insider, 2017), the Internet of Things (IoT) is disrupting businesses, governments, and consumers and transforming how they interact with the world. Companies are going to spend almost \$5 trillion on the IoT in the next five years — and the proliferation of connected devices and massive increase in data has started an analytical revolution. According to this report, there will be 22.5 billion IoT devices in 2021, up from 6.6 billion in 2016 and \$4.8 trillion in aggregate IoT investment between 2016 and 2021. As pointed out in the latest BITAG (Broadband Internet Technical Advisory Group) unanimous report<sup>7</sup> (BITAG, 2016), the IoT and has brought with it new security and privacy risks. The number and diversity of consumer IoT devices is growing rapidly; these devices offer many new applications for end users, and in the future will likely offer even more. Many IoT devices are either already available or are being developed for deployment in the near future, including: sensors to better understand patterns of daily life and monitor health; monitors and controls for home functions, from locks to heating and water systems; devices and appliances that anticipate a consumer’s needs and can take action to address them (e.g., devices that monitor inventory and automatically re-order products for a consumer). The same report points out that if IoT devices are compromised by malware they can become a platform for unwanted data traffic — such as spam and denial of service attacks — which can interfere with the provision of these other services. It also reports evidence that some devices do not abide by rudimentary security and privacy best practices. In some cases, devices have been compromised and allowed unauthorized users to perform surveillance and monitoring, gain access or control, induce device or system failures, and disturb or harass authorized users or device owners. Risks are linked to: lack of IoT supply chain experience with security and privacy; lack of incentives to develop and deploy updates after the initial sale; difficulty of secure over-the-network software updates; devices with constrained or limited hardware resources (precluding certain basic or “common-sense” security measures); devices with constrained or limited user-interfaces (which if present, may have only minimal functionality), and devices with malware inserted during the manufacturing process. With the IoT millions of devices are connected, which in jargon means that the ‘attack surface’ widely expands. Critical infrastructures, such as for example electricity generation plants or transportation systems, are controlled and monitored by Industrial Control Systems (ICS), including SCADA (Supervisory Control and Data Acquisition) systems. Today ICS products are mostly based on standard embedded systems platforms and they often use commercial off-the-shelf software. In particular, some sectorial industries such as transport, energy, health, and others do not have a solid and reliable scheme providing them assurance on the level of security of ICT components integrated into their systems (European Commission, 2016b, p. 10).

**Figure 4 The potential reach of cyber incidents**



Source: European Commission (2016b, p. 4)

<sup>6</sup> <http://www.businessinsider.com/the-internet-of-things-2017-report-2017-1?IR=T>

<sup>7</sup> BITAG. (2016). Internet of Things (IoT) Security and Privacy Recommendations. A Uniform Agreement Report: BROADBAND INTERNET TECHNICAL ADVISORY GROUP (BITAG).

---

For these reasons, ICT embedded systems and the IoT are by themselves a new source of vulnerability and are placed in our problem tree among the root causes.

ICT products as computers or smartphones are often replaced regularly and this ensure a certain degree of security. Instead, ICT system are not replaced so often and, under the Directive for the security of networks and information systems (NIS), operators of critical infrastructures will be required to invest in their overall security in order to comply with the NIS Directive. However, not all IoT applications (e.g. smart home appliances) are linked to critical infrastructures and for those use cases, NIS directive would not be applicable.

**Lack of full users' awareness due to information asymmetry.** The third root cause has to do with the particular nature of cybersecurity as a 'credence good' and the implications in terms of information asymmetry. In order to shed light on this aspect it is useful to make the analogy with the various experiments and studies<sup>8</sup> conducted in the domain of environmental impact of home appliances and cars<sup>9</sup> (Codagnone et al., 2013; Codagnone et al., 2016). The "greenness" of a dishwasher or of a car are 'credence' goods; consumers cannot ascertain their environmental qualities during purchase or use. They are not present during the production process of the product and therefore cannot observe environmental friendliness of production. The objective of eco-labels based on certification standards and requirements is to reduce information asymmetry between the producer of green products and consumers by providing credible information related to the environmental attributes of the product and to signal that the product is superior in this regard to a non-labelled product. The implicit goal of eco-labels is to prompt informed purchasing choices by environmentally responsible consumers. This same reasoning applies to the cybersecurity ecosystem and in this respect a common certification framework and a lightweight labelling scheme may greatly reduce information asymmetry and increase demand-side awareness.

As more connected home devices enter the market at different price points, devices such as home security systems, smart thermostats and baby monitors are shifting from "nice to have" accessories to necessary gadgets. With every connected home device purchase, consumers are unknowingly providing hackers with new avenues to launch their attacks. In some instances, poor consumer security habits and vulnerabilities in connected devices are letting hackers into consumers' homes. According to 2016 Norton Cyber Security Insights Report<sup>10</sup>, Fifty-one percent of consumers think it's becoming harder to stay safe and secure online than in the real world and one in five connected home device users don't have any protective measures in place for their devices. Over six in 10 (62 percent) consumers said they believe connected home devices were designed with online security in mind. However, Symantec researchers identified security vulnerabilities in 50 different connected home devices ranging from smart thermostats to smart hubs that could make the devices easy targets for attacks. Data show that there is a clear information asymmetry between designers and vendors on one side, and customers/users of ICT solutions on the other.

The UK government document "Using behavioural insights to improve the public's use of cyber security best practices"<sup>11</sup> provided by the UK government, it is argued that there is a considerable gap between what is currently known and what needs to be understood in order to address the cyber security behaviours of individual internet users. For instance, users report awareness and concerns about security but in practice never change privacy default settings and leave their devices always on and online.

There is certainly a need for good communication within the cyber security user community and a lack of knowledge and skills remains a problem. The '*provide information and they will use it*' approach does not appear to be effective in spreading the message fully or widely enough. It could be argued that communication should be through more diverse methods than a passive web page and key messages should be proactively pushed to the most relevant user communities. We know that interventions that rely solely on knowledge transfer may struggle. Even if people do find and read the information, behaviour change theories would tell us that while information is necessary it is not sufficient and the other influencers are important. Any knowledge-based intervention is more likely to be successful if other influencers, highlighted in behaviour theories are incorporated into the intervention – designing the right defaults; creating a security culture; having champions and opinion leaders etc.

---

<sup>8</sup> Codagnone, C., Veltri, G. A., Bogliacino, F., Lupiáñez-Villanueva, F., et al. (2016). Labels as nudges? An experimental study of car eco-labels. *Economia Politica*, 33, 403-432.

<sup>9</sup> Codagnone, C., Bogliacino, F., & Veltri, G. (2013). Testing CO2/Car labelling options and consumer information. Final Report. Brussels: European Commission

<sup>10</sup> <https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf>

<sup>11</sup> <https://www.gov.uk/government/publications/cyber-security-using-behavioural-insights-to-keep-people-safe-online>

---

## 2.3. Information Asymmetry

There are three classical market failures that according public economics warrant a policy or regulatory intervention: a) externality; b) market power; and c) information asymmetry. There can be no doubt in the fact that the cybersecurity market is currently affected by a clear case of information asymmetry; it is an information asymmetry that is particularly acute both because of the technicalities of the topic and because of fragmentation in certification scheme.

The security properties of a software product are a quality dimension, which is difficult to assess for an end user prior to purchase, at least not at a justifiable cost. In this situation, the market fails to provide optimal resource allocation. Consider a vendor A selling a product with desirable quality features (in this case strong security) and a vendor B selling a product without the desirable features (i.e. with weak or no security). Vendor A cannot reap the benefits of better quality because vendor B has lower costs and can therefore offer his product at a price which is prohibitively low for vendor A. As the customers cannot tell the difference due to the information asymmetry, they will buy from vendor B. This initiates a race to the bottom with regard to the desired quality property. This is commonly called a “market for lemons” referring to the seminal paper of Akerlof (1970).

This argument, however, can be further reinforced by an ongoing debate in the public and behavioural economics literature on whether or not the limited rationality, heuristics and biases that characterise the behaviour of both citizens and businesses as consumers may represent a fourth type of market failure lending further supports to policy or regulatory intervention (for a review of this debate see Lunn, 2015). Whereas the resolution of this ongoing theoretical and normative debate is yet to come, it is worth exemplifying the cognitive and behavioural limitations affecting both consumers and businesses when dealing with cybersecurity. There is no single behaviour that can keep people secure online, but rather cybersecurity requires multiple interrelated behaviours, and each one is potentially influenced by different factors. The cognitive load on final users is heavy and many times they do not behave safely. This applies equally to consumers and businesses:

- Home users and small companies may lack the required expertise to set up the technical defences. Often, security is managed by an individual as one part of their overall role who may rely on help from family and friends, rather than an external specialist company. The worst-case scenario is small companies having no in-house staff being responsible for cyber-security.
- Company employees may not follow the cyber-security policies put in place by the company;
- Many do not perceive a risk. Small businesses believe they are safe from cyber threats, even though they have no policy or ways of knowing if this is the case. A National Cyber Security Association (NCSA) survey of small businesses in the US, conducted in 2012, suggested a cyber security disconnect where 77% of companies believed their company was safe from cyber threats and 47% believed a data breach would have no impact on their business, yet 87% did not have a formal written Internet security policy and 69% did not even have an informal one. Finally, 18% said they would not even know if their computer network was compromised.

There are behaviours that increase the risks

- Always being connected has become both a habit and an expectation - The need to be connected at that place/at that time outweighs risk of insecure connection or interacting in a public space. For instance, in 2017, people in Italy spend an average of 6 hours per day on internet (through both laptops and mobile phones). In other countries, such as UK, France, Spain, Poland and Germany, the average ranges between 4h30 and 5h45<sup>12</sup>.
- People are habituated to the “I accept” button and warning messages – do not read what they are agreeing to or think about the consequences of their behaviour, just click. They do not always make

---

<sup>12</sup> <https://wearesocial.com/special-reports/digital-in-2017-global-overview>

---

rational, thought through decisions. 73% of the people admit of not reading the whole fine print and only 17% of those who did understand it.<sup>13</sup>

- Convenience (or taking the easy way) always wins over security. An example of this could be a basic action like setting a password. Practices such as sharing a passwords and using the same ones on multiple platforms is still very common among individuals, even though it is highly recommended not do so.<sup>14</sup>
- Desirability wins over security – the desire to be connected, to download applications, music, video etc., to share information with people online. To do this at no expense or simply for information is also desirable. The Data-for-Access trades are in fact based on the desire and the convenience of being connected but at the cost of sharing private and sensitive information.<sup>15</sup>
- Financial costs do not justify security gains - security software is expensive, software upgrades are expensive. A recent investigation by the Polytechnic University of Milan's Information Security & Privacy Observatory<sup>16</sup> stresses that only 39% of large businesses have enacted a multi-year investment plan, and only one out of every two organizations has managers dedicated to these tasks. This is a precarious situation, with potential consequences not only for their offices but for the factories too, where modern machinery has become increasingly connected and dependent on the ability to gather, transmit, and analyze data. Companies often find it difficult to understand the benefits or gains of major investment in cyber security.
- Incentives for insecure behaviour mean that security risks are ignored– cost benefit analysis in favour of insecure behaviours (desire for immediate, concrete gain versus potential abstract risk in future). Especially Small Business do not perceive themselves as possible victims of cyber threats and therefore do not invest in cybersecurity measures.<sup>17</sup>
- Effort required is too high – to understand how to use the different tools, to keep up to date, to log in, to remember passwords, to complain. As a study from the National Institute of Standards and Technology (NIST) reports, individuals often deal with “Security fatigue” due to the many and various cybersecurity procedures that they have to follow.<sup>18</sup>
- No perceived benefit – belief that behaviours will not make a difference to security. Cybersecurity measures need to be constantly updated in order to face new possible cyberattacks. Because of this necessity, it is commonly believed that the companies that have not been hacked have not discovered it yet.<sup>19</sup>
- No perceived risk or risks downplayed - people justify their behaviours, e.g. being on an insecure connection for a short time is safe, personal information is not of value or simply thinking that attacks will not happen. For this reasons, illegal streaming websites<sup>20</sup> and social media are hackers' favourite target because people do not perceive them as not secure.<sup>21</sup>

---

<sup>13</sup> <https://www.theguardian.com/commentisfree/2014/apr/24/terms-and-conditions-online-small-print-information>

<sup>14</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4291202/#B1>

<sup>15</sup> <https://www.forbes.com/sites/marymeehan/2015/03/17/how-much-of-your-private-data-are-you-willing-to-share/#7d04406e3530>

<sup>16</sup> <http://www.italy24.ilsole24ore.com/art/business-and-economy/2017-05-29/cybersecurity-171538.php?uud=AEX5bAVB>

<sup>17</sup> <https://staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity>

<sup>18</sup> <https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly>

<sup>19</sup> <http://hbswk.hbs.edu/item/target-s-expensive-cybersecurity-mistake>

<sup>20</sup> <https://www.netnames.com/insights/blog/2016/02/the-dangers-of-illegal-streaming/>

<sup>21</sup> <https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/>

- Do not perceive need for change – Lack of belief that negative consequences will result from noncompliance. The longer a person uses the internet with no negative consequences, the less they believe they are susceptible to risk.
- Lack of knowledge and skills – knowledge about what to do and how to do it, and skills to detect fraudulent activity. People must constantly update this knowledge. The [Frost & Sullivan 2015 \(ISC\) Global Information Security Workforce Study](#) lays bare the scale of the cyber security skills shortage, demonstrating that while demand for security professionals is growing, the supply of these professionals is not able to keep pace. The report estimates a global shortfall of 378,000 information security staff today, a figure that is projected to increase to 1.5million by 2019. Echoing these findings, [Harvey Nash's 2015 CIO Survey](#) found that 23 per cent of CIOs report a skills shortage in security and resilience and that only around a quarter (23 per cent) feel that they are very well prepared for a serious cyber security incident<sup>22</sup>.
- Do not know which information to trust - who are the credible sources, who do you believe when different people make conflicting recommendations.
- Simply forget to behave securely when distracted by other things when online.
- Social etiquette – it is a sign of trust/intimacy to share information including passwords and devices.

The certification, however, is only a signalling mechanism, if the criteria actually represent the desired property of the certified product, i.e. whether they are meaningful or not<sup>23</sup> (Schierholz & McGrath, 2010). A buyer needs to be able to assess whether the criteria match his needs. Usually this can only be achieved if the criteria are transparent to the buyer or even publicly available. However, the challenge remains to create a meaningful set of criteria applicable to a broad enough number of buyers to create a sufficient market for certified products. Testing a given product for vulnerabilities can only produce relatively short-lived test results, as attackers and security researchers continuously discover new ways of attacking systems and vulnerabilities in components used in products and systems (i.e. operating systems and applications). Thus, the test cases for certification have to be updated very frequently and for a product that has passed certification last month, today there may be a dozen known vulnerabilities and exploits. Lifecycle considerations Nowadays it is commonly accepted that the threat landscape is continuously changing and that target systems need to react to this change. One example is the significant number of researchers that search for vulnerabilities in products to which vendors react by publishing updates to their products. A change to the product however invalidates the certificate and therefore requires a re-certification (incl. the time delay and additional cost associated with this). This puts an end-user organization which mandates certified products into the dilemma of either sticking to their policy of using certified products only versus fixing a known issue in their system. Similarly, product vendors are in a dilemma. They have to choose between fixing a known issue and loose certification for the latest release of their product (at least until re-certification can be achieved) or not fixing a known but maintaining the product certification (which again points out the limited meaningfulness of product certification). However, there are multiple points often criticized about security certification and the criteria against which certification happens, among them are lack of publicly accessible, standardized certification criteria and processes, meaningfulness of the results (or rather lack thereof) and cost of certification. Also The German Association of Electric Manufacturers, while recognising that in the domain of ICT certification product characteristics remain hidden and are not fully transparent, points out that there are multiple aspects often criticized about security certification and the criteria against which certification happens, among them are lack of publicly accessible, standardized certification criteria and processes, meaningfulness of the results (or rather lack thereof) and cost of certification<sup>24</sup> (ZVEI, 2017) .

At any rate, empirical evidence shows that there is still and awareness and information gaps among the final users of ICT products about security. The study conducted by IDC EMEA on "The European Network and

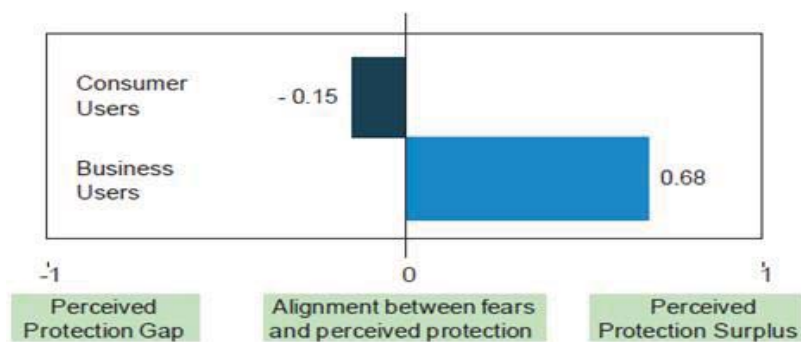
<sup>22</sup> <http://www.apmg-international.com/en/news-events/542074.aspx>

<sup>23</sup> Schierholz, R., & McGrath, K. (2010). Security Certification – A critical review. ABB by DHS.

<sup>24</sup> ZVEI. (2017). Benefits and limitations of certifications and labels in the context of cyber security: German Electrical and Electronic Manufacturers' Association (ZVEI)

Information Security Market”<sup>25</sup> (IDC, 2009), developed the Trust and Confidence Gap Indicator, which measures the gap between business and consumer users’ fears of main security threats, and the perceived level of protection, thanks to the use of security solutions. The indicator varies between –1 and +1. When fears are higher than the perceived protection there is a protection gap (indicator from 0 to –1); when perceived protection is higher than fears there may be a protection surplus (indicator from 0 to +1). According to this study, business and consumer users show a similar, moderate level of fear of main security threats (described by the statement “I am somehow worried”). The level of perceived protection instead is higher for businesses than for consumer users, but this is more due to lack of awareness than real implemented protection measures. Firstly, business users rarely systematically assess their security risks and damages in case of security breaches, so the perceived protection is more often based on assumptions than specific facts and assessments. In fact, the business demand survey calculated by the study shows a lack of correlation between the level of perceived protection and the frequency of security breaches.

**Figure 5 IDC trust and confidence Gap Indicator, EU average**



NOTE: The indicator measures the difference between the average rating of perceived protection and the average rating of fear of IT security threats. It varies between +1 and -1.

Source: IDC (2009)

The Trust and Confidence Gap Indicator for EU Consumers is slightly negative with an average level of –0.15, pointing out that consumers perceive a protection gap against the main security threats. The confidence gap affects particularly two main security threats, the abuse of personal information and children accessing inappropriate websites. On the contrary, exposure to a virus is the only case in which perceived protection exceeds fears. Internet users are not so optimistic about spamming, which is rated low in terms of fears but a lot lower in terms of protection, meaning that there is not much confidence in solutions able to solve this problem. It is not unlikely that many users simply accept Spam as an unavoidable, but unwanted, consequence of being online.

<sup>25</sup> IDC. (2009). The European Network and Information Security Market Brussels: Report delivered by IDC for the European Commission.

## 1.3 The Labelling Concept

As illustrated in a DG SANCO report<sup>26</sup> (European Commission, 2006), Labelling is an important market tool which should be viewed as an integral part of communication between societal players (business to consumers, directly and via intermediaries, authorities to consumers, etc.). Labelling is no longer the only reliable route for communicating information to the consumer, as it once was, but it remains an effective tool. The benefits of consumer information in general and labelling in particular are clear. For the consumer, it provides the means for the operator to pass on essential information about products (use-by dates, safety warnings, etc.) as well as information which, perhaps not being essential, is still considered useful (nutrition labelling, recycling details, etc.). As such, the label allows the consumer to make an informed choice at the point of sale about whether to purchase a product and, if they do so, to consider how best it should be used. For the industry, labelling is a powerful tool which, when used effectively and responsibly, not only ensures the operators provide essential information, but also enables them to highlight the benefits of their products when compared to those of their competitors<sup>27</sup>. This is even more of an important factor if there are additional costs in providing these benefits and the operator needs to convince the consumer to pay a higher price with respect to competing products on the market. Indeed a sociological study<sup>28</sup> carried out in Europe revealed that a lack of labelling on production methods was preventing consumers from possibly shifting towards such products. However, although labelling should be a win-win situation for both the consumer and operator, in practice there is often a market failure and many stakeholders would argue that labelling schemes are not living up to their full potential. Simply put, consumer use of labels is inconsistent and the effectiveness of labelling as a communication tool can be questioned. The reasons for this failure are varied, but perhaps start with a simple lack of consumer interest in the information a label provides. Even if the consumer is interested, many find using labels difficult as they contain too much information, much of which is not understood, is confusing and is poorly presented.

The concept of applying a label on a product after a successful security certification is not new, as the EAL certificates from common criteria, the IACS (ERNICIP 2014), the four levels of FIPS can all be related to a labelling scheme, which gives an indication on the level of security protection or trust of a system (Baldini, et al., 2017). The critical task is how to associate the labels in a harmonized way across different certification schemes, protection profiles and so on. In France, the ANSSI has defined a label system for trusted products and service providers. The labelling concept could be extended to cover not only the traditional levels of Common Criteria (EAL), but to address specific security functions, which can be linked to specific protection profiles. For example, labels could be defined for specific security properties like confidentiality, integrity and authentication or for a specific Security Target (ST), which is defined in the related protection profile.

We can define different dimensions for which the label can be defined:

1. Level of assurance. This is the equivalent of the EAL in Common Criteria. We note that EAL level does not measure the security of the system itself, it simply states at what level the system was tested.
2. Protection profile for a specific domain (energy, road transportation and so on). Each protection profile can be associated to a specific level of assurance (dimension 1). Each domain has its own specific features and configuration environment, which must take in consideration for the security certification and deployment. For example, the security certification of a crypto-module for the road transportation may not be valid for the energy sector. This is why, the label must have a separate dimension to identify the domain.
3. To define how the certification was achieved: self-certification, third-party compliance assessment and so on how it is defined for IACS in section 3.3.1.

<sup>26</sup> [https://ec.europa.eu/food/sites/food/files/safety/docs/labelling-nutrition\\_better-reg\\_competitiveness-consumer-info\\_en.pdf](https://ec.europa.eu/food/sites/food/files/safety/docs/labelling-nutrition_better-reg_competitiveness-consumer-info_en.pdf)

<sup>27</sup> [https://ec.europa.eu/food/sites/food/files/safety/docs/labelling-nutrition\\_better-reg\\_competitiveness-consumer-info\\_en.pdf](https://ec.europa.eu/food/sites/food/files/safety/docs/labelling-nutrition_better-reg_competitiveness-consumer-info_en.pdf)

<sup>28</sup> “Consumer concerns about animal welfare and the impact on food choice”. EU FAIR-CT36-3678. Dr Spencer Henson and Dr Gemma Harper, University of Reading.

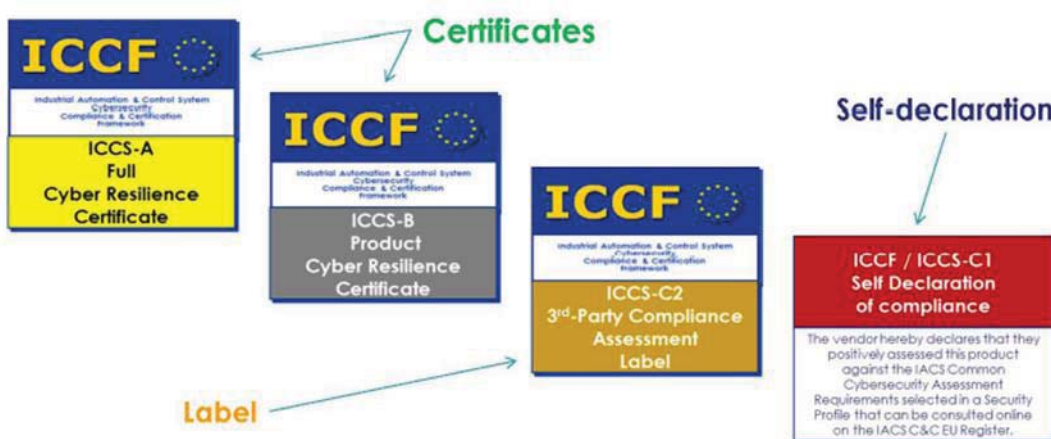


## The IACS scheme

The ICCF proposes (Thales, 2016) four possible approaches to certification in the form of four “schemes” named IACS Cybersecurity Certification Schemes (ICCS). The following diagram recapitulates these four schemes.



Definitions follow and the labels proposed for marking certified products, i.e. those that passed the evaluations with success, are presented in regard of each scheme. These graphic marks are only indicative and will need to be further validated and elaborated during the second phase of this feasibility study (to take place in 2017).



**Example: Mark “ITC certified quality”**<sup>29</sup> ITC has been providing professional services in the field of testing and certification for more than 15 years. The project of the new “ITC certified quality” mark is intended for producers and distributors that seek careful assessment of products and confirmation of their above standard properties by an independent accredited body. **Unlike common certification, the product quality and safety information reach directly the final consumer through this mark.** Continuous supervision of the product quality and safety throughout its sale provides a high degree of assurance that the product will keep its declared standard verified by the certificate. The objectives are:

- Providing information about higher level of product safety and quality to distributors and consumers;
- Marketing support of quality products on the expense of products meeting only the minimum legislative requirements;
- Visible information about successful product certification, which assessed conformity to the specified legislative and technical requirements.
- Guarantee of continuous safety and quality compliance of the products provided with ITC mark;

<sup>29</sup> <http://www.itczlin.cz/en/certified-quality>

- Support of communication between clients and suppliers in the field of competitive products with high standard of safety and quality.
- The mark is determined for placing on products, documents and in publications, where it shows conformity of the product properties to above standard requirements specified by a standard, specification or any other suitable document, while meeting all legislative requirements.

Industry associations have, however, expressed reservations on the applicability of a labelling approach in the domain of ICT security certification (see for instance: ZVEI, 2017; DIGITALEUROPE, 2017). Cyber security will be used across the board in the Internet of Things and will serve as a distinguishing feature. An excessively narrow and static certification and labelling system may actually restrict the range of technical security solutions, particularly if it does not only outlines the requirements but also the implementation measures. This prevents innovation and market diversity. In particular, the differences from energy efficiency labelling and security certification are stressed. The state of science and research clearly shows that cyber security cannot be measured using conventional means. The conditions change too quickly and, as a consequence, the requirements may no longer be met in the time between certification and product launches. In the case of cyber security, in/for the product this is equally dependent on the technical properties, processes, user competence, deployment environment and implementation within the overall system. This clearly distinguishes cyber security from energy efficiency, which is illustratively printed on relevant products in the form of a traffic-light label. Because of the existing design and methodical discrepancy, this approach cannot be applied to cyber security. Support the transfer of international security industry standards: in the area of cyber security, the international security standard IEC 62443 is concerned with requirements for technical aspects of products (through the security level) and process-organisational aspects of the company (through the maturity level), and combines these into an holistic approach (through the protection level). In particular, the approach discussed above is taken into account by means of process observation instead of product certification. This procedure has gained acceptance and agreement for numerous industrial applications across different sectors. It may therefore be possible to transfer the approach to other sectors. DIGITALEUROPE believes any future actions by policy makers in the field of cybersecurity certification and labelling should take into consideration the following criteria:

- **Cybersecurity is a global issue and requires international solutions** - Cyber-attacks know no borders and therefore standards and related certifications play a significant role in creating a safer ICT environment. In the last few years, various and not fully coordinated certification initiatives are increasing the problem of fragmentation across Europe. The lack of an EU wide approach for ICT Certification means that different Member States are developing their own National Certification Scheme with different cybersecurity requirements, different level of tests and different level of assurance. Germany, France and UK have developed their own National Certification Scheme and each certification scheme is not mutually recognised by each other, creating additional market barrier. Other emerging initiatives come for example from Italy, Netherlands, Norway and Sweden. In Italy, based on the national decree DPCM 17 February 2017<sup>30</sup>, it should be established a National evaluation and certification centre for verifying security and non-vulnerability conditions for products, devices and systems for networks, services and critical infrastructures. In Netherlands, the BSPA scheme is in pilot phase since 2015. *Norway* and *Sweden* have the intention to develop a protection profile based on Common Criteria. The different international and national approaches will be widely argued within the chapter 3. Any future EU activity in the field of cybersecurity standards, certifications and labels should take into due account the existing international ecosystem.
- **Flexible cybersecurity solutions** - To stay ahead of malicious attackers, industry must be able to develop and deploy new tools to protect our digital economy against changing cyber risks.

<sup>30</sup> Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, Gazzetta Ufficiale n. 87 del 13 aprile 2017 (Italian Prime Minister Decree, 17/02/2017, Directive on guidelines for national cyber protection and cybersecurity, Official Bulletin n.87, 13/04/2017)

---

Policymakers should make sure that any regulatory action in this field keeps abreast of state-of-the-art technology.

- **One size does not fit all in a complex cyberspace** - A new EU certification framework would not be able to cover a broad set of products/services as the nature of products and services as well as the magnitude of cybersecurity risk vary significantly.
- **Promoting consumer protection and innovation** - Component/product labelling could potentially lead to a false sense of security for end-users in the consumer market. Benchmarking cybersecurity practices, on the contrary, would allow both consumers and organisations to compare situations and form an idea of the cybersecurity state-of-the-art.
- **Certification and competitiveness** - Regulated certifications and security **evaluation involve considerable costs**. It is important that they remain voluntary and that a range of agile self-certification mechanisms are allowed to flourish according to the existing market. It is important **not to erect market barriers to smaller companies** by mandating high entry costs.

A contrast is often made to energy-efficiency labelling, but there are some important differences. Firstly, while energy use can be subject to fairly homogenous or limited measurements (e.g. kWh), security is not as consistent. What matters for one set of products does not necessarily matter for others. Secondly, and most importantly, security is not static. While a product may achieve a top rating at the moment it is put on the market, six months down the line the fast paced changes of the threat landscape may render it insecure. **Labelling, therefore, creates the very real risk of a false sense of security.**

### *The Labelling Impact*

Within these paragraphs, some examples and studies on labelling, experienced in different industry sectors, will be shown. Although there are no objective measurement methods to compare two labels of different sectors, the aim of this section is to provide some elements of comparison and possible scenarios or impacts in case of adoption of an EU labelling Scheme for ICT Products.

### *Energy Labels*

The “Study on the impact of the energy label – and potential changes to it – on consumer understanding and on purchase decisions”<sup>31</sup> explores consumers’ understanding of the individual elements of the energy label and how the label design influences consumer choice. The study has been conducted in two phases:

- *Phase I* is a targeted literature review and an online behavioral experiment.
  - The objective of the review is to investigate existing knowledge on consumer behavior and understanding under alternative energy labelling frames.
  - The online experiment tested choice and understanding in an incentivized experiment and understanding test. The behavioral experiment is conducted in seven Member States.
- *Phase II* is a bricks-and-mortar experiment that is carried out at retail stores and centralized locations in four Member States.

The findings from both phases of the study combined, along with literature review, indicate the following in terms of consumer choice and understanding under the label frames tested.

### **Consumer understanding**

- Energy efficiency scales that include letters as opposed to numbers are generally better understood by consumers.
- Consumer understanding of the energy efficiency scale with A+++ to D and A to G scale is similar between the two.
- The differences in understanding between the alternate numeric scales tested is mixed and provides no clear indication as to which numeric scale may be best understood by consumers in the market.

---

31

<https://ec.europa.eu/energy/sites/ener/files/documents/Impact%20of%20energy%20labels%20on%20consumer%20behaviour.pdf>

- One third of consumers understand the meaning of the open ended scale. This increases to just under two thirds when consumers are provided with prior information in regard to the meaning of the open ended scale.
- Over half of consumers understand that the benchmark marker indicates best available technology.
- The provision of prior information can improve consumer understanding of the energy efficiency scale. As previously stated, this is particularly the case with the open-ended scale where understanding improves substantially if a prior explanation is provided.
- The majority of consumers were able to correctly identify the product that was least costly to use indicating that they understand the meaning of kWh/annum. Similarly, consumers that understand the meaning of kWh/annum are more likely to correctly identify the product that is least costly to run.
- Consumers are less likely to identify the least costly product to use when the product is affixed with a numeric or reverse numeric label compared to the A+++ to D and alphabetic label.
- Understanding the energy efficiency scale is an important determinate in whether the consumers choose the most energy efficient product; and, understanding is generally higher for the A+++ to D and alphabetic scale than the numeric scales.

### **Consumer choice**

- There is some evidence that label frames which use alphabetic scales lead to more consumers choosing energy efficient products compared numeric scales.
- There is some evidence that labels with an A to G scale lead to more consumers choosing energy efficient products compared to the A+++to D scales.
- The choice between one and another label design has a greater difference in impact on behaviour for consumers who consider energy efficiency of low importance in their purchasing decision, compared to consumers that consider energy efficiency as an important criterion in product choice.
- The choice of label design is of greater importance in influencing behaviour for products where energy efficiency is not of key importance to consumers when selecting a product.

### **Average additional amount that participants are willing to pay for a more energy efficient product**

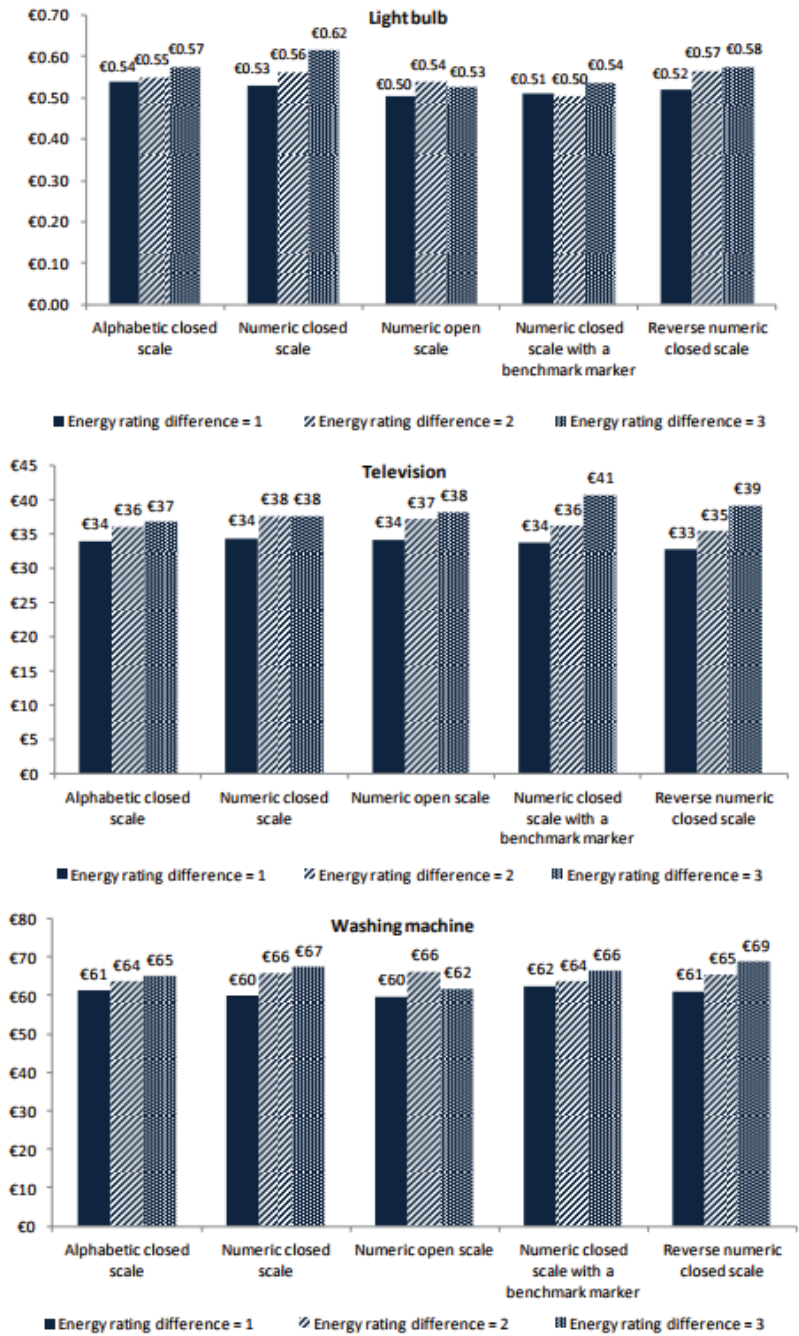
The study analyse the average additional amount that participants are willing to pay for a more efficient product and whether this varies depending on the energy label framing, as known as the average minimum premium. To explain this using an example, if a participant from Italy was faced with the following two options for a television:

- Price: €150 and Energy efficiency rating: C
- Price: €180 and Energy efficiency rating: B

If they choose the second option, this shows that they are prepared to pay at least a €30 premium for the more energy efficient option. However, this participant may have been willing to pay a much higher premium for a television with an energy efficient of 'B' rather than one with an energy efficiency rating of 'C'. However, this potentially higher price premium was not included in the set of choices within the experiment.

The figure below shows the average minimum amount that participants are willing to pay for a more energy efficient product across each of the different framings and for each product. Results are divided depending on the energy efficiency rating difference between the two products involved in the choice experiment decision. Given the energy efficiency combinations used in the choice experiment the energy efficiency rating difference is either 1, 2 or 3 levels. For example, if a participant in the alphabetic closed scale framing is faced with a decision of choosing between a product with an energy efficiency rating of 'B' and another of 'C', the energy efficiency rating difference is 1. Similarly, if they are faced with a choice between a 'B' rated product and a 'D' rated product, the energy efficiency rating difference is 2. Finally, if they are faced with a chose between a 'B' or an 'E' rated product, the energy efficiency rating difference is 3. It is possible to observe in the Figure below that participants are willing to pay a higher premium for products with a larger energy efficiency rating difference, in the majority of cases. For example, participants in the numeric closed scale with benchmark marker framing are willing to pay €2 more for a television that is two energy efficiency

ratings higher than the alternative product (Energy rating difference = 2) than they would pay for a television that is one energy efficiency rating higher than the alternative (Energy rating difference = 1).



**Figure - Average minimum premium participants are willing to pay for a more energy efficient**

Another study entitled "Energy Labels: Formats and Impact on Consumption Behavior"<sup>32</sup> investigates the moderating role of energy labels on the relationship between consumer predispositions (energy consciousness) and purchase of energy saving products.

<sup>32</sup> <http://www.duplication.net.au/ANZMAC09/papers/ANZMAC2009-334.pdf>

Symbolic labels are used to communicate product information (e.g., nutritional ingredients, product safety warnings, and product ecological footprint) to consumers to increase their knowledge in purchase decisions. Energy labels are one of the widely used symbolic labels. They are legally required by many governments and technically endorsed by authoritative third parties in many nations. Different product categories are included in the labelling schemes in different countries, but high energy consuming appliances such as refrigerators and air conditioners are commonly included. Placed on the front side of the machine, energy labels certify the energy efficiency level of the appliance. The aim of using energy labels, like other ecological labels, is to encourage manufacturers and consumers towards more environmentally positive actions (OECD, 2005).

Researchers suggest that attitudes that are more accessible from memory are more predictive of behaviour, influence what messages are attended to, and how those messages are processed, and are more stable across time (Alwitt and Berger, 1993; Fazio, Herr and Olney, 1984; Fazio, Powell and Williams, 1989). Consumers with high energy consciousness may buy energy inefficient models due to the inactivation of their environmental attitudes (Alwitt and Berger, 1993). Considerable amount of information is processed at the point of purchase, and energy consciousness may not be the operant attitude. **The energy rating label can serve as a reminding notice, raising the accessibility and relevance of consumer energy consciousness in ecological consumption.**

Evidence presented within the report “Impacts of the EU’s Ecodesign and Energy/Tyre labelling legislation on third jurisdictions”<sup>33</sup>, shows that **international cooperation on equipment energy efficiency standards and labelling has contributed to delivering much greater energy, economic and environmental savings than would have occurred otherwise.** Willingness to share programmatic experience, learn from and emulate the successes of other programmes is an essential component of the product policy achievements made so far and this has led to the rapid promulgation of equipment energy efficiency measures round the world.

As stated within the paper “Consumer Response to Energy Labels - Insights from Choice Experiments”<sup>34</sup>, **markets for energy-efficient goods are commonly characterized by information asymmetries.** Buyers are often not aware of the fact that the good they are about to purchase is also an energy service with running costs such as costs for electricity (Wilkenfeld et al., 1998). In addition, even those buyers who possess information about the existence of such costs are often not able to identify the level of energy efficiency of a good before their purchase decision. The energy consumption is therefore commonly an unobservable, or credence, characteristic; such characteristics can commonly lead to negative externalities of asymmetric information (e.g., Akerlof, 1970). In his seminal article on the market for lemons, Akerlof (1970) shows how the presence of information asymmetries can lead to market failure and adverse selection, and discusses signaling and screening as ways to overcome those challenges. One method of signaling that has received increasing attention from academics, policy makers and industry professionals is environmental or eco-labelling (De Boer, 2003; Pedersen and Neergaard, 2006; Rubik et al., 2007; Thøgersen, 2000).

### *Eco-Labels*

**Third party certified eco-labeling schemes are increasingly used worldwide as a means to overcome such information asymmetries and to increase trust in the validity of the environmental information. By providing information on the environmental performance of products, eco-labels can guide consumers towards more environmentally friendly purchasing behaviour (Grankvist and Biel, 2007).** When consumer’s see a third-party certification is displayed or visible on a product, customers believe that specific standards have been met because an outside organization has verified findings through an audit or a rigorous testing process<sup>35</sup>. Furthermore, such labels help manufacturers to gain a competitive advantage by producing environmentally friendly products (Thøgersen, 2000). Eco-labeling programs for promoting energy efficiency have gained particular importance for stimulating the sales of energy efficient electrical appliances and buildings worldwide. Energy labels can be used to provide information to consumers in order to enable them to compare the energy efficiency of a good on an equitable basis (Mahlia et al., 2002). **Labels can reduce uncertainty and**

<sup>33</sup> <http://www.ecofys.com/files/files/ec-2014-impacts-ecodesign-energy-labelling-on-third-jurisdictions.pdf>

<sup>34</sup> [https://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4020/\\$FILE/dis4020.pdf](https://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4020/$FILE/dis4020.pdf)

<sup>35</sup> <https://www.uschamberfoundation.org/blog/post/certification-can-help-boost-consumer-trust/31481>

---

**overcome information asymmetry, but the optimal design of energy labels is a critical success factor and might even hinder energy labels' effectiveness when not carefully designed.**

Eco-labeling could bring to a number of major benefits<sup>36</sup>:

1. **Informing consumer choice:** Eco-labeling is an effective way of informing customers about the environmental impacts of selected products, and the choices they can make. It empowers people to discriminate between products that are harmful to the environment and those more compatible with environmental objectives. An eco-label makes the customer more aware of the benefits of certain products, for example, recycled paper or toxic-free cleaning agents. It also promotes energy efficiency, waste minimization and product stewardship.
2. **Promoting economic efficiency:** Eco-labeling is generally cheaper than regulatory controls. By empowering customers and manufacturers to make environmentally supportive decisions, the need for regulation is kept to a minimum. This is beneficial to both government and industry.
3. **Stimulating market development:** When customers choose eco-labeled products, they have a direct impact on supply and demand in the marketplace. This is a signal which guides the market towards greater environmental awareness.
4. **Encouraging continuous improvement:** A dynamic market for eco-labeled products encourages a corporate commitment to continuous environmental improvement. Customers can expect to see the environmental impacts of products decline over time.
5. **Promoting certification:** An environmental certification program is a seal of approval which shows that a product meets a certain eco-label standard. It provides customers with visible evidence of the product's desirability from an environmental perspective. Certification therefore has an educational role for customers, and promotes competition among manufacturers. Since certified products have a prominent logo to help inform customer choices, the product stands out more readily on store shelves. Coveting the logo may induce manufacturers to re-engineer products so that they are less harmful to the environment.
6. **Assisting in monitoring:** Another benefit of an official eco-labeling program is that environmental claims can be more easily monitored. Competitors and customers are in a better position to judge the validity of a claim, and will have an incentive to do so should a claim appear dubious.

### *Food Labels*

Firms typically have more information about the quality of their products than do consumers, creating a situation of asymmetric information<sup>37</sup>. It is prohibitively costly for most consumers to acquire nutritional information independently of firms. Firms can use this information to signal their quality and to receive quality premiums. However, firms that sell less nutritious products prefer to omit nutritional information. In this market setting, firms may not have an incentive to fully reveal their product quality, may try to highlight certain attributes in their advertising claims while shrouding others (Gabaix & Laibson 2006), or may provide information in a less salient fashion (Chetty et al. 2007). Mandatory nutritional labeling can fill this void of information provision by correcting asymmetric information and transforming an experience-good or a credence-good characteristic into search-good characteristics (Caswell & Mojduszka 1996). Golan et al. (2000) argue that the effectiveness of food labeling depends on firms' incentives for information provision, government information requirements, and the role of third-party entities in standardizing and certifying the accuracy of the information.

According to the survey conducted within the study "Labeling Policy for Genetically Modified and Organic Food: Impact on Consumer Choice"<sup>38</sup>, more than half of participants (68.3%) expressed that they prefer to purchase foods with a non-GMO label versus foods without a non-GMO label. Furthermore, a majority of participants (87.8%) would like to see more labeling that distinguishes non-GMO and organic from GMO products. However, a small number of participants (24.4%) report that GMO food labeling impacts their purchasing decisions all the time, while approximately half of participants (51.2%) reported that GMO labeling affects their purchasing decisions only sometimes. Combined, 75.6% of participants allow GMO

---

<sup>36</sup> [https://www.iisd.org/business/markets/eco\\_label\\_benefits.aspx](https://www.iisd.org/business/markets/eco_label_benefits.aspx)

<sup>37</sup> <http://kiesel.ucdavis.edu/AR%20KieselMcCluskeyvillasBoas.pdf>

<sup>38</sup> <http://www.fasebj.org/content/31/1/Supplement/640.32.short>

---

labeling to influence their purchasing decisions. Those who believe organic foods have a *beneficial* impact on the environment reported that their views impact their purchasing decisions more frequently than those who were unsure of their effects.

Many consumers actively seek information about products that have qualities that serve their health needs and are consistent with their values<sup>39</sup>. As a result of these varied interests, food labels are increasingly being used to provide consumers with information about the environmental, technical and socioeconomic conditions under which the products were produced, as well as the health and safety aspects of food products. The growing consumer and industry interest in food labels presents challenges for government authorities, which **must ensure that the information that appears on food packages is useful, credible and presented clearly, so that it does not mislead the consumer**. With the increase in global trade in food, there is a need to harmonize food labelling so that product information is easily understood and is relevant to consumers in different markets.

As discussed within the paper "Is Organic Labelling Enough? Information Disclosure as Policy Instrument to Empower Consumer Choices"<sup>40</sup>, **consumers are generally not satisfied with the availability of information that can guide their purchase decision**, and arguably, they are especially in a disadvantaged position to judge the potential compromises that the organic certification system creates. Information asymmetry, the gap of information with regard to the quality of organic products between consumers and producers, are expressly severe because of the nature of the products. In making choices for products, consumer typically relies on the dominant quality attributes, namely search, experience, credence and Potemkin attributes. A search attribute, such as freshness or appearance, is known before the purchase and consumers have the ability to examine it. Experience attributes, such as taste, are known after the consumption of the product. Credence attributes, such as nutrition or contamination, are difficult to be observed by consumers, but they can rely on third parties for quality assurance.

Recent expansion of organic food market has also been seen as the results of heightened awareness of the impact of food systems on environment. Such consumers are willing to pay a price premium for the additional benefits consuming the organic products. However, these values are not attributes that can be directly observed by consumers. Instead, **they rely on various information cues on the label when evaluating products under uncertainty. Labels or organic claims are widely used to transmit important quality information to consumers**. Organic labeling has been observed to be associated with a higher level of perceived healthfulness, hedonism, environmental friendliness and food safety. Since organic eggs are credence and Potemkin products, labels bearing organic certification elicit certain level of confidence of the values acquired through consuming organic egg. Not all organic labels, however, elicit the same level of trust. **In general, a third-party certification schedule is considered to be more trustworthy than producers' or retailers' private labelling scheme**<sup>41</sup>. Label agency makes a difference to consumers' perception and willingness to pay. For example, in Switzerland, organic consumers were willing to pay a higher premiums for products with the Bio Suisse's label, a label backed by the farmers' umbrella organization, compared to products with other organic label. Consumers in Denmark and Czech Republic are willing to pay the highest price premium for governmental logo. The reputation and brand image of the label agency lend creditability to the label, and enhance the level of consumer trust. Although consumers are not willing to automatically assume fidelity of quality assurance behind of every label, they may place greater level of trust over the logos backed by ethical practices and stringent legal requirements. In the US, USDA organic has been an established logo with high level of consumer awareness and positive perception of the certification scheme behind it, consumers are responding to USDA organic milk more positively than generic organic labels.

It is important to remark that the perception of overall quality depends on both the consumer's awareness of the label and the label's subsequent ability to generate positive descriptive and inferential beliefs. Label

---

<sup>39</sup> <http://www.fao.org/docrep/018/i0576e/i0576e00.pdf>

<sup>40</sup> <http://hl-128-171-57-22.library.manoa.hawaii.edu/bitstream/10125/41482/1/paper0333.pdf>

<sup>41</sup> S. Eden, "Business, trust and environmental information: Perceptions from consumers and retailers," *Business Strategy and the Environment*, vol. 3, no. 4, pp. 1-8, 1994.



equity thus enhanced purchasing intention.<sup>42</sup> The impact on overall quality and purchase intention only emerged, for example, when the unrecognized PGI (Protected Geographical Indication) label was explained to consumers, thus highlighting the importance of building awareness of a values-based label. When it was explained, the values-based label was shown to operate as an effective market signal that generated both descriptive and inferential beliefs in relation to the products bearing the label. **These beliefs in turn explained consumers' perception of overall quality and influenced purchasing intention. Finally, consumers – individually and collectively – will be better served by labelling schemes that incorporate an understanding of their perspective and thus reduce misinformation.**<sup>43</sup>

The study "Consumer market Study on the functioning of voluntary food labelling schemes for consumers in the European Union"<sup>44</sup> has identified a large number of food labelling schemes across the EU Member States, Iceland and Norway but with important country variations. The study identified Spain, Germany, Italy and Portugal as the countries with the highest number of schemes while Romania, Cyprus and Malta were found to have a very limited number of food labelling schemes.

**Increasing transparency and minimising consumer confusion seem to be the key drivers for schemes to follow the guidelines while lack of awareness, administrative burden and cost of compliance were identified as key obstacles for compliance.** The guideline criteria most often met by food labelling schemes that were identified in the websweep were provision of contact information and/or feedback mechanisms on scheme websites for which 100% of schemes met this criterion. Clarity and transparency of scheme requirements and claims made was also met by a large number of food labelling schemes. Here we observe that between **91% and 82% of schemes clearly state their objectives**; between 79% and 73% have claims and requirements which are clearly linked to their stated objectives, and similarly the scope of the scheme in regard to the products and process it covers are clear. However, when seeking more detailed information on scheme requirements and specifications this is not always available for free on the website. Only 59% of schemes met this criterion in the websweep index. Further, when these specifications are available they can often be difficult to understand from the point of view of a consumer. An important recommendation would be to encourage schemes to provide information on their websites about their requirements, their specifications and their membership fees, and fees for certification, in a form that is easy to understand for all relevant actors, including consumers. This would help improve compliance of schemes against the 2010 Commission guidelines. In addition, encouraging schemes to provide information on the evidence used to make any claims about scheme requirements easily available on their websites, (again) in a form that is easy to understand for all relevant actors, including consumers is recommended.

To improve transparency, a recommendation would be to encourage schemes to clearly state whether, where and to what extent their specifications go beyond the relevant legal requirements. Provisions for enabling and promoting the participation of small scale producers could also be explored as this was met by a low proportion (35%) of schemes that responded to the scheme operator survey. Further, clearly stating that the scheme is public or private and whether it is certified or self-declared would be useful for consumers as this information is often hard to find on scheme websites. While not specifically addressed in the assessment of schemes, the provision of a web address on the scheme label affixed to the product may also help consumers as they could then easily find additional information on the scheme if they want. Methods to minimize the administrative burden and costs for producers and scheme operators in complying with the guidelines could also be explored.

Overall, results of the consumer survey show that consumers are aware of food labelling schemes, **they buy products affiliated to food labelling schemes, believe there are benefits to these products and to some extent are willing to pay a premium price for labelled products.** Providing consumers with more and better accessible information on the different types of labelling schemes and the meaning of

---

<sup>42</sup> Third party labeling and the consumer decision process, HEC -

<https://basepub.dauphine.fr/bitstream/handle/123456789/12755/CR891Flarceneux.pdf?sequence=1&isAllowed=y>

<sup>43</sup> Third party labeling and the consumer decision process, HEC -

<https://basepub.dauphine.fr/bitstream/handle/123456789/12755/CR891Flarceneux.pdf?sequence=1&isAllowed=y>

<sup>44</sup>

[http://ec.europa.eu/consumers/consumer\\_evidence/market\\_studies/food\\_labelling/docs/final\\_report\\_food\\_labelling\\_scheme\\_full\\_en.pdf](http://ec.europa.eu/consumers/consumer_evidence/market_studies/food_labelling/docs/final_report_food_labelling_scheme_full_en.pdf)

---

the most common ones, as well as educating them through, for example, an information campaign would be a good way of reducing this risk. Improved information provision, information campaigns or educational initiatives could help consumers distinguish between the different types of schemes, in particular between certified and self-declared or between public and private. This could also increase their knowledge of regulations for schemes and help them make more informed choice. A clear indication on the scheme label about whether the scheme is public or private (where it is possible to qualify clearly), certified or self-declared could also be an easy way of increasing scheme transparency without adding a lot of text on the label.

To improve understanding and access to information about food labelling schemes for all interested parties, a model scheme could include the following key elements.

- Clear statement of the scheme name and website address on the label affixed to the product.
- Website with scheme contact details.
- Statement of the scheme objectives and the types of products and process it covers.
- Clear statement of the organisations or bodies that own and manage the scheme, including their contact information.
- If the scheme is endorsed by third parties, the names and contact details of the parties should be provided.
- Clear statement of whether the scheme is public or private, and certified or self-declared.
- If a certified scheme, the name of the certification body should be provided and clear and transparent information on the key certification processes and requirements for nontechnical readers should be available.
- If the scheme covers areas where there are specific legal requirements, such as organic farming or animal welfare this should be clearly stated, and the extent to which the scheme goes beyond the relevant legal requirements should be understandable to nontechnical audiences.
- Provision of clear guidance on how to meet the scheme main requirements for parties interested in joining the scheme. Contact details, question forms or other mechanisms to access assistance with understanding and meeting the requirements for membership should be available.

### *Healthcare Labels*

A pre-requisite for a market to be able to function properly is transparency on prices and quality so that the end user can inform himself fully and correctly before making a purchasing decision. In the case of medical devices, between demanders and providers there is an 'unbalanced' spread of knowledge of the market. **Manufacturers have the benefit of having much more information than users:** they know the functioning (and limitations) of their product, know the cost structure, etc. The demand side of the market, on the other hand (specialists, nurses, buyers, management/board), is very fragmented, both in terms of knowledge of the (sometimes very specialized) use of the devices and also knowledge about what other (substitutable) devices are available. The users of medical devices are therefore strongly dependent on the knowledge, expertise and information provided by manufacturers (for example with specialised operations, with the use of equipment, etc.). The fact that the users share little or no information between themselves (price, quality, etc.) is also a factor, with the result that the problem of information remains<sup>45</sup>.

Transparency and better information are crucial to give more autonomy to patients and health professionals and enable them to take decisions with full knowledge of the facts, in order to give a solid base to regulatory decision-making process and to make sure the latter is trust-worthy. To do so, it is essential that Eudamed (European Database on Medical Devices) electronic systems related to existing devices, concerned economic operators and certificates allow public opinion to be well informed about devices circulating on the market. The clinical investigation electronic system should serve as a tool for cooperation between Member States and enable promoters to deliberately introduce a unique application process for several Member-States, and in this case to report serious incidents. Otherwise, manufacturers should convey the main safety and performance characteristics and the clinical evaluation results for high-risk medical devices via a public

---

<sup>45</sup> Sector Study Medical Devices Study of the structure and functioning of the market for medical devices

document The well-functioning of notified bodies is also essential to guarantee a high level of health and safety protection, as well as citizen trust in the system.<sup>46</sup>

Medical device labeling assists patients or their lay caregivers in understanding the device; its operation, care, and maintenance; the way it interacts with the body to accomplish its purpose; its place and purpose in the patient care regimen; and any safety or disposal issues. Medical device labeling is essential to assure safe and effective use of many, but not all, devices. It informs patients or their lay caregivers about proper use, risks, and benefits of the device in language they can understand. Adequate directions for operating the devices are needed to make devices safe and effective. For example, as more patients use complex medical devices at home, medical device patient labeling becomes necessary to better communicate to the lay person how to operate the device. Devices that might have labeling that would include instructions for use would be those the patient or lay caregiver have to set up, operate, clean, etc. They might include such devices as suction equipment, intravenous infusion pumps, physical therapy equipment, or transdermal electrical nerve stimulation (TENS) devices. Devices that would have labelling consisting primarily or completely of risk/benefit information might be implants that have no external patient interface, once they are implanted, or prescription, diagnostic or therapeutic devices that the patient is actively involved in choosing (e.g., laser eye surgery, lithotripsy, intraocular lenses)<sup>47</sup>.

## 2.4. The problem of Fragmentation

One of the key drivers of increasing cybersecurity risk is that the European cybersecurity industry is fragmented for historical reasons and remains fragmented<sup>48</sup>. Historically, firms grew in this sector as a result of governmental demand and remain largely dependent on this very domestic revenue stream, which reduce cross-border purchases and the incentives for firms to grow outside their national market. The EU cybersecurity market is dominated by a small group of global vendors, competing with a high number of smaller European suppliers that remain regional or national players (IDC, 2009)<sup>49</sup>. The EU suppliers, while showing a positive dynamism, remain mostly national or regional players. The presence of third country suppliers drives the competitiveness and innovation in the market (Optimity Advisors, 2015)<sup>50</sup>.

### Box 2 Key evidence on the cybersecurity market

- The **global size** of the privacy and cybersecurity (PAC) market vary from **EUR 47bn to EUR 76bn (2014)** and the industry is expected to **grow by around 7–8% per annum over the next 5–6 years**.
- The total EU market (including non-EU countries) is worth **26% of the global market**: EUR 12bn–EUR 19bn (2014) and is considered the second largest cybersecurity market behind North America, which controls a large segment (43%) of the global market;
- Governance is fragmented at EU level due to the fact that **security in general, and cybersecurity in particular** – especially as a component of critical infrastructures and national assets protection – **remains a national responsibility within the EU treaties**;
- Governance fragmentation is visible also at Member States level where the arrangements between national civilian and military CERTs fragmented;
- Another barrier for the emergence of a more cooperative European industry is the presence of entrenched **third-country companies** that tend to be preferred to EU domestic companies with similar or better solutions, due to **reputation and maturity of third-country suppliers**;
- Summing up **EU weaknesses** that could jeopardise innovation and synergies in the cyber domain, the key factors are **fragmentation in governance, lack of consistency in the EU data collection and data analysis and lack of end-user knowledge** of the cybersecurity market. There is also a shortage of EU companies that can offer the **whole value-chain of cybersecurity solutions**, and that are able to absorb the talent on the market, and there is **limited entrepreneurial activity** when compared with the US.

Source: Optimity Advisors (2015)

<sup>46</sup> Françoise Grossetete, Revise the Rules Relating to MD Advertising to Ensure the Right Information and Optimal Patients Protection, <http://www.ealth.org/images/speak-about-us/european-files-magazine-march-2013.pdf>

<sup>47</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3255430/>

<sup>48</sup> European Commission, SWD(2016) 216 final, Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

<sup>49</sup> IDC. (2009). The European Network and Information Security Market Brussels: Report delivered by IDC for the European Commission.

<sup>50</sup> Optimity Advisors. (2015). Study on Synergies between the civilian and the defence cybersecurity markets Brussels: Report delivered by Optimity Advisors for the European Commission.

This situation results in the the difficulty to compete on the European and global levels and to grow (**problem**), which often leads to mergers and acquisitions of Europe's SMEs by non-European actors, weakening the European sector and leaving Europe also more vulnerable and technologically dependent on others (**direct effect**); furthermore this also cause the risk of know-how outflow as the European cybersecurity firms cannot absorb the newly skilled professionals produced by European academic institutions who end up working for foreign global companies . Second, there is the European cybersecurity ecosystem is characterised by low dialogue and coordination (**driver**), which result (**problem**) in the lack of 'a well-functioning mechanism ensuring trustworthiness & readability of cybersecurity products and solutions' (European Commission, 2026b, p. 10); this further creates barrier to both cybersecurity and other cross-border activities (**direct effect**). Finally, leaving aside the cyber-security sector itself, there is a lack of expertise both in ICT producing firms and in ICT using firms as regard cybersecurity (**driver**), which contributes to low demand-side awareness (**problem**); the latter further reinforce the cross-border barriers (**direct effect**). Taken altogether these drivers, problems, and direct effects, contribute to the **indirect effect** of missing the growth opportunities that would derive from a more dynamic and competitive European cybersecurity industry.

**The certification landscape.** First, various and not fully coordinated certification initiatives (**driver**) increase fragmentation in the domain of certification (**problem**), resulting in duplication of efforts and waste of resources (**direct effect**). Second, the sectorial fragmentation of initiatives (**driver**) increase fragmentation in the ICT market for lack of product comparability with respect to cybersecurity (**problem**), resulting in lower competition in the ICT sector (**direct effect**). Third, lack of expertise on the users' side (**driver**), cause an insufficient demand side awareness (**problem**), and combined with the other problems leads to an increase rather than a decrease of the information asymmetry (**direct effect**). The earlier cited literature on energy labels shows, in fact, that lack of credibility or understanding and proliferation of different and not comparable labels create confusions and negative reactions on the side of users. The fragmentation of certifications schemes (and possibly of associated label) would have the same effects and induce more rather than less information asymmetry also in relations to cognitive phenomena such as heuristics and biases. Taken altogether these drivers, problems, and direct effects, contribute to the **indirect effect** of missing the growth opportunities that would derive from boosting cybersecure European ICT products in the global market. The certification fragmentation is further discussed in the next sections of this document.

**Common end effects.** The problems and effects of the ecosystem as whole combined with, and compounded by, those of the certification landscape cause the end effects of: a) not reducing the net losses from cyber incidents for citizens, businesses, and public administrations; b) creating hindrances to the full implementation of the DSM strategy; c) foregoing several sources of potential growth for European economies.

## 3. The ICT security certification landscape

Certification can be defined as: *'a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system'* (NIST, 2010).

The certification of products generally requires the following four phases:

- 1) Application. A company applies a product for evaluation to obtain a certification;
- 2) An evaluation is performed to obtain certification. The evaluation can be mostly done in three ways:
  - a) The evaluation can be done internally to support self-certification;
  - b) The evaluation can be performed by a testing company, which is legally belonging to the product company;
  - c) It can be third party certification where the company asks a third party company to perform the evaluation of its product;
- 3) In case of an internal company or a third party company evaluation, the evaluation company provides a decision on the evaluation.
- 4) Surveillance. It is a periodic check on the product to ensure that the certification is still valid or it requires a new certification.

In the following, we review international and emerging national schemes to highlight the main problems and challenges, and conclude with a qualitative analysis of the costs of benefits of no EU action as compared to a broadly conceived EU Intervention. The following sections have been drafted extracting information from various sources including the JRC report<sup>51</sup> (Baldini et al., 2017), a report (Enisa, 2014) and the proceedings of two workshops by Enisa (Enisa, 2016a, 2016b), two key reports delivered by Ecorys (2011) and ERNCIP (2014), documents from the French and German Certification Authorities (ANSSI, 2015; ANSSI & BSI, 2017), as well as the Communication and supporting SWD on Security Industrial Policy (European Commission, 2012a, 2012b). In addition, information has been retrieved from interviews with National Certification Authorities and from the websites of Certification Authorities and similar institutions, which are indicated in footnotes.

### 3.1 International schemes and other initiatives

**Common Criteria (also known as ISO 15408)**<sup>52</sup>. The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA). It is a framework in which computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and security Conformity Assessment Bodies can evaluate the products to determine if they actually meet the claims. It ensures that:

- Products can be evaluated by competent and independent Conformity Assessment Body so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;
- These certificates are recognized by all the signatories of the CCRA.

The CC permits comparability between the results of independent security evaluations and is flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT

<sup>51</sup> Baldini, G., Giannopoulos, G., & Lazari, A. (2017). Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.

<sup>52</sup> <https://www.commoncriteriaportal.org/>

products. It can be used in the smart grid to verify if a product meets the claims regarding the technical implementation of those security functions (Enisa, 2014). CC certified products provide assurance on a wide range of product categories from, databases, operating systems, access control systems, network devices, to Trusted platform modules, biometric systems and devices<sup>53</sup>. Namely, for certified products and Protection Profiles are currently defined 15 categories (in fact, one of these (“Other devices and systems”) captures everything not included in the other 14 categories). A certified product/Protection Profile no longer recognised within CCRA is reported as “Archived” (Notice that, an official resolution, effective at June 1<sup>st</sup>, 2019, limits to 5 years the validity of recognition. Starting from that date, all certificates issued from 5 or more years will be archived.). In the next tables the current state is shown by official CCRA statistics showing, for the period 1999-2017, valid and archived certificates for products and protection profiles, per year, per scheme (country), and per assurance level (EAL).

2206 Certified Products by Category \*

Category	Products	Archived
Access Control Devices and Systems	64	57
Biometric Systems and Devices	3	0
Boundary Protection Devices and Systems	77	124
Data Protection	60	75
Databases	33	51
Detection Devices and Systems	15	49
ICs, Smart Cards and Smart Card-Related Devices and Systems	1063	21
Key Management Systems	23	27
Mobility	26	3
Multi-Function Devices	137	165
Network and Network-Related Devices and Systems	235	188
Operating Systems	94	69
Other Devices and Systems	264	276
Products for Digital Signatures	92	7
Trusted Computing	20	0
<b>Totals:</b>	<b>2206</b>	<b>1112</b>
<b>Grand Total:</b>	<b>3318</b>	

\* A Certified Product may have multiple Categories associated with it.

<sup>53</sup> See also the certified product list (cpl) of CCRA portal at, [www.commoncriteriaportal.org/products](http://www.commoncriteriaportal.org/products).

Certified Products by Assurance Level and Certification Date

<b>EAL</b>	<b>1999</b>	<b>2000</b>	<b>2001</b>	<b>2002</b>	<b>2003</b>	<b>2004</b>	<b>2005</b>	<b>2006</b>	<b>2007</b>	<b>2008</b>	<b>2009</b>	<b>2010</b>	<b>2011</b>	<b>2012</b>	<b>2013</b>	<b>2014</b>	<b>2015</b>	<b>2016</b>	<b>2017</b>	<b>Total</b>
EAL1	0	0	0	0	0	0	1	1	6	3	1	0	1	10	2	2	4	3	2	36
EAL1+	1	0	0	0	0	0	0	0	17	0	2	11	2	0	1	2	1	0	0	37
EAL2	0	0	0	0	0	0	1	0	8	1	7	2	3	2	10	12	18	15	6	85
EAL2+	0	0	0	1	1	1	2	2	8	8	8	4	5	20	23	29	59	76	21	268
EAL3	0	0	0	0	0	0	0	0	10	4	1	9	5	13	11	12	9	2	3	79
EAL3+	0	0	0	0	0	2	1	1	37	10	12	12	12	28	20	23	17	18	2	195
EAL4	0	1	0	1	0	0	0	0	28	5	9	4	6	2	7	2	0	5	1	71
EAL4+	0	1	1	2	2	3	3	2	142	58	67	56	60	91	64	52	58	56	19	737
EAL5	0	0	0	0	0	0	0	0	6	3	2	0	1	0	0	0	0	3	0	15
EAL5+	0	0	0	0	0	0	3	0	50	27	31	43	35	28	56	53	44	69	30	469
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL6+	0	0	0	0	0	0	0	0	0	0	2	3	0	4	6	6	13	11	4	49
EAL7	0	0	0	0	0	0	0	0	0	0	1	0	0	0	4	0	0	0	0	5
EAL7+	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
Basic	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	10	41	67	36	159
<b>Totals:</b>	<b>1</b>	<b>2</b>	<b>1</b>	<b>4</b>	<b>3</b>	<b>6</b>	<b>11</b>	<b>6</b>	<b>312</b>	<b>119</b>	<b>143</b>	<b>145</b>	<b>130</b>	<b>199</b>	<b>208</b>	<b>203</b>	<b>264</b>	<b>325</b>	<b>124</b>	<b>2206</b>

Certified Products by Scheme and Assurance Level

<b>Scheme</b>	<b>EAL1</b>	<b>EAL1+</b>	<b>EAL2</b>	<b>EAL2+</b>	<b>EAL3</b>	<b>EAL3+</b>	<b>EAL4</b>	<b>EAL4+</b>	<b>EAL5</b>	<b>EAL5+</b>	<b>EAL6</b>	<b>EAL6+</b>	<b>EAL7</b>	<b>EAL7+</b>	<b>B</b>	<b>M</b>	<b>S</b>	<b>N</b>	<b>Total</b>
Australia	2	1	9	7	2	3	5	12	0	0	0	0	1	0	0	0	0	19	61
Canada	1	0	8	129	0	9	0	8	0	0	0	0	0	0	0	0	0	21	176
Germany	9	4	10	26	14	56	15	310	8	169	0	20	0	0	0	0	3	644	
Spain	8	8	7	7	4	12	0	30	0	3	0	0	0	0	0	0	2	81	
France	1	18	1	15	0	39	4	276	3	259	0	14	4	0	0	0	0	634	
India	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	3	
Italy	4	6	0	1	2	0	1	9	0	0	0	0	0	0	0	0	0	23	
Japan	0	0	6	41	35	38	0	0	0	0	0	0	0	0	0	0	0	120	
Republic of Korea	3	0	5	8	9	15	24	15	0	15	0	0	0	0	0	0	1	95	
Malaysia	6	0	14	6	0	4	1	2	0	0	0	0	0	0	0	0	0	33	
Netherlands	0	0	4	1	1	1	1	19	0	13	0	15	0	1	0	0	1	57	
Norway	0	0	1	17	2	11	15	16	3	7	0	0	0	0	0	0	0	72	
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Sweden	1	0	9	2	5	4	5	4	1	0	0	0	0	0	0	0	1	32	
Turkey	0	0	7	1	3	0	0	9	0	0	0	0	0	0	0	0	0	20	
United Kingdom	0	0	3	7	1	3	0	26	0	3	0	0	0	0	0	0	2	45	
United States	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	109	110	
<b>Totals:</b>	<b>36</b>	<b>37</b>	<b>85</b>	<b>268</b>	<b>79</b>	<b>195</b>	<b>71</b>	<b>737</b>	<b>15</b>	<b>469</b>	<b>0</b>	<b>49</b>	<b>5</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>159</b>	<b>2206</b>

344 Protection Profiles by Category \*

Category	PPs Archived	
Access Control Devices and Systems	10	7
Biometric Systems and Devices	7	5
Boundary Protection Devices and Systems	36	24
Data Protection	15	4
Databases	9	7
Detection Devices and Systems	17	17
ICs, Smart Cards and Smart Card-Related Devices and Systems	88	20
Key Management Systems	15	11
Mobility	7	4
Multi-Function Devices	4	3
Network and Network-Related Devices and Systems	35	22
Operating Systems	17	15
Other Devices and Systems	63	18
Products for Digital Signatures	21	2
Trusted Computing	9	4
<b>Totals:</b>	<b>353</b>	<b>163</b>
<b>Grand Total:</b>	<b>516</b>	

\* A Protection Profile may have multiple Categories associated with it.

Protection Profiles by Assurance Level and Certification Date

EAL	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
EAL1	0	0	0	0	0	0	0	5	0	1	0	2	0	0	0	0	0	0	0	0	8
EAL1+	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	4
EAL2	1	1	1	3	1	0	0	5	3	0	1	0	1	2	1	0	1	4	1	0	26
EAL2+	1	0	2	1	2	0	0	1	7	12	2	0	6	0	1	0	2	4	1	2	44
EAL3	2	4	1	0	0	0	0	0	0	2	2	1	0	0	0	1	1	1	0	0	14
EAL3+	0	0	0	1	3	0	2	0	0	2	9	1	1	3	0	0	1	3	0	0	26
EAL4	0	0	2	1	1	0	0	1	0	1	2	1	0	4	1	0	0	0	1	0	15
EAL4+	0	8	1	11	7	7	0	3	3	5	9	14	15	4	5	4	4	7	10	4	121
EAL5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL5+	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL6	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
EAL6+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Basic	0	0	0	0	0	0	0	2	7	2	0	1	0	0	0	0	0	0	0	0	12
Medium	0	0	0	1	0	1	1	1	4	15	1	2	0	0	0	0	0	0	0	0	26
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	9	11	12	5	1	45
<b>Totals:</b>	<b>4</b>	<b>16</b>	<b>7</b>	<b>19</b>	<b>14</b>	<b>8</b>	<b>3</b>	<b>18</b>	<b>24</b>	<b>39</b>	<b>26</b>	<b>23</b>	<b>26</b>	<b>15</b>	<b>12</b>	<b>13</b>	<b>20</b>	<b>31</b>	<b>18</b>	<b>8</b>	<b>344</b>



Protection Profiles by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Canada	0	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	4
Germany	6	0	2	9	3	7	3	59	0	0	0	0	0	0	0	0	0	0	89
Spain	2	0	2	1	2	0	4	0	0	0	0	0	0	0	0	0	0	0	11
France	0	1	0	8	0	11	0	34	1	1	0	0	0	0	0	0	0	6	62
India	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Italy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Japan	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	5
Republic of Korea	0	1	0	0	0	0	2	5	0	0	0	0	0	0	0	0	0	0	8
Malaysia	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Netherlands	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	3
Norway	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	0	0	0	3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	4
Turkey	0	0	6	2	0	0	0	2	0	0	0	0	0	0	0	0	0	0	10
United Kingdom	0	0	1	0	5	0	3	3	0	0	0	0	0	0	0	0	0	0	12
United States	0	1	15	21	2	7	2	11	0	0	1	0	0	0	12	26	0	38	136
<b>Totals:</b>	<b>8</b>	<b>4</b>	<b>26</b>	<b>44</b>	<b>14</b>	<b>26</b>	<b>15</b>	<b>121</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>12</b>	<b>26</b>	<b>0</b>	<b>45</b>	<b>344</b>

The CCRA framework, within the definition of Collaborative Protection Profiles (cPP), introduces the concepts of "technical community (TC)" and Essential security Requirements. Two or more Schemes can declare their interest in setting up a TC in charge of facing a specific issue in a specific Technical Domain (TD). The TC will produce an ESR in order to take into account requirements as much as possible shared with all the Schemes in the CCRA and then will be define the cPP and the relative supporting documents to be used to evaluate a specific product in the TD against the cPP.

CCRA Schemes can chose to

- 1) [Involved Schemes] - contribute to the TC from the beginning of the project (interested nations): this contribution can be interpreted as the willing of the Scheme to evaluate the results of the community and eventually to propose the solution for a national procurement.
- 2) [Position Statement] - officially communicate a "position statement" in support of the ESR, meaning that the ESR is a correct and shared instantiation of the requirements in order to solve the issues defined for the setting up of the TD. A correct definition of a cPP in this area can be promoted in a national procurement.
- 3) [Endorsement] - officially communicate an endorsement of the cPP that means that the cPP as has been defined by the TC (and relative supporting documents) can be promoted for a national procurement.

The following table shows the EU schemes involved in the CCRA Technical Domains ant the position statements to the relative ESR (for all CCRA nations)

### Technical Domain

	Position Statement		EU Involved Schemes
	EU Nations	Non EU nations	
USB Protable Storage devices	DK,SE,FI,UK,GE	AU-NZ,JP,USA,	SE,UK,GE, (TK), NL
FDE	UK, NO,	USA, AU-NZ, CA	SE,UK, (TK), NO
Network Devices	UK	USA, AU-NZ, CA	UK, (TK), NO
Application Software			SE, (TK), UK
Dedicated Security Component			UK, SE, NL
Biometric Security			SP, (TK)

The following table shows the Endorsment statements of CCRA Schemes to the cPP defined in a specific technical domain

	Endorsment	
	EU Schemes	Non EU schemes
<b>Collaborative Protection Profiles</b>		
<b>Stateful Traffic Filter Firewalls</b>	UK	US, CA, AU-NZ
<b>FDE- Encryption Engine v.2.0</b>		US
<b>FDE - Authorizaion Acquisition v.2.0</b>		US
<b>FDE- Encryption Engine v.1.0</b>	UK	US, CA, AU-NZ
<b>FDE - Authorizaion Acquisition v.1.0</b>	UK	US, CA, AU-NZ
<b>Network Devices V.2.0</b>	US	
<b>Network Devices V.1.0</b>	UK	US, CA, AU-NZ

**SOG-IS.** SOG-IS is the main certification mechanism existing at European level. However, it only includes 12 Member States plus Norway and has developed only a few protection profiles regarding digital products (such as digital tachograph and smart cards)<sup>54</sup>. Moreover, Member States often request certification as a pre-condition to be admitted to national public procurement tenders. Additional national certification frameworks and schemes are expected to develop in the coming years. Here are presented some statistics for some producing members of SOGIS agreement. Differences between the numbers of recognized certificates issued by the scheme are represented only where present.

Next table reports some CC certification statistics for the Italian Common Criteria Scheme (OCSI).

Product type (CCRA categories)	#	CCRA & SOGIS					
		2012	2013	2014	2015	2016	2017
Products for Digital Signatures	7		1	1	2	2	1
ICs, Smart Cards and Smart Card-Related Devices and Systems	4				2	2	
Multi-Function Devices	3				2	1	
Data Protection	1				1		
Operating Systems	1			1			
<b>Total</b>	16		1	2	7	5	1*

Italian CC certification statistics - \*14 evaluation processes in progress (July, 21 2017)

<sup>54</sup> A Protection Profile (PP Profile (PP) is a document used as part of the certification process. A PP states a security problem of a given system or products and it specifies the security requirements needed to address that problem.) is a document used as part of the certification process. A PP states a security problem of a given system or products and it specifies the security requirements needed to address that problem.

Next table reports some CC certification statistics for the French Common Criteria Scheme (ANNSI)

Product Type	#	SOGIS/CCRA									
		#	<2010	2010	2011	2012	2013	2014	2015	2016	2017
Smart Card	347	333/332	57	32	29	36	38	37	34	52/51	18
Digital Tachographs	6	6	5	0	0	1	0	0	0	0	0
Miscellaneous	5	5	0	0	0	2	0	1	0	1	1
Micro-chips	182	180	71	15	4	15	22	14	8	20	11
Product for PC and servers	35	31	8	3	5	7	0	1	0	6	1
Network Product	23	22	9	2	1	1	1	4	0	4	0
Systems	1	1	1	0	0	0	0	0	0	0	0

Next table reports some CC certification statistics for the Dutch Common Criteria Scheme (NLNCSA).

Product Type	#	SOGIS/CCRA									
		#	<2010	2010	2011	2012	2013	2014	2015	2016	2017
Smart Card	14	11/14	1/4	0	0	1	5	1	1	0	2
Digital Tachographs	3	3	1	1	0	0	1	0	0	0	0
Miscellaneous	14	11/13	1/3	0	3	0	1	1	1	2	2
Micro-chips	4	4	1	0	1	0	0	0	1	1	0
Product for PC and servers	3	2/3	0	0	0	0	0	0	0	1	1
Network Product	8	7	1	0	0	2	0	1	1	0	2
Systems	2	2	0	0	0	0	1	0	1	0	0
HW devices	6	6	0	0	0	0	0	1	2	1	2
Crypto Library	8	8	0	0	0	1	1	0	3	2	1

Next table reports some CC certification statistics for the German Common Criteria Scheme (BSI).

Product Type	#	SOGIS/CCRA						
		#	2012	2013	2014	2015	2016	2107
Digital Signature	7	7	2	2	3	0	0	0
Digital Tachograph	5	5	1	2	0	2	0	0
eHealth	6	6	0	0	1	3	2	0
electronic ID documents	41	41	8	11	12	1	7	0
Network devices and system	18	18	1	3	4	8	2	0
operating system	13	13	4	3	2	2	2	0
other devices and systems	9	9/6	1	4/2	2/1	0	1	0
server applications	17	17	1	6	3	5	1	0
smart card and similar devices	72	72	9	14	14	14	17	0
smart metering systems	1	1	0	0	0	0	1	0

Next table reports some CC certification statistics for the UK Common Criteria Scheme (NCSC). Note that UK statistics are represented only on CCRA website and product categorization is same as CCRA.

Product Type (*)	#	SOGIS/CCRA						
		<2012	2012	2013	2014	2015	2016	2017
Access Control Devices and Systems	4	1	1	0	0	2	0	0
Boundary Protection Devices and Systems	2	2	0	0	0	0	0	0
Smart Cards and Smart Card-Related Devices and Systems	22	0	2	0	6	10	3	1
Network and Network-Related Devices and Systems	5	2	1	0	1	1	0	0
Operating Systems	2	1	1	0	0	0	0	0
Other Devices and Systems	6	5	1	0	0	0	0	0

**Information Technology Security Evaluation Criteria (ITSEC)**<sup>55</sup>. Used for evaluating computer security for IT products and systems. It is a structured set of criteria for evaluating computer security within products and systems. The ITSEC was first published in May 1990 in France, Germany, the Netherlands, and the United Kingdom based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 by the European Commission for operational use within evaluation and certification schemes. It is still used for some evaluation in the classified information but it has to be considered superseded by the publication of ISO 15408 Common Criteria for ICT security product evaluations.

**ISA Secure Certification Programme**<sup>56</sup>. It independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities. It is by the the IEC/ISA standardisation recognised, but the ISASecure is ye only existing certification service and is available at Certification Authorities in the US and Japan, and recognised by ANSI (American National Standards Institute).

**Federal Information Processing Standards FIPS-140**<sup>57</sup>. These are U.S. government computer security standards, which specify requirements for cryptography modules.

**Industrial Automation and Control Systems (ISA/IEC-62443 /IACS)**<sup>58</sup>. ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems. These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards.

**EN50128**. It specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications

**IEC61508**. It is aimed at the electrotechnical industry.

**ISO 27001**<sup>59</sup>. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. The ISO 27001 standard provides a framework that helps organisations: protect clients and employee information; manage risks to information security effectively; achieve compliance; protects the company's brand image.

**IASME** is a UK-based standard for information assurance at small-to-medium enterprises (SMEs). It provides criteria and certification for small-to-medium business cyber security readiness. It also allows small to medium business to provide potential and existing customers and clients with an accredited measurement of the cyber security posture of the enterprise and its protection of personal/business data. IASME was established to enable businesses with capitalization of 1.2 billion pounds or less (1.5 billion Euros; 2 billion US dollars) to achieve an accreditation similar to ISO 27001 but with reduced complexity, cost, and administrative overhead (specifically focused on SME in recognition that it is difficult for small cap businesses to achieve and maintain ISO 27001). The cost of the certification is progressively graduated based upon the employee population of the SME (e.g., 10 & fewer, 11 to 25, 26 - 100, 101 - 250 employees); the certification can be based upon a self-assessment with an IASME questionnaire or by a third-party professional assessor. Some insurance companies reduce premiums for cyber security related coverage based upon the IASME certification.

<sup>55</sup> See official document published on the website of the German Certification Authority BSI at: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en\\_pdf.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile)

<sup>56</sup> <http://www.isasecure.org/en-US/>

<sup>57</sup> <http://csrc.nist.gov/groups/STM/cmvp/standards.html>

<sup>58</sup> See: <https://www.isa.org/isa99/> and

<sup>59</sup> <https://www.iso.org/standard/54534.html>.

**ISO/IEC 19790 and ISO/IEC 24759** are applicable to validate whether the cryptographic core of any security product is properly implementing an approved suite of cryptographic protocols, modes of operation and key sizes, while protecting this implementation and the critical security parameters, such as keys, in accordance to the design and specification requirements laid out in the standards. There are four levels of security defined, and ISO/IEC 19790 includes a variety of possible implementations, both software and hardware.

**IECEE CB Scheme**<sup>60</sup>. It is operated by the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), is an international system for mutual acceptance of test reports and certificates dealing with the safety of electrical and electronic components, equipment and products. It is a multilateral agreement among participating countries and certification organizations, which aims to facilitate trade by promoting harmonization of national standards with International Standards and cooperation among accepted National Certification Authorities (NCBs) worldwide. By achieving this, it brings product manufacturers a step closer to the ideal concept of "one product, one test, one mark, where applicable".

In the specific domain of smart grids the list of applicable schemes includes the following (Enisa, 2014): ISO 9001; ISO/IEC 27001; IEC62443; ISO/IEC 15408, Common Criteria; ISO/IEC 19790; CPA, CSPN; and IASME. The latter, for instance, is a British standard that is not widely recognised outside the UK

## 1.1. National initiatives

**France**<sup>61</sup>. The National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d'information – ANSSI) established in 2008 the Certification Sécuritaire de Premier Niveau (CSPN), which is an IT Security Certification Scheme. Its main purpose is to offer a faster and cheaper alternative for IT Security Certification as compared to the Common Criteria (see below) approach. The security criteria as well as evaluation methodology and process are based on an ANSSI created standard. Similarly, to the CPA, there is no MRA for CSPN, which means that products tested in the France will not normally be accepted in other markets. CSPN is recognized only by ANSSI in France<sup>62</sup>. As reported in an ANSSI presentation (2015) the CSPN was developed as shorter and cheaper alternative to the Common Criteria evaluations, whose cost and duration are considered a barrier for the security industry development. The CSPN can be used when a low level of assurance is required and it ensures a product evaluation in 25 days (while CC evaluation of a smart card can take from 6 months to 1 year). ANSSI provides around 25 CSPN certificates (mainly on software) and 100 CC certificates (mainly hardware) per year. Currently, ANSSI recognises and issues two main types of labels. These labels are used for:

- certifying products
- qualifying products and services

**Germany**<sup>63</sup>. The German Federal Office for Information Security (**BSI**) is developing an approach for low level assurance to improve the efficiency of Common Criteria evaluation. The approach is still under development and is very close to the CSPN French framework.

The *IT-Grundschutz Certificate*<sup>64</sup> offers companies and agencies the possibility of making transparent their efforts regarding IT security. After consulting with registered IT-Grundschutz users and IT security experts, the BSI has defined three variants of the IT-Grundschutz qualification: the IT-Grundschutz Certificate and the self-declarations "IT-Grundschutz entry level" and "IT-Grundschutz higher level". The issuance of the IT-Grundschutz Certificate is based on an audit carried out by an external auditor licensed with the BSI. The outcome of the audit is an audit report which is submitted to BSI that decides on the granting of the IT-Grundschutz Certificates.

<sup>60</sup> <https://www.iecee.org/about/cb-scheme/>.

<sup>61</sup> Based on information from website (<http://www.ssi.gouv.fr/administration/produits-certifies/cspn/>) and from official case study presentation (ANSSI, 2015).

<sup>62</sup> ENISA - Smart grid security certification in Europe.

<sup>63</sup> Based on information reported in Baldini et al. (2017).

<sup>64</sup> [https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCertification/itgrundschutzcertification\\_node.html](https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCertification/itgrundschutzcertification_node.html)

**UK.** The *Commercial Product Assurance* (CPA)<sup>65</sup> is the UK national scheme for commercial off-the-shelf products; products successfully evaluated according to CPA obtain a Foundation Grade certification, meaning that they proved to be good commercial security practice and are suitable for lower threat environments. CPA is open to all vendors, developers and suppliers of security products with a UK sales base. However, there is no Mutual Recognition Agreement (MRA) for CPA, which means that products tested in the UK will not normally be accepted in other markets. CPA is similar to common criteria, however not so widely recognised outside of UK (Enisa, 2014). Information about products certified and cost to sustain for CPA certification can be retrieved on the online website of CPA scheme. Certified Products<sup>66</sup> under CPA scheme are actually **37** and **15** products are in evaluation.

The Costs<sup>67</sup> to sustain to certify a product under the CPA scheme are:

- Paid by Test Lab to NCSC for each task = £4,640
- Membership fees = £2,220
- Certified Consultancy for Large Companies = £10,100
- Certified Consultancy for SMEs = £1,010
- Additional Head Consultant with a single service offering = £1,010
- Each additional service offering for existing Head Consultant = £1,010

*Cyber Essentials*<sup>68</sup> is a government-backed, industry-supported scheme to help organisations protect themselves against common cyber-attacks. The full scheme, launched on the 5 June 2014, is used to “give assurance” to wider industry. For central government procurement of technology products and services, which involve handling of personal information, it is required that the Cyber Essentials scheme, or Cyber Essentials Plus, is in place<sup>69</sup>. The evaluation criteria currently recognised by the UK certification scheme, and the methodologies associated with them, are: a) the Common Criteria (CC) ISO/IEC 15408 and the Common Methodology for IT Security Evaluation (CEM) ISO/IEC 18045; b) the IT Security Evaluation Criteria (ITSEC) and the IT Security Evaluation Manual (ITSEM).

**The Netherlands.** Dutch approach Baseline Security Product Assessment (BSPA) scheme is intended to judge the suitability of IT security products for use in the “sensitive but unclassified” domain: the requirements are expressed in the Dutch “Baseline Informatiebeveiliging Rijksdienst” (Government security baseline, BIR). The BSPA scheme is in pilot phase since 2015. During the pilot phase BSPA scheme received **6 requests** for certification: three of them are completed and the other three are starting up. The average costs of a certification under BSPA scheme are approximately **40 thousand euros**. An evaluation performed under the BSPA scheme has the following main characteristics: it is carried out in constrained time frame and with limited resources; it determines the conformity of the product to the security specification in the Security Evaluation Target and it determines the effectiveness of the security features offered by the product. The evaluation process should take 25 person days within a calendar period of 8 weeks. The BSPA scheme is comparable to the CSPN scheme of ANSSI. Dutch scheme is then in charge of overseeing the entire process, to validate the report and to publish a “statement of conformity”. The Dutch national organization of DSO’s “Netbeheer Nederland”, has also developed the Dutch Smart Meter Requirements (DSMR). In December 2014, The Netherlands was considering developing a protection profile based on Common Criteria, anyhow, in order to be recognized among participants of any Mutual Recognition Arrangement based on Common Criteria certification (e.g. SOGIS, CCRA), any protection profile will need to be certified in a scheme that has been recognized as “certificate producing member”.

The objective of the Netherlands scheme for Certification in the Area of IT Security (NSCIB) is to enable IT products and systems to be evaluated and certified in the Netherlands in a way that conforms to the ‘Common Criteria’ methodology (ISO-standard 15408) for Evaluation and Certification.

A concrete example where the Dutch Certification scheme is requested in public procurement acts is represented by all taxis (more than 10 thousand) in the Netherlands, which have to contain an On-Board Computer (Dutch BCT). The relevant regulatory act came into force on 1 October 2011. The regulations specify that all taxi operators must purchase an on-board computer and have it installed and activated before

<sup>65</sup> <https://www.cesg.gov.uk/scheme/commercial-product-assurance-products-foundation-grade>

<sup>66</sup> [https://www.ncsc.gov.uk/index/certified-product?f\[0\]=field\\_assurance\\_scheme%3A226&f\[1\]=field\\_assurance\\_status%3AAssured](https://www.ncsc.gov.uk/index/certified-product?f[0]=field_assurance_scheme%3A226&f[1]=field_assurance_status%3AAssured)

<sup>67</sup> <https://www.ncsc.gov.uk/articles/products-and-services-scheme-fees>

<sup>68</sup> <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>

<sup>69</sup> <https://www.gov.uk/guidance/public-sector-procurement-policy#procurement-policies-for-technology>

---

1 February 2015. On-board computers in taxis must have a type-approval and must comply with the requirements for (software) security<sup>70</sup>.

## **Pricelist for certification under the Netherlands Scheme for Certification in the area of IT Security (NSCIB)**

### **Certification of a Protection Profile / Product**

NSCIB new certification € 3.300,00

Certificate is valid for a maximum of 5 years

Includes one certificate in Dutch or English and web publication of certification report

NSCIB re-certification (minor change) € 275,00

Original certificate remains

Based on Impact Analysis Report of changes, no updated vulnerability assessment

Certifier creates maintenance report

TUV updates records and adds maintenance report to web publication

NSCIB re-certification (major change) € 550,00

Re-issue of original certificate, original expiry date remains

Re-use possible of previous results, new vulnerability assessment

Certifier updates certification report

TUV updates records, re-issues certificate and updates web publication

### **Site Certification**

NSCIB site certification € 1.900,00

Site certificate is valid for a maximum of 2 years

Includes one certificate in Dutch or English and web publication of certification report

Translation per certificate € 275,00

Use of internal non-commercial certifiers (very limited availability) - Free

Use of external commercial certifiers (for regular certifications) - 175,00 p/h

**All costs exclude VAT and travel costs**

---

<sup>70</sup> <https://www.rdw.nl/sites/tgk/englishversion/Paginas/On-board-computers-for-taxis.aspx>

	Total	Certification fee	Certifier costs	Certifier hours
<b>New certifications EAL4-6</b>				
Small TOE (simple applet)	€20.800,00	€3.300,00	€17.500,00	100
Normal TOE (IC, Crypto Library, ePassport, HSM)	€29.550,00	€3.300,00	€26.250,00	150
Big TOE (JavaCard, complex HSM)	€33.925,00	€3.300,00	€30.625,00	175
<b>Re-certification Major change ("Maintenance")</b>				
Big TOE medium delta	€13.675,00	€550,00	€13.125,00	75
Re-certification Minor change	€9.425,00	€275,00	€9.150,00	50
<b>New certifications EAL2-3</b>				
Small TOE (e.g. simple network device)	€13.800,00	€3300,00	€10.500,00	60
Normal TOE (e.g. BCT)	€17.300,00	€3300,00	€14.000,00	80
Big TOE (complex network device)	€20.800,00	€ 3300,00	€17.500,00	100

*Figure - Average certification costs (ex VAT)*

### Number of NSCIB certificate applications received

Year	Type	New certifications	Recertifications	Maintenance
2011	Smartcards	4		1
	Network devices	1		
2012	Smartcards	3		
	Datadiode	1		
	Boundary protection	1		
2013	Smartcards	6	1	
	HSM	1		
	BCT	3		
2014	Smartcards	3		2
	Network devices	1		
	BCT			1
	POI (payment terminal)	1		
	Boundary protection	1		
	Site certificates	5		
2015	Smartcards	4	5	
	Network devices	1		
	PP BCT		1	
	Site certificates		1	
2016	Smartcards	5	3	6
	Network devices	3		
	Tachograph	1		
	Site certificates		4	



Year	Type	New certifications	Recertifications	Maintenance
Total 2011 - 2016	Smartcards (EAL4-6)	25	9	9
	HSM, POI (EAL4)	2	0	0
	Network devices (EAL2-3)	6	0	0
	BCT (EAL3)*	3	1	1
	Tachograph (EAL4)**	1	0	0
	Other (EAL3-7)	3	0	0
	Site certificates (EAL6)	5	5	0

\*National Regulation (Taxi)

\*\* EU Regulation

Year	Type	New certifications	Recertifications	Maintenance
Completed 2017	Smartcards	6	4	0
	Network devices	2	1	0
	HSM	1	0	0
	Datadiode	1	0	0
Ongoing 2017	Smartcards	3	3	0
	Network devices	1	0	0
	HSM*	3	0	0
	Datadiode	1	0	0

\*eIDAS Regulation

**Selective examples of emerging certification schemes across Member States.** In the *Czech Republic* the Institute for Testing and Certification (ITC) issue reports and certificates that, however, are not widely recognized<sup>71</sup>. *Norway* and *Sweden* have the intention to develop a protection profile based on Common Criteria. *SERTIT* (Sertifiseringsmyndigheten for IT-sikkerhet) is currently representing *Norway* as a member of the international community called "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)". The average number of certificate applications received by SERTIT for the last five year period (2013-2017) is 11,6 per year. The annual numbers of applications from 2013 – 2017 (up to the 3<sup>rd</sup> of August 2017) are: 14, 9, 13, 13, 9. SERTIT does not charge for the certification as it is a Governmental service, but companies have to cover travel expenses related to progress-meetings and site-visits. The cost of the evaluation itself is a matter between the Evaluation Facility and the Industry. SERTIT is not involved in the commercial part between the ITSEF and the Industry. Mandatory requirements for Certification are stated in the Security Act. The average number of certificate applications for the last five year period linked to the before mentioned mandatory requirements is 3,2 per year. The annual numbers of such certifications from 2013 – 2017 (up to the 3<sup>rd</sup> of August 2017) are: 6, 0, 4, 1, 5. In *Ireland* the *Cyber Essentials* scheme is used to "give assurance" to wider industry and interested parties that the certified organisation is applying basic levels of IT related security to address the threat of cyber-attacks. *Poland* recently joined SOG-IS<sup>72</sup> and will be able to self-assess and certify IT products in compliance with the international standard ISO/ IEC 15408 adopted by the Polish legal system. This standard allows formal verification of information systems security. This will increase the level of cyber security and raise the competitive efficiency of Polish companies on the global market. In *Spain* the CCN (Centro Certificación Nacional) adopts as common evaluation criteria those included in the following schemes: Common Criteria for Information Technology Security Evaluation» (CC); ISO/IEC 15408, Evaluation Criteria for IT Security; Information Technology Security Evaluation Criteria (ITSEC). The Number of certificate applications received by the CCN are 112 applications since January 2013 to August 2017. On average, the CCN receive around 22 applications per year. The Certification Authority does not request any fee for the release of the certificates. The costs come from the labs, which are not controlled by CCN. In the Spanish regulation, the National security Framework (Eqsuqema nacional de seguridad, defined

<sup>71</sup> <http://www.itczlin.cz/en/certification-products>

<sup>72</sup> <http://commoncriteria.pl/index.php/en/common-criteria-standard/common-criteria-in-poland>

in the "Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica") operates a classification of the system to be adopted in the public administration; at a high level, a certification against recognized european and international standard is requested. ISO 15048, is an explicit option described in the National Security Framework. In Italy, based on the national decree DPCM 17 February 2017<sup>73</sup>, it should be established a National evaluation and certification centre for verifying security and non-vulnerability conditions for products, devices and systems for networks, services and critical infrastructures.

## 1.2. Main challenges and the need for a EU approach

From the analysis of the international and national schemes the JRC Report<sup>74</sup> (Baldini et al., 2017) identifies a number of challenges, including:

- **Re-certification and patching.** This require the definition of a new process or a modification of the existing approach for Common Criteria;
- **Security and trust coverage.** Security certification with Common Criteria may not be enough to provide full security and trust of a product;
- **Certification costs.** Common criteria certification is considered a long and expensive process, which does not make it suitable for fast market deployment or relative short product cycles as in the consumer market
- **Non-applicability to specific products and systems.** Some classes of system and products are difficult to certify due their intrinsic features and characteristics.
- **Comparability and visibility of the certification.** Users do not have a clear metric of comparison among different certified products.
- **Usability.** The Common criteria certification does not give a clear and simple indication to the users of the provided level of trust. Metrics are missing for this purpose.

The report further stresses that in the energy sector some of the potential security threats are still not clearly understood and there is a growing body of research on security and privacy aspects of the energy sector including its evolutions to the Smart Grid. The complexity and scale of future power systems that incorporate smart-grid concepts will introduce many security challenges. With respect to the issue of the energy sector and of smart grids the Enisa report (2014) draws the following conclusions:

- **Price.** Current certification schemes are considered rather expensive due to fragmented national policies, lack of resources, the need for repeatability and consistency of the results and the large number of components involved in the smart grid supply chain;
- **Lack of a uniform approach.** Stakeholders are facing a fragmented situation where different initiatives regarding the cyber security of smart grids are being developed;
- **Long life cycle.** The certification process takes some time which usually is more than the time needed for new vulnerabilities to appear in the cyberspace.
- **Legal framework.** There are only a few legal texts concerning security in smart grids and this is leaving enough space for grey zones and/or interpretations.
- **Common Criteria.** Although is the predominant certification scheme in the market, it will be unrealistic to have a Common Criteria certificate for the whole smart grid supply chain; it should be extended to include specific protection profiles for the smart grid, similar to those related to the smart card industry, where a joint interpretation library was developed.

During the February 2016 Enisa workshop (2016a) MS representatives, among other things, voiced the following concerns:

<sup>73</sup> Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, Gazzetta Ufficiale n. 87 del 13 aprile 2017 (Italian Prime Minister Decree, 17/02/2017, Directive on guidelines for national cyber protection and cybersecurity, Official Bulletin n.87, 13/04/2017)

<sup>74</sup> Baldini, G., Giannopoulos, G., & Lazari, A. (2017). Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.

- Certification should be, in general, voluntary. Mandatory certification might be justified for some areas, or specific products, with high security requirements;
- Mandatory certification should be assessed carefully, as it may introduce economic/administrative burdens for European industry;
- During the design of the EU certification framework it should be taken into account that some Member States have national certification schemes for certain high assurance sectors, and both schemes should not be confused
- As SMEs are key to ensure economic growth in EU, any future mandatory certification scheme should not introduce unjustified barriers for SMEs to enter the market.
- Any proposed certification scheme should not create bottlenecks for introducing products to the market.
- Certification based on international standards (e.g. on ISO standards) would facilitate EU industry to operate globally.
- European certification is one pillar of the European Digital Single Market (DSM). While global interests should be taken into account, Europe and EU legislation have specific requirements due to a risk-based approach.
- European Member States which are non-members of the SOG-IS, were invited to join the mutual recognition agreement.

In a subsequent workshop taking place in October of 2016 (Enisa, 2016b) the following conclusions were adopted:

- Need of a roadmap for a European security certification framework;
- Certification framework should be based on different certification levels/schemes including self-certification (compliance assessment);
- Need of harmonized security requirements at European level;
- Accredited/licensed European security certification labs;
- Definition of roles and governance aspects for European security certification;
- Combination of security and privacy certification, when possible;
- Security certification per domain (sector) when necessary (e.g. IACS);
- Label as marketing / certificate recognition tool. If feasible, ICT security labelling could be associated with any certification level;
- Identification of the need to develop new underlying criteria for certification;

During a workshop organised by the French and German Certification Authorities (ANSSI & BSI, 20179) it was recognised that in the absence of an EU-wide cybersecurity certification scheme:

- Companies have to be certified individually in each country (except within SOG-IS);
- The Digital Single Market (DSM) is too fragmented;
- The reinforcement of digital security in Europe and user's trust can't be properly achieved;
- EU legislations adopt different approaches to security evaluation adding to the fragmentation of the DSM.

The same document concludes that, the development of an EU cybersecurity certification scheme should support the development and the well functioning of the Digital Single Market by:

- Reinforcing the security and trust in digital products, systems and services in Europe;
- Reducing fragmentation thus facilitating access to market for products, systems and services within the EU;
- Increasing companies' competitiveness through security;
- Building a leading security evaluation ecosystem in Europe ;

- 
- Contributing to making the EU an attractive and competitive digital player;

At the more general level of the security industry as a whole the problems that the EU is facing have been fully documented in the Communication and supporting SWD (European Commission, 2012a, 2012b). Although ICT security is only a part of the broader system of industrial security, it suffers from the same challenges evidenced in these two documents. First, the fragmentation along national and even regional lines has created 28 different security markets, a situation that is an anachronistic rarity in the European Union with several negative consequences for both the supply and the demand side creating market barriers and higher costs. Second, in large part the security market remains largely an institutional market where the larger buyers are public authorities. The SWD (European Commission 2012b) stresses that: a) no common system of certification exists at a European level for security equipment; b) there is no mechanism of mutual recognition across countries. Therefore, a producer of security technologies has to go through the costly and lengthy certification processes for each country in which he wants to commercialise his technologies.

The analysis of the above sources confirm that need for a European certification scheme that had already been suggested by various studies including (ECORYS 2011) and (ERNICIP 2014). A European security certification scheme should be set-up to overcome the national differences on security certification and support a European-wide cybersecurity market. The majority of countries, with or without a national framework, expressed their favourable opinion of setting a common European scheme that they could be part of, either as producers or consumers of certifications. To sum up the main drivers are:

- The need to harmonize the current national certification schemes (Germany, UK and France) and to cover areas not fully addressed in order to create a common European certification scheme based on a common approach
- Testing and certifying the cyber-security of IACS components/devices it is a needed step to take as it would bring a higher level of cyber-confidence to industry buyers and users.
- The need to establish a practical scheme guaranteeing mutual recognition of certificates across Europe and compatible with similar requirements beyond. The current collaboration schemes like CCRA and SOG-IS could be a starting point for the establishment of a common format and semantic of the certificates.

## 4. Policy objective and intervention logic

### Needs and strategic objective

In terms of needs the following three can be identified:

- (1) Reduce the current EU vulnerability and equally protect citizens, businesses, and public administrations
- (2) Forster dialogue, coordination, and trustworthiness in the cybersecurity ecosystem
- (3) Respond to the DSM, which identified cybersecurity gap as a key hindrance to the achievement of a digital single market and the cybersecurity standardisation was defined as one of its priorities (European Commission, 2015b)

As a result, the overall strategic objective of a EU cybersecurity certification and labelling scheme can be formulated as follows: *Create a European ICT Security Certification Framework that at the same time, avoids the fragmentation resulting from different approaches across European Union and is as close as possible up to international standards in order reduce trade hindrances*

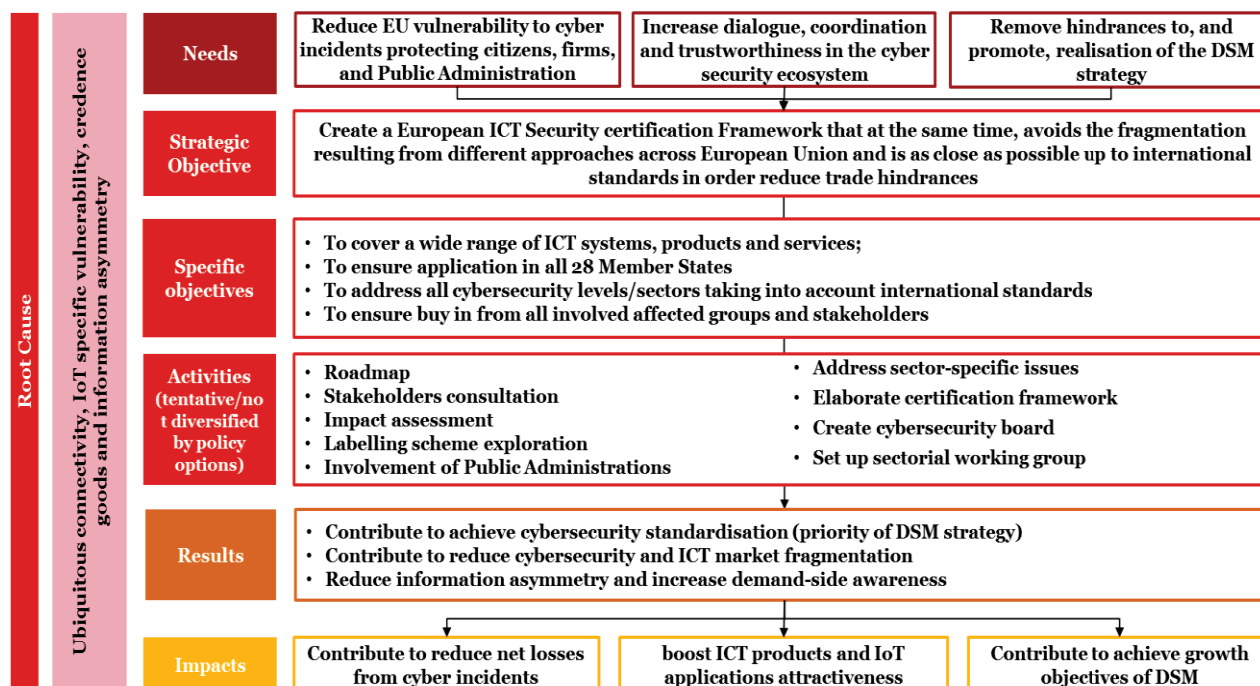
### Specific objectives

Descending from the analysis of the problem and from the formulation of the needs and of the strategic objectives the specific objectives are in our view the following: a) To cover a wide range of ICT systems, products and services; b) To ensure application in all 28 Member States; c) to address all cybersecurity levels/sectors taking into account international standards; d) to ensure buy in from all involved affected groups and stakeholders.

### Preliminary and simplified intervention logic

The Intervention Logic derived from the above sub-paragraph is depicted below and require no further comments.

**Figure 6 Certification scheme and labelling: preliminary Intervention Logic**



Source: own elaboration on secondary sources (obtained by the Commission and retrieved ourselves)

### 1.3. Policy options

The rise of cybercrime and security threats has spurred in recent years stimulating the emergence of national initiatives to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Albeit important, these initiatives bear the risk of creating single market fragmentation and barriers for interoperability. The proliferation of national certification and labelling initiatives increase costs for businesses operating cross-border and is likely to create obstacles for the internal market, as it raises the costs for companies/vendors operating across borders. This barrier is more significant for small and medium sized enterprises, which have usually less resources to dedicate to certification programmes. The risk of fragmentation of security requirements and related certification schemes emerges as an important concern for the industry. In the context of the public consultation related to the cPPP, some respondents emphasized that no reliable certification scheme exists at the moment at the European level, while some others pointed to the fact that existing national schemes act as barriers to market entry, complaining about the costs of complying with several certification schemes in Europe. Some of the industry associations state that further fragmenting the market with numerous certification schemes should be avoided.

On the other hand, while a European certification framework can reduce the costs and risks broadly sketched above and produce some benefits for both supply and demand, potentially negative impacts should not be overlooked. A mandatory security certification can introduce additional costs on the manufacturer and the citizen. While some types of products would require secure certification because of safety reasons (healthcare, road transportation) other products may be based on a voluntary basis approach. From an economic point of view, there is also the risk to introduce market distortion because large/midsize companies would be able to invest more money on the security certification process, while small companies could be excluded by some markets. The dynamicity of specific domains or technologies (e.g., IoT) introduces the issue of the staticity of security certification and of considering the life-cycle of the various products. This means that if a product is submitted to frequent changes, the security certification will be not worth the effort involved in the initial phases (on this see more also in the section on ICT certification labelling).

In April, a stakeholder consultation with DG CNECT (EC/ENISA, Towards a European ICT Security Certification Framework, April 27, 2017) concerning policy options was held. The presented options are briefly described here along with the results from the discussion with the stakeholders (as provided by DG CNECT):

#### Option 0

**No action.** The overwhelming majority of stakeholders stated that “no action” is not a viable possibility.

Under this option, the Commission would maintain the status-quo and not undertake any policy or legislative action. The option would result in the following situation:

1. The problem relating to the **limited information asymmetry and ineffectiveness/inefficiency of the current certification** schemes is **unlikely to be solved** in the absence of intervention.
2. As technology becomes increasingly complex and pervasive, it will be more and more **difficult for buyers to ascertain the security qualities of ICT** products and services.
3. In the lack of the proper economic incentives, it is also **unlikely that operators could establish self-regulatory measures fixing the existing information gap**. Such incentives are likely to exist only for markets where institutional or very organised buyers are present and can therefore exercise pressure on the side of the vendors.
4. The problem of **market fragmentation is very likely to increase** in the short-medium term (next 5-10 years) as a number of national and sectorial certification schemes are emerging.
5. The lack of coordination and interoperability across such schemes **hampers** the potential of **the digital single market**.

The **SOG-IS** agreement and the CCRAs **will not solve the problem** in the short-medium term. The criticism towards common criteria, on which SOG-IS is based, will remain an issue as the limited geographical and substantive coverage of the agreement.

Under the **Do-Nothing scenario**, the current situation would be continued and there would be no common EU wide system of Conformity Assessment and Certification (CAC). Security products subject to approval/certification requirements would continue to undergo national testing, validation and approval/certification procedures. No priority would be given to certain products. Furthermore, no additional development of EU-level structures and processes for the implementation of conformity assessment and certification requirements and procedures would take place.

Under this scenario the main impacts for **producers and suppliers** would be:

- **Costs of complying with multiple national procedures.** Multiple certification and conformity assessment country by country entails substantial costs.
- **Delay in ‘time to market’ of products.** Such multiple procedures prevent EU producers to enter rapidly all EU markets and achieve economy of scale and volumes to compete with third-country players.
- **Adaptation costs to meet national CAC systems.** Additional production costs may apply if variants of products are needed to get the certification in a given country.
- **Slow development and diffusion of new solutions.** Limited market access and scale reduce the incentives to R&D and innovation.

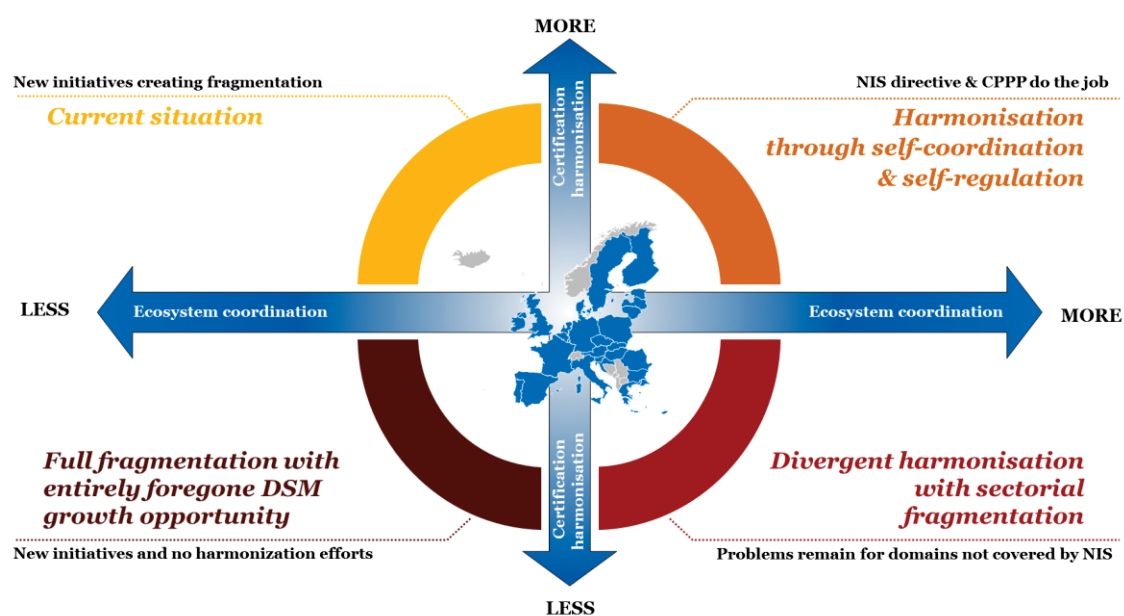
For **procurers** the status quo also entails lack of transparency and especially limited choices of suppliers, reducing the possibility to get the best value for money.

With no intervention in the Member States, only a limited number of **Certification Authorities** operate with quasi-monopolistic power. Obviously, this condition persists only because suppliers of security products are obliged to have their products certified in each Member State and cannot opt to have their product certified once for the entire EU.

In certain countries with well-functioning certification systems **regulators** may not perceive any immediate need for an EU-wide CAC scheme. However, many countries lack the technical expertise and capacity to support such functions. This may limit the scope for developing and implementing regulations requiring conformity assessment of security products and may result in insufficient or appropriate national regulatory frameworks for security products. Such circumstances may necessitate that Member States make reference to, and are reliant upon standards to certification procedures available from other Member States but which may not be aligned to their own national situations.

As a result of the various negative impacts illustrated above, costs are passed onto final users (both citizens and businesses) representing the negative impacts for **society** as a whole. Users of security products are not always able to buy the best security products at the lowest price.

**Figure 7 Scenarios under no action**



Source: own elaboration on secondary sources (obtained by the Commission and retrieved ourselves)

---

## Option 1

**Soft law tools.** EC would encourage MS and industry initiatives, such as developing relevant guidelines and methodologies, and promote MS participation to SOGIS-MRA. This solution should have low costs but is not expected to adequately address the fragmentation risk.

## Option 2

**SOGIS mandatory.** EC would make SOGIS-MRA mandatory for all MS. This solution would allow only the Common Criteria approach, so leaving out, e.g., some national approaches based on low time/cost/assurance requirements.

## Option 3

**Framework option.** EC would mandate the creation of the EU cybersecurity certification and labelling framework based on a board made of the 28 cybersecurity agencies. The framework could initially rely on Common Criteria and (extended participation to) SOGIS-MRA. Different certification approaches would be submitted to the board, and, if accepted, would gain mutual recognition within EU. A secretariat run with the assistance of an EU agency or body (e.g., ENISA) would ensure efficiency within the framework. Working group under the board would capture/anticipate the certification needs from different industry sectors, so triggering, via board approvals/decisions, the creation of the needed tools (e.g., the relevant protection profiles). Even though the corresponding costs need to be well analysed, this solution seems to be flexible and manageable enough to meet the relevant expectations, as confirmed by a majority of the participant stakeholders.

The following points demonstrate the potential positive and negative impact of having an EU general ICT Security certification and labelling framework structured by type of affected player.

Producers:

- **Reduction of costs associated to multiple testing to obtain national certification and labels.** Security products will have to be certified only once rather than multiple times, thus reducing overall conformity assessment and certification costs;
- **Reduction of adaptation costs to meet national product standards/specifications.** Common EU product standards reduce the need to produce product variants adapted to meet different national standards;
- **Reduction of the need for product trials for Priority and sensitive security products<sup>75</sup>.** The possibility to certify products meeting EU requirements after initial trials should reduce the subsequent need for further national and/or client trials;
- **Reduction of the ‘time to market’ of products.** Having obtained EU certification, products may be introduced to the whole EU market without delays caused by the need to obtain national certification;
- **Improved alignment of production to the expected EU market as a whole.** Production (of certified products) can be aligned at the outset to the expected size of the EU market rather than being conditioned on the uncertain timing associated with obtaining national certification;
- **Reduction of risk that competitors are able to ‘replicate’ new product developments and innovations.** Simultaneous access to the EU market as a whole limits the opportunities for competitors to use in a strategic manner delays in obtaining national certification to launch competing products;
- **Enhanced transparency of performance requirements and standards / specifications.** Common EU performance requirements and conformity assessment protocols should enable

---

<sup>75</sup> Priority and sensitive security products are security products and solutions addressing ‘unfamiliar’ or new types of threats that require the development or application of new technologies, and equipment and may be extended to changes in organisation and implementation of security functions; for example through the automation of security functions.



producers to better develop products according to 'predetermined' criteria, reducing uncertainty of product conformity assessment outcomes;

- **Acceleration of development process.** A common regulatory framework with reference to defined product standards/specifications should make it easier for producers to direct their RTD efforts to meeting regulatory/market requirements.
- **Negative impacts.** Potentially negative impact for producers relates to the additional costs of obtaining EU certification and labelling (for products that are currently not covered by national conformity assessment and certification and labelling requirements but that will be brought within a future EU-wide system). However, in a longer-term perspective, certification could be an investment for companies and transformed in a market advantage. In fact, the savings obtained from one certification instead of multiple certifications could be reinvested, for example, in research and innovation.

#### Market conditions:

- **Increased transparency regarding product performance.** EU certification and labelling provides an indicator of product performance based on common standards/specifications and, hence, increases market transparency;
- **Increased market openness.** Increased market transparency should reduce market entry barriers by facilitating market acceptance of (certified) products offered by new market entrants and reducing the importance of "reputation effects";
- **Increased competition in security product markets.** Greater market transparency and openness should reduce fragmentation and increase the level of competition within markets. Existing suppliers will be more easily able to serve different national markets, which may be particularly beneficial to SMEs. The EU market would also be more attractive to new entrants, both new business start-ups and non-EU based suppliers. Increased competition should put downward pressure on the price of security products, which reduces costs for procurers / users of the products;
- **Increased competitiveness of European manufacturing industry.** Increased competition should drive improvements in productivity performance by forcing improvements in production efficiency and/or raise value added (e.g. higher value-added products). At the same time, improved market access that increases the size of the potential market for new products, should provide a positive incentive for producers to engage in RTD activities and promote innovation. Finally, EU certification may support exports of products to markets outside the EU if it engenders greater recognition in international markets than the existing multitude of national certification schemes.
- **Negative impacts.** The main identified potentially negative impact on market conditions concerns the possibility that minimum EU standards may become de facto market requirements. This may, in turn, reduce the market opportunities for products with performance levels above minimum requirements and, reduce, incentives for investments in RTD to raise product performance. Similarly, it may limit market acceptance of 'alternative' or 'innovative' products, particularly if they are costlier than standard products that comply with minimum requirements.

#### Procurers and users:

- **Lower price for security products.** As outlined above, there are a number of impacts that affect producer costs and prices and that should feed through to the purchase cost of security products;
- **Increased product choice / availability.** Increased market openness should result in more suppliers on the market. At the same time, a less fragmented EU market should promote RTD and innovation and raise entry into the market of new technologies and innovative solutions;
- **Enhanced information / transparency on product performance.** An EU-wide conformity assessment and certification scheme should increase market transparency and provide potential purchasers with greater information on product performance. This should contribute to reducing information asymmetries between purchasers and producers;
- **Facilitation of procurement procedures.** Procurers – and where relevant regulatory authorities – would be able to include EU standards and an EU certification as a requirement in their contracts. Furthermore, an EU wide scheme with mutual recognition of certification should support greater openness in procurement procedures by making it easier for potential suppliers

---

## Certification Authorities

- **Change in the volume of demand for CAC (Conformity Assessment and Certification) services.** A single 'one-stop' EU-wide approach should decrease total number of CAC procedures required for each individual product. However, bringing products currently not covered by national CAC requirements within the scope of an EU-wide scheme should increase in the volume of demand for CAC procedures. The overall balance will depend on the actual scope of an EU-wide conformity assessment and certification scheme(s);
- **Increased competition for the provision of CAC services.** For Type-1 products, the introduction of an EU-wide CAC scheme should remove the controlling position that CAC bodies are able to occupy over their national markets, thus promoting competition between CAC bodies. For Type-2 products, the scale of the existing infrastructure for conformity assessment and testing relatively limited, making it difficult to assess the impact of a 'one stop' EU system on competition and on the cost and quality of CAC service provision;
- **Strengthened EU-wide accreditation.** For Type-1 products, it is foreseen that there will be EU accreditation of conformity assessment and Certification Authorities following common rules and requirements for obtaining accreditation. For Type-2 products, it will be essential that appropriate checks are made to assure the quality and independence of CAC service providers. This implies a strong emphasis on the accreditation of conformity assessment and Certification Authorities. Accordingly, part of the implementation of an EU CAC system for Type 2 products would relate to the development and operation of the infrastructure and procedures for accreditation of conformity assessment (e.g. Conformity Assessment Body) and Certification Authorities;
- **Increase of administrative costs related to the CAC system.** For Type-1 products it is foreseen that conformity assessment and Certification Authorities will be EU accredited, which will result in corresponding (additional) administrative costs. For Type-2 products, the introduction of an EU-wide CAC system together with the definition of product requirements and technical standards/specifications would require the development of a corresponding organizational structure. Again, this implies some additional administrative costs.

## Regulators

- **Conformity with EU standards as a basis for national regulations.** The development and introduction of European Standards and an EU-wide CAC scheme may make it easier for national authorities to introduce national regulations setting product requirements aligned to these standards;
- **Facilitation of regulations through existence of conformity assessment infrastructure.** The existence of an EU-wide CAC system could remove the need to countries to independently develop such an infrastructure. This may reduce the associated CAC infrastructure costs from introducing regulatory requirements for security products. In turn, this may speed-up the adoption of regulations as there will be lower cost and shorter delay in meeting the corresponding requirements for a CAC infrastructure/scheme to verify compliance with regulations.

## Society

- **Raised average security performance characteristics of deployed products.** By ensuring that all products meet minimum requirements, an EU-wide CAC system should raise the average performance level of deployed security products. However, there may be risks that an EU-wide CAC system may have a negative impact on overall security performance if it reduces incentives for the development of products with performance characteristics above EU (minimum) requirements;
- **Accelerate the deployment of security products.** To the extent that an EU legislative and CAC 'package' accelerates the deployment of security products (e.g. reduced time to market), particularly to address new threats, it should have a positive impact on security.

## *The costs of fragmentation: indicative estimations*

Lack of standardisation of technical rules and of mutual recognition together with the cost of multiple conformity assessments and certification has long been recognised as one of the main barriers to the single market (Ilzkovitz et al., 2007, pp. 59-63). The fragmentation of in ICT security certification and labelling is just one manifestation of such phenomenon. Depending on the industry such fragmentation and the need of multiple conformity assessments can cost to enterprises between 2% and 15% of their production costs (Ilzkovitz et al., 2007, p. 61). Based on this estimation produced by DG ECFIN economists, it is possible to first produce the following high level and indicative calculation:

- According to PwC and LSEC Cyber Security market study<sup>76</sup> the EU cyber security market is estimated at 157 € billion;
- To be conservative, we assume that industry aggregate production costs are 40% of the market value (63 € billion), and that only 60% of products require certification, so that the total relevant value for production costs is 38 € billion (60% of 63 € billion);
- Again remaining on the conservative side, if we use only the lower bound (2%) from DG ECFIN analysis, the total costs of multiple testing due to fragmentation for the entire EU cybersecurity industry would amount to 760 € million per year.

This high level and indicative aggregate calculation could be further contextualised and applied in more granular fashion to very specific sectors. Ecorys (2011, p. 48 and pp. 209-211) has applied the same line of reasoning illustrate above for the very specific sector producing 'intruder alarm systems'. Currently a producer of a security alarm system seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates from different Member States. This certification including but not limited to:

- **CertAlarm<sup>77</sup>**: The CertAlarm Certification Schemes provide a proof of conformity the European (EU) product, system, installation and service standards. The scheme is based on the principle of independent third-party assessment and certification of security products. In February 2011, the European cooperation for Accreditation (EA) confirmed the status of CertAlarm as a scheme covered by the EA Multilateral Agreement (MLA). The CertAlarm Certification includes some standards on IP interoperability implementation based on Web services for each kind of alarm<sup>78</sup>.
- **Common Criteria**
- **EuroPriSe** (Privacy for IT products): EuroPriSe, the European Privacy Seal, is a European scheme providing privacy and data protection certification for IT products and IT-based services. The European Privacy Seal embodies a visible trust mark certifying that a product or service has been checked by independent experts and approved by an impartial privacy organisation. The EuroPriSe website privacy certification is awarded to websites that are compliant with EU data protection law and that meet all of EuroPriSe's high-quality data protection requirements. Specifically, the evaluation covers publicly available parts of a website and focuses on the interaction between a web server and the browser of a visitor on the website. This includes topics such as cookies, IP address processing and social plugins<sup>79</sup>.
- **ONVIF and PSIA** (Video surveillance): the Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA) are two recently created organisations with the aim of developing interoperability standards for Internet Protocol (IP) based security systems. Both these bodies are promoting conformity schemes based on manufacturers undertaking their own conformance testing. ONVIF's Profile Q offers the advanced security required in today's technological world, giving integrators and end users the necessary protections from today's cyber security threats, in addition to providing out-of-the-box interoperability<sup>80</sup>.
- **Alarm System Certificate<sup>81</sup>**: The alarm system Certificate is the UL Mark for programs designed to meet the needs of alarm service providers, their customers, and interested stakeholders. It is the

<sup>76</sup> The study is still ongoing and the preliminary results presented within the Interim Report are updated to June 6, 2017.

<sup>77</sup> ECORYS. (2011). Security Regulation, Conformity Assessment & Certification. Brussels: Report delivered by ECORYS for the European Commission.

<sup>78</sup> [http://www.certalarm.org/ca/sites/default/files/Scheme%20Rules-2-Iss\\_5.pdf](http://www.certalarm.org/ca/sites/default/files/Scheme%20Rules-2-Iss_5.pdf)

<sup>79</sup> <https://www.european-privacy-seal.eu/EPSe-en/website-privacy-certification-overview>

<sup>80</sup> <https://www.ifsecglobal.com/onvif-introduces-profile-q-to-tackle-cyber-security-challenges/>

<sup>81</sup> <http://industries.ul.com/blog/alarm-system-certificate>

---

alarm company's declaration that the system will be installed, maintained, tested and monitored in accordance with applicable codes and standards. The Alarm System Certificate includes a cybersecurity standard (UL 2900)<sup>82</sup>

- **ISA/IEC-62443 (formerly ISA-99):** ISA/IEC-62443 is a series of cyber security standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems. The concept of manufacturing and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and control systems include, but are not limited to<sup>83</sup>:
  - o hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems
  - o associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.
- **IECEE CB Scheme<sup>84</sup>:** The CB Scheme is an international program created by the International Electrotechnical Commission for Electrical Equipment (IECEE) for the acceptance of product safety test results among participating laboratories and certification organizations around the world. The CB Scheme offers manufacturers a simplified way of obtaining multiple national safety certifications for their products — providing entry into over 50 countries.

Their estimation is that, under an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU and would avoid multiple testing in several national market, the cost savings for intruder alarm systems would amount to a range of EUR 4.7 million to 9.9 million per year. As this is a very tiny sector within the broader cybersecurity industry, the above estimate of total costs of fragmentation in the range of 760 € million per year seems reasonable.

---

<sup>82</sup> [http://industries.ul.com/wp-content/uploads/sites/2/2016/04/UL\\_CAP-Overview-Info.pdf](http://industries.ul.com/wp-content/uploads/sites/2/2016/04/UL_CAP-Overview-Info.pdf)

<sup>83</sup> <https://www.isa.org/isa99/>

<sup>84</sup> <http://www.intertek.com/marks/cb-scheme/>



EUROPEAN  
COMMISSION

Brussels, 13.9.2017  
SWD(2017) 500 final

PART 5/6

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF  
THE COUNCIL**

**on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013,  
and on Information and Communication Technology cybersecurity certification  
("Cybersecurity Act")**

{COM(2017) 477 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

## Table of contents:

<b>5. Stakeholders’ support</b> .....	59
<b>6. Work Plan</b> .....	75
<b>6.1. Update on Project Tasks</b> .....	77
6.1.1. <i>Task 1: Evidence Gathering and Analysis</i> .....	77
6.1.2. <i>Task 2: Assess the impact</i> .....	81
6.1.3. <i>Task 3: Other specific tasks</i> .....	82
6.1.4. <i>Task 0: Project Management</i> .....	84
<b>7. Annex</b> .....	87
<b>7.1 Minutes of the interviews</b> .....	87
<b>7.2 Questionnaire</b> .....	118
<b>7.3 Stakeholder Mapping</b> .....	134
<b>7.4 An overview of criticism related to Common Criteria</b> .....	145
<b>7.5 Cyber Security market Insights</b> .....	148
<b>7.6 Case Study – “The impact of an EU wide Certification Scheme on Smart-Meter Industry”</b> .....	152
<b>7.7 Case Study – “The impact of an EU wide Certification Scheme on Alarm Systems Industry”</b> .....	155
<b>7.8 Case Study – “The impact of an EU wide Certification Scheme on Cloud Computing Industry”</b> .....	159
7.9 IoT Trust Label - Proposed Requirements as a Basis for Endpoint Trust Labels (from Stakeholder Support) .....	164
7.10 German Ministry of Interior – Study on “Introduction of a label of quality for IT security features of Internet-enabled products” .....	171
7.11 Cyber Risks and Cyber Resilience of Critical Infrastructures .....	174
7.12 The Lack of Appropriate Standards and the Need for a Common International Approach .....	179
7.13 Economics of Standards .....	185
<b>7.14 References</b> .....	186



## 5. Stakeholders' support

The following section described the information gathered through interview activities to selected participants from these categories:

- Smart meters Industry
- Semiconductors industry
- Other private sector representatives
- Members of ICT Certification Authorities

Questions were asked in order to cover the following areas of interest:

- Evidence of fragmentation
- Labelling and information asymmetry
- Policy Option 1: Non-legislative "Soft-law" measures
- Policy Option 2: EU legislative act to extend SOG-IS agreement to all MS
- Policy Option 3: EU general ICT security certification and labelling framework
- Institutional costs

### 5.1 Evidence of fragmentation

Interview data gathering activities provided key examples of fragmentation of ICT Security Certification across Europe pinpointing what are the cross-border trade challenges the industry must face when entering the market of several EU countries.

Representatives from smart meters industry provided a position on fragmentation in the field of smart metering products, which is worth reporting: *"If the question is: Are there countries that accept each other certificates? The answer is no"*. As example, it has been explained that there are currently three certification for smart-meters in three countries. In the UK, the certification scheme is called the CPA (Commercial Product Assurance), which is a scheme applied for smart-meters but also for other products. In France they have the CSPN (Certification de Sécurité de Premier Niveau) certification scheme and in Germany they have their own protection profile based on Common Criteria. There are also national communications infrastructure for devices connected to smart-meters including interfaces with the different stakeholders involved such as the German Smart Meter Gateway and in the UK the so-called "Communication Hub". These are all examples where additional certification requirements are needed for a vendor to access the market of these countries.

Specific examples of fragmentation are widespread. For instance in the field of VPNs related network products, although VPNs are certified against a "collaborative" protection profile (cPP), meaning that the PP has been harmonized with International Mutual Recognition Arrangement, vendors wanting to access the French market have to undergo the additional CSPN certification process (and in some cases a completely new common criteria evaluation). This means that the VPNs requirements must be certified through national approval which in the French case will last from 6 to 9 month and the costs are estimated to around 80k euros as well as the EU approval process which is free of charge but takes 2 months to be completed.

Market fragmentation within the EU exists even for trust service products, which have been certified against US FIPS certification schemes. For Hard Security Modules initial certification of the crypto module acquired through the American FIPS), and the SOGIS members, via CEN, request for additional Common Criteria certificates with related vulnerability analysis. Some



European countries accept FIPS certifications for electronic signature products as equivalent to Common Criteria certified, yet other certify their products exclusively through the CC. The share of products certified with both systems, therefore allowing the vendor to sell its product in both US and European markets is even narrower.

Additionally for SSCD products, there are examples in SOGIS Member States where the original common criteria certification is not sufficient for national needs and the product has to undergo again the certification process of that country.

Respondents from National ICT Certification Authority pointed out the fact that fragmentation may exist even within the same country. This may happen as in the case of Italy, where procurement requirements may be established by administrative subject with a fair degree of autonomy. There is also a second example. In Italy, a public local authority (Provincia di Trento), in a public procurement procedure<sup>1</sup> has recommended the security certification of a video surveillance system according to Common Criteria (low assurance, i.e., EAL 1). Duration and costs of this security certification can be estimated in about 6 months and 20K euros.

The interviewees from smart meters industry provided some concerns on the future scenario of multiplication of national certification schemes for what concerns the industry of smart-metering if no action is taken. If MS continue not to accept each other Certification schemes, each MS will continue to improve its own Certification scheme and this could create a strong legacy making harmonisation more difficult. Furthermore, such fragmentation is also happening on the evaluation side. There are only limited number of Conformity Assessment Body that are able to certify against the requirements of different schemes. In this way, additional market entry barrier are created. The interviewers explained that the single most important barrier to trade for the smart metering industry are the costs for certification. Without specifying better the unit of analysis, the respondent stated that the cost of certification is about 1 million and the SMEs are out of this gain. In Germany, only one of the biggest smart-metering companies is starting a certification to enter other markets and all the other companies are present only in the German market".

## *5.2 Labelling and information asymmetry*

Interviewees from several interviews addressed the issue of information asymmetry. For Semiconductors industry representatives the situation is today polarised between products for public security and consumers' product. For the former certification is long and costly and only the big company can manage such processes. At consumers' product level the requirements are lighter, but what is currently needed are solutions that are in between these two extremes. Currently, there is also the need to raise awareness about the importance of security using some forms of labelling schemes. On the other hand, according to some respondents the market problem is not one of fragmentation but rather of awareness and demand.

For Semiconductors industry representatives it is paramount to distinguish customers from users when trying to assess whether there is an information asymmetry with behavioural impacts. The final consumer is not well informed on the security properties of ICT products/services, this is due to a lack of awareness due to absent labelling. From the point of view of industry and government customers, the information in labelling schemes is likely to have an impact on its behaviour and purchases. An example can be found in cable TV that need to be connected to a router for internet connections, these products do not respond to specific security requirements and are vulnerable to hacker attacks. On the other hand, consumers are not aware of this kind of deficiencies, so they continue buying products without considering security requirements.

---

<sup>1</sup> Further details are not available

According to Smart meters industry representatives the situation on information asymmetry is different if we consider business-to-business products. The suppliers buy millions of meters and they of course have good understanding of security specifications of the products and in this domain labelling would not be of much use.

On the other hand, labelling and other means to reduce information asymmetry are important to increase trust in the public and the government should be very interested in this topic. The public opinion is more concentrate on privacy issues (e.g. personal data). For smart-meters, in UK, there is a display connected to the meters and consumers can simply read data on this display. There are devices connected with meters and you could be connected to the meters and read data where you want. The consumer decision to buy a product is often on the utility of the product. You should differentiate what products/device needs to be certified and what devices needs to be labelled.

### *5.3 Policy Option 1: Non-legislative "Soft-law" measures*

Whilst some interviewees explained that voluntary labelling schemes and other non-legislative measures may provide some benefits to the industry, this policy option does not stands on its own feet as a way to address the main concerns of market fragmentation and information asymmetry.

On the positive note by letting the industry voluntarily put forward their own labels in coordination with public authorities it allow it to provide information to the users in a cost-efficient way.

The value of voluntary schemes and industry labelling initiatives is positive when considering the national level. Yet when considering cross-border trade of ICT products voluntary labelling approaches seem to pose additional problems. In fact, consumers may have awareness for labels existing at the national level but less so for labels from other countries, which do not abide to a certain degree of cross-country standardisation.

Furthermore, voluntary labelling initiatives may avoid some market inefficiencies that arise with regulated certification schemes, particularly for national or regional schemes that define standards and evaluation methodology and only recognise certain certification bodies within their own territory. Therefore, mandatory certifications which may introduce economic/administrative burdens could be limited by relying on voluntary schemes, which provide greater industry flexibility and rely on a lightweight system to demonstrate to their customers the security level of the products they market.

Against this background, labelling schemes without a sound legal and mandatory framework may lose their purpose in terms of trust and reliability. In fact, the deficiency of such non-legislative policy measures depends on the good will of the industry that adopt such measures and on the likelihood of providing trusted and reliable information to the users.

Labelling also depends on the user perception and quality of information. In fact, for the end-user such labels may lead to more confusion. If the label is too simple, the user could misunderstand the corresponding information. If the label is too complex, the user could be unable to understand it. With respect to business-to-business, marketing the impact of voluntary labelling may not be the most conducive argument in reducing market fragmentation and information asymmetry. When having to purchase very high quantity of products the certification behind the label and the security specifications of the product may be considered more important.

### *5.4 Policy Option 2: EU legislative act to extend SOG-IS agreement to all MS*

To face the challenges of market fragmentation and information asymmetry in the ICT security sector the option of extending the SOG-IS agreement to all EU member states did not receive support from any of the interviewees.

The reasons are varied. For Smart meters industry representatives, decision-making between all EU countries may be too burdensome. At the moment SOG-IS goes up to EAL-4 and up to EAL-7 for specific domains. The challenge with SOG-IS is the unanimity of the Member State.

One critique addressed to the extension of the SOG-IS is that the agreement is based on the Common Criteria, which is not the right solution for ICS at the moment (please refer to Annex 7.4 for a developed overview of the criticism of the Common Criteria). Common Criteria costs 500k and lasts more than one year, which is a problem for a vendor. Common Criteria may be a good approach for some kinds of components and products. When the lifecycle of a product is longer than 20 years, we have to find approaches at a system level based on procedures and self-declaration.

The extension of SOG-IS agreement to all MS is not a valid policy option to be considered since there are Member States which are too small and for which the start-up and maintenance of a Certification Authority may be too costly. Not all countries have the ability to join the SOG-IS agreement. Therefore, there is a question of trust between governments. Procedures in France may receive more trust compared to certification procedure in other countries, making their activities superfluous and too costly.

### *5.5 Policy Option 3: EU general ICT security certification and labelling framework*

According to the opinions provided by stakeholders interviewed, an EU ICT certification scheme could be a valuable policy options to face the challenges of market fragmentation and information asymmetry of ICT security products.

Representatives from ICT Certification Authority claims that there is an urgent need to establish a proper EU framework that will analyse, select and improve, where necessary, the acceptable approaches for EU wide certification, and will rationalize the certification decisions for both MSs and industry. Harmonizing will only be possible through technical exchanges between the MSs Schemes, which obviously relies on open certification approaches.

The interviewees from ICT Certification Authority think that a mutual recognition agreement of certification schemes existing in different countries have indeed a positive impact on industry costs. As remarked by the Certification Authorities, obviously a recognition agreement would eliminate the need and cost of re-certification in the domain covered by the agreement.

For Smart meters industry representatives it would be welcome to have one methodology on how you asses the risk, how you define security requirements and how you go through certification and a recognition across Europe. It is very important to have flexibility in certification scheme, determine on the risk connected to the product evaluated and the risk connected to the location of the product. Moreover, if MS continue not to accept each other Certification schemes, each MS will continue to improve its own Certification scheme and this will create a strong legacy to be later overcome in order to introduce a general EU framework.

Questions were also addressed on the institutional responsibilities that an EU management board of a possible EU wide certification framework would have. An interviewee explained that ENISA could play a role within industries to help to understand the concerns of the different national agencies. For smart-metering industry representatives, ENISA can play a key a role to harmonize Members States' Agencies on definition of national requirements and assurance, by making sure that the solutions meet the needs of the industry. ENISA should also cooperate with European and international standardisation institutions. Working with ENISA, it would be important to understand and harmonize the security language of the energy sector, in order to understand each other complementing both energy and smart-meters sectors. Therefore, representative from Smart meters industry explained it would be important to combine the approach of DG CNECT with the approach of DG ENERGY.

## 5.6 Institutional costs

Insights from the interviews to representatives of national ICT Certification Authorities as well as desk research on start-up and maintenance costs of institutions similar to ENISA have been done to provide the following estimates:

1. Costs incurred by an IT Certification Authority for the participation in the SOG-IS MRA
2. Costs incurred for the start-up of an IT Certification Authority
3. Costs incurred for the operational management of an IT Certification Authority
4. Costs estimated for the start-up of an EU wide ICT framework management board (6 months)
5. Costs estimated for the running of an EU wide ICT framework management board

These estimates are supported by a separate excel file listing the data entries and underlying calculations presented below in a more extended and narrative mode.

### 1.2.1. Costs incurred by an organization for the participation in the SOG-IS MRA

In relation to the costs incurred by an organization for the participation in the SOG-IS agreement the consortium asked its interviewees to provide the related break down of costs such as the ones to support harmonization activities and to participate into SOG-IS technical meetings.

Representative from National Certification Authority explained that MC meetings take place 1-2 times per year and the JIWG meetings 3-4 times per year respectively. The interviewee explained that on average the yearly travelling costs for **three members** attending **six meetings** are approximately **33 thousand euros**. In addition, for the preparation of meetings, attendance and national reporting the personnel cost estimated for 0,5 FTE of an Assistant is approximately **25 thousand euros**.

Therefore, for one of the Certification Authority that were interviewed the costs incurred for the participation in the SOG-IS MRA are approximately **58 thousand euros**.

### 1.2.2. Costs incurred for the start-up of an IT Certification Authority

Secondly, the consortium aimed at gathering data on the costs incurred for the start-up of an IT Certification Authority such as the costs related to staff competence building on ICT security certification, process setup, accreditation of Conformity Assessment Body and institutional communication etc.)

However for one of the interviewees it was impossible to provide any cost estimate for the start-up of the ICT Certification Authority as it was were created long time ago and most of the personnel initially involved is no longer operative. Moreover, in some cases, analytical cost records on IT Certification Authorities creation were not collected. However, the interviewee stated that the most time-consuming activities were related to drafting of IT Certification Authorities procedures and overall organization compliant to mandate received from the Government law and international standards.

Another interviewee from ICT National Certification Authority stated that costs estimate for setting up a Certification Authority is approximately **1.2 million** euros for 3 years. Total costs for the whole scheme, consisting of one Certification Authority and two ITSEFs (Conformity Assessment Body) is estimated to approximately **5 million Euros**.

### *1.2.3. Costs incurred for the maintenance of the operational management of a Certification Authority*

Thirdly, we asked to ICT Certification Authorities representatives to provide some estimates of the costs incurred for the management of their institution (i.e. costs related to infrastructure and personnel, maintenance of technical expertise, management of the schemes etc.).

For one of the interviewees two main cost items must be considered. For the maintenance of the operational management of a Certification Authority, an organization needs 5 person/year. Work force is needed, on the one hand, for product certification activity, on the other hand for the management of the scheme at national level (initial accreditation and periodic reassessment of private Conformity Assessment Body, exams for evaluators and other experts assisting the scheme). The total personnel cost, considering the estimate of approximately 140 thousand euros for 2 Administrator (AD5) and 150 thousand euros gross (with taxes and contributions paid by the employer) for 3 Assistant (AST3), is **approximately 290 thousand euros**.

### *1.2.4. Costs estimated for the start-up of an EU wide ICT framework management board (6 months)*

In the context of an EU wide ICT Security Certification Framework, the costs estimated by the Consortium for the start-up phase of a Management Board are described below, taking into account all the assumptions and data considered. However, the Consortium provides a raw estimate considering that a more detailed analysis would be necessary in order to have a more accurate capacity plan. The following proposal is based on a preliminary analysis of the existing ENISA organizational structure and desk research on the functioning of other European Agencies (e.g. EASA<sup>2</sup>).

As provided in the ENISA Regulation (EU) No 526/2013, the bodies of the Agency comprise<sup>3</sup>:

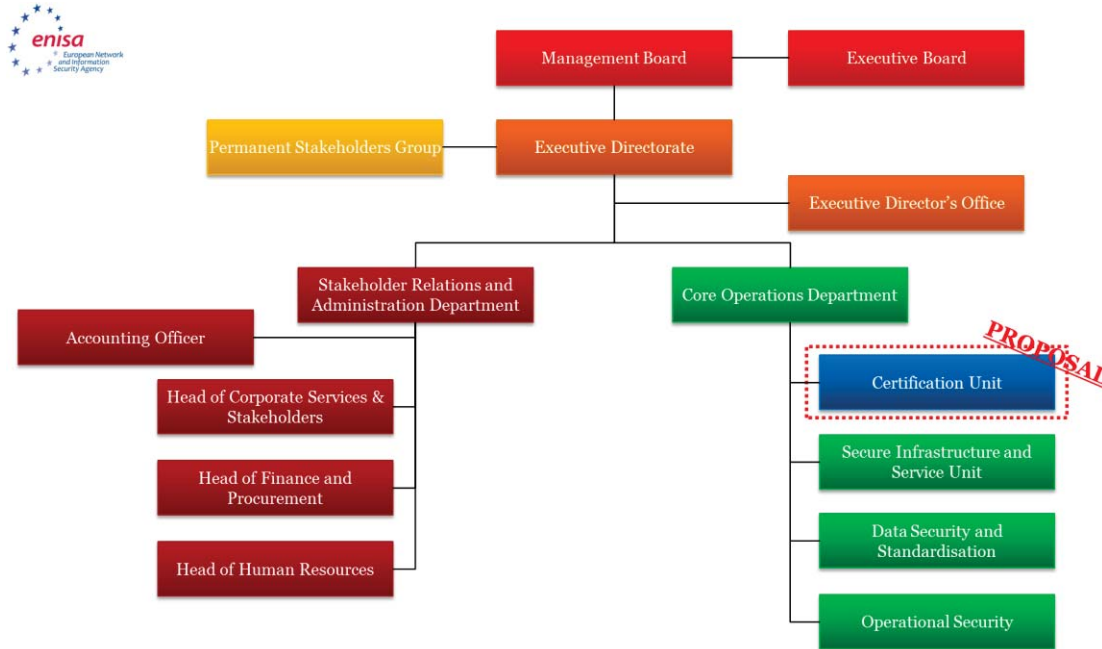
- **A Management Board:** The Management Board is ensuring that the Agency carries out its tasks under conditions which enables it to serve in accordance with the founding Regulation.
- **An Executive Board:** The Executive Board is preparing decisions to be adopted by the Management Board on administrative and budgetary matters.
- **An Executive Director:** The Executive Director is responsible for managing the Agency and performs his/her duties independently.
- **A Permanent Stakeholders' Group:** The PSG advises the Executive Director in the performance of his/her duties under this Regulation.

---

<sup>2</sup> EASA is the competent authority to issue type certificates for aircraft, to approve changes to the type design etc. Before issuing the certificate or approval, the Agency has the obligation to assess the design and that the applicant has demonstrated compliance. This can be done by a 100% check of everything, by sampling some parts etc.; in the end of this process the Agency needs to be "convinced" that that the design is safe (airworthy) and that it can legitimately issue the certificate / approval. "Level of Involvement (LOI)" is a method / concept trying to formalise this checking / verification function. EASA does it already today, but not in a formalised, objective and transparent manner. Only few guidance is given by EASA to its staff members: based on his/her engineering judgement, experience with the applicant etc. The Agency has to determine its involvement on a risk based approach and will provide the criteria that the Agency should use in that exercise. The risk, as it will be defined in the law, is that a design is not compliant with the rule, because the Agency has not verified this part of the project, and that this non-compliance has an impact on safety. The objective is to focus in the future the resources to where it is necessary: where the highest risks are.

<sup>3</sup> <https://www.enisa.europa.eu/about-enisa/structure-organization>

A new Certification Unit or a specific team within one of the existing ENISA units (depending on the size of the team) would be necessary in order to ensure the functioning of an EU wide Certification scheme. Here after is presented a proposal of the new ENISA structure and organization, based on the information gathered during the first part of the activities and on a preliminary analysis of the existing European agencies (e.g. EASA):



**Figure – Proposal for the New ENISA Structure and Organisation**

The start-up activity is estimated in 6 months. This phase would include all activities needed to set up the Framework, the definition of the organizational structure and responsibilities for each role. It would also include the definition of procedures rules and the terms of reference of the Board as well as the negotiation and validation with the Member States.

The corresponding main costs can be clustered as follows:

- A. External Experts
- B. Skills development and training
- C. Website Creation

Taking into account all the data and assumptions shown above, the total cost estimated for the start-up phase is **280 thousand euros**.

Description	Unit #	Unit of measure	Occurance	Unit price	Sub-Total	Total	Cost Tipology
Expert	3	Person	1	€ 75.000,00	€ 225.000,00	€ 225.000,00	Event-based
Skills Development and training	0,4	Person	1	€ 75.000,00	€ 30.000,00	€ 30.000,00	One-time
Website Creation	1	Price	1	€ 25.000,00	€ 25.000,00	€ 25.000,00	One-time

**GRAND TOTAL € 280.000,00**

- A) The major costs are related to Personnel expenditures. Three Experts would carry out the activities during the 6 months duration. The three external experts will have to be followed and coordinated by at least two ENISA employees that do not represent additional costs as they are already remunerated by ENISA. According to ENISA procurement rules<sup>4</sup>, each selected Expert can be remunerated with a fixed fee of €450 per person-day plus any travel and subsistence related costs, which will be based on the European Commission's standard 'Daily allowance' or per diem rates for each European Country. To better estimate the travelling cost and allowances for each experts, the Consortium have taken into account a study specifically conducted for another EU Agency on the "Experts Meetings". During the start-up phase, considering for each experts 130 working days in 6 months, a very rough estimate of the total fee is:

**Total Fee for each Expert:** 130 working days \* 450€ + 11'000€ (Travelling cost estimate) + 5'000€ Allowances ≈ **75'000€**

Travelling cost includes:

- Tickets
- Travel Agency Fees
- Catering
- Shuttle
- Allowances (attendance fee, accommodation allowance, other transportation cost to be reimbursed)

In addition to the travelling cost, 5 thousand euros of other Allowances (e.g. health insurance) are to be considered.

Considering three Experts for the Start-up phase, the total estimated cost for personnel is **225 thousand euros**.

- B) Moreover, during the start-up phase, cost for skills development and training of the new Administrators and Assistants of the Certification Unit must be considered. For this activities the estimate cost is approximately 0,4 FTE of an Expert for a total of **30 thousand euros**.
- C) The estimate cost for the website creation is calculated considering two information: an interview with representative from National Certification Authority and desk research. During an interview with representative from National Certification Authority, the estimated cost for the creation of the website which includes a registry of all certification undertaken in that country is around 10 thousands euro. Assuming that the European Commission will store in its registry information concerning product certification of all EU countries and not merely information from a single country. A more reasonable estimate cost could be **25 thousands euros** which is based on the costs for this database characteristics<sup>5</sup>:

- **Number of pages:** 10 - 50
- **Style of design:** Moderately stylized
- **Copywriting # of pages:** 5-10
- **SEO w/ Placement Guarantee:** 30 keywords
- **Responsive Design:** Yes
- **Database Integration:** Full development
- **e-Commerce Functionality:** None
- **CMS:** Standard

<sup>4</sup> [https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts/technical-description-cei-list-of-nis-experts/at\\_download/file](https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts/technical-description-cei-list-of-nis-experts/at_download/file)

<sup>5</sup> <https://www.webpagefx.com/How-much-should-web-site-cost.html>

### 1.2.5. Costs estimated for the running of an EU wide ICT framework management board

In order to consider different options for the maintenance costs of Institutions similar to ENISA in the context of an EU wide ICT Framework, costs related to the creation of a Management Board have been analysed.

In the context of the creation of an EU general ICT Certification scheme, representatives from National Certification Authorities expect not negligible costs to run a European certification boards. At least, the following costs should be considered: costs to produce/maintain the relevant competencies in the Framework (e.g., security specification, evaluation, certification), costs to call/launch ad hoc projects on relevant security requirements and corresponding security certification requirements, and costs for logistics. Costs could be in fact reduced to those needed to coordinate and/or extend pre-existing structures and/or tools and/or standards.

Interviewees from ICT Certification Authority said that a very quick estimation of manpower needed to run a European Certification board is not that obvious, however if we consider the existing SOG-IS MRA and EU Authorities (ENISA, JRC), ICT Certification Authority representatives suggest that a permanent secretariat of 5 people could support the MSs to:

- Organize the appropriate exchanges of strategies to address the certification needs in the EU and establish roadmaps
- Approve the certification methods considered applicable for EU certification and recognized by all MSs
- Offer a front office for new certification needs expressed by vertical sectors
- Publish certificates and promote certification activities

A proposal of the new Structure and Organisation of the new Certification Unit is shown below:

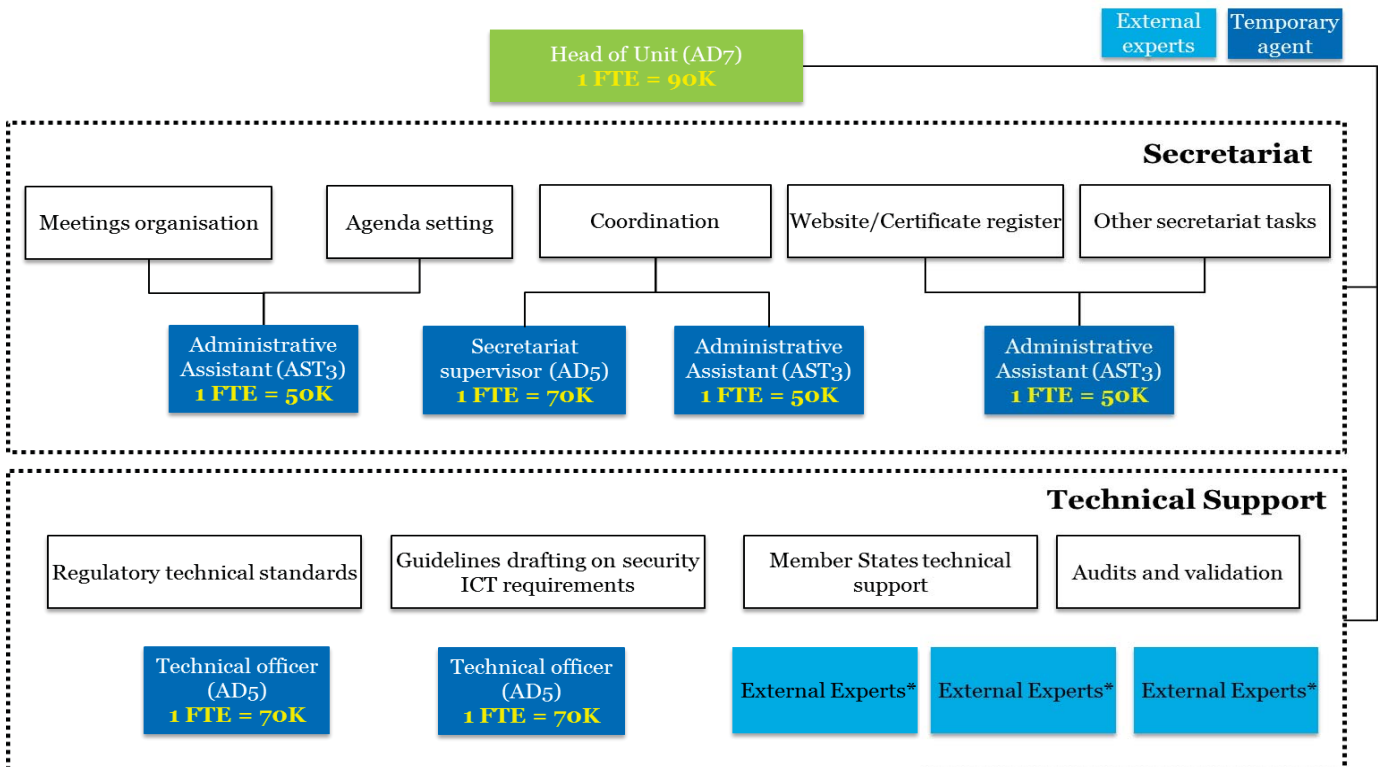


Figure - Proposal for the new Certification Unit



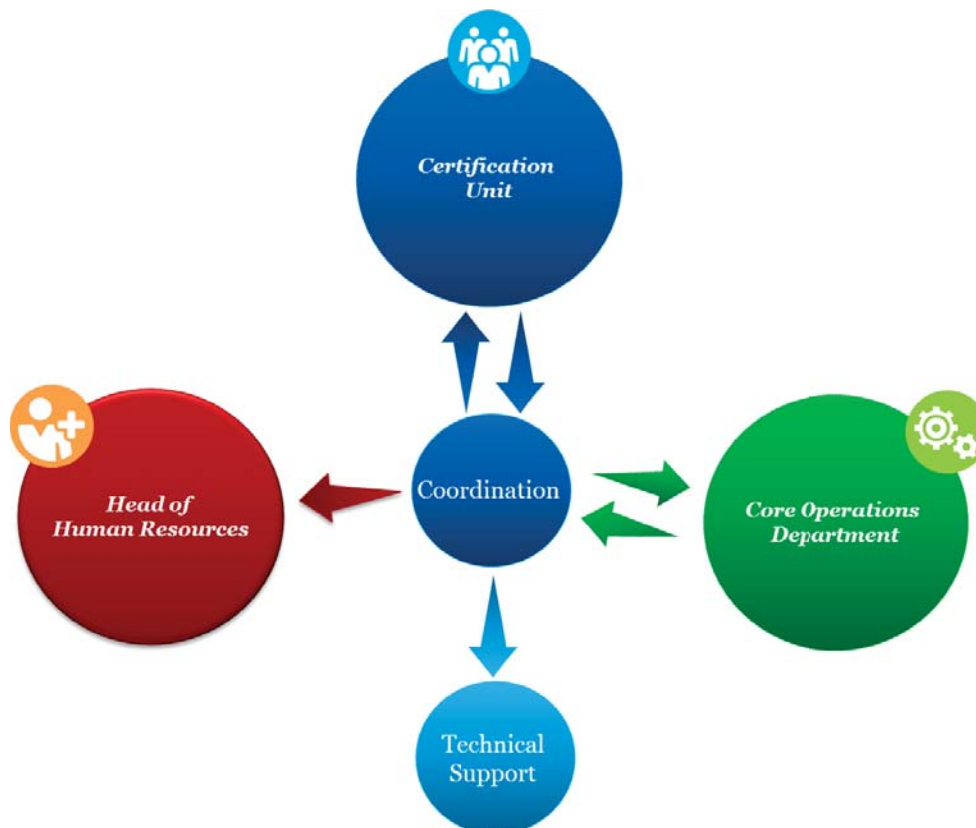
The new Certification Unit could be composed by:

- **1 Head of Unit (or Team Leader):** For the estimate cost, the Consortium considered a salary for a Temporary Agent (AD7). The Head of Certification Unit will be responsible for maintaining relationships with ENISA Management Board as well as EU Member States and supervising the Secretariat Team and the Technical Support. **The total cost estimated is 90k/€ per 1 FTE.**

Under the Head of Certification Unit, the Secretariat will be composed by one Administrator Temporary Agent (AD5) and three Assistants (AST3) that will be responsible for the following activities:

- **Coordination:** coordinate department functions, identifying needs, information sharing
- **Meetings organization:** organize transfers and technical and/or support meetings to MS and industry
- **Agenda setting:** draft agenda and the decisions/opinions of the Board, maintaining relations with MS
- **Website/Register of Certificates:** maintain/update the website and the register of the certified products and the list of products under evaluation
- **Other secretariat tasks:** provide support to and/or participate in various (technical) meetings, working groups etc.

Assuming for the Administrator a salary of 70 thousand euros per year and for the Assistants a salary of 50 thousands euros per year , the total cost estimated for running and maintain the Secretariat is **220k/€ for 1 Administrator (AD5) and 3 FTE Assistant (AST3).**



**Figure - Roles Interrelationships**

The Secretariat of the Certification Unit will need of Technical Support responsible for the following activities:

- **Regulatory technical Standards:** Responsible for evaluating standards and the certification scheme's security requirements, preparing and collecting reports
- **Guidelines drafting on security ICT requirements: involve industry and certification authorities stakeholders to draft guidelines on given ICT requirements**
- **Member States technical support:** Responsible for providing technical expertise to MSs (e.g.: MSs taking part in the framework on issues related to ICT Products)
- **Audit and Validation:** Conduct audit on Conformity Assessment Bodies and Certification Authorities and validate the products/services certified

To run and maintain the Technical Support Unit, two Administrators and three External Experts must be recruited. Assuming for the Administrators a salary of 70 thousand euros per year and for the External Experts a salary of 75 thousands euros per year (Total Fee for each Expert: 130 working days \* 450€ + 11'000€ + 5'000€ Allowances ≈ 75'000€ as explained in detail in the previous pages), the total cost rough estimation for running and maintaining the Technical Support is **365 thousand euros per year** for 2 FTE Administrator (AD5) and 3 External Experts.

In addition to the personnel cost, the following costs must be considered:

- Costs for meetings and events (e.g.: catering; rooms rent, etc.)
- Costs for travelling of ENISA Certification Unit personnel

ENISA could organize 6 major events per year with representatives from all Member State as actually organized by SOG-IS. The estimate costs for each events should be include at least:

- Catering
- Event Room Rent

Assuming for the Catering approximately 100 euros for each participants (including breakfast, lunch and dinner) and for the room rent an estimated cost of 500€ per day, the total estimate cost for 6 events of two day and 60 participants is **42 thousand euros**.

Moreover, audit activities must be undertaken by ENISA Certification Unit personnel on MS having national certification authorities. We assume that after the creation of an EU wide certification framework around 15 country of the total 27 EU countries will be audited. Considering for each travel abroad an estimated cost of 2 thousand euros per participants and considering an average of 15 travel per year, the total cost is **45 thousand euros**.

In the end, for minor meeting organised at the ENISA Headquarter, a light brunch could be offered. We estimate that in general for the working of an organisation such as ENISA in order to involve industry and certification stakeholders around 5-6 working meetings per month. In total 72 minor meetings per year could cost up to **1'440 euros**.

To have an overview of the estimated costs explained above, here after all the costs details are shown in table:

Description	Unit #	Unit of measure	Occurance	Unit price	Sub-Total	Total	Cost Tipology
Event Room Rent	2	Day	6	€ 500,00	€ 1.000,00	€ 6.000,00	Event-based
Catering for Event	60	Person	6	€ 100,00	€ 6.000,00	€ 36.000,00	Event-based
Catering for Meeting (ENISA Headquarter-based)	1	Day	72	€ 20,00	€ 20,00	€ 1.440,00	Event-based
Travelling Costs for Meetings abroad	1,5	Person wage	27	€ 2.000,00	€ 3.000,00	€ 45.000,00	Event-based
Head of Unit (AD7/9)	1	Person wage	1	€ 90.000,00	€ 90.000,00	€ 90.000,00	Recurring
Maintenance Costs - Secretariat (AD5)	1	Person wage	1	€ 70.000,00	€ 70.000,00	€ 70.000,00	Recurring
Maintenance Costs - Secretariat (AST3)	3	Person wage	1	€ 50.000,00	€ 150.000,00	€ 150.000,00	Recurring
Secretariat - Meetings organisation	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Secretariat - Agenda setting	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Secretariat – Coordination	1,0	Person wage	1	€ 70.000,00	€ 70.000,00	€ 70.000,00	Recurring
Secretariat – Coordination	1,0	Person wage	1	€ 50.000,00	€ 50.000,00	€ 50.000,00	Recurring
Secretariat - Website/Certificate register	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Secretariat - Other secretariat tasks	0,5	Person wage	1	€ 50.000,00	€ 25.000,00	€ 25.000,00	Recurring
Technical Support - Technical Support (AD5)	2	Person wage	1	€ 70.000,00	€ 140.000,00	€ 140.000,00	Recurring
Technical Support - External Experts	3	Person wage	1	€ 75.000,00	€ 225.000,00	€ 225.000,00	Recurring

GRAND TOTAL € 788.440,00

**Figure - Total estimate costs for the running of an EU wide ICT framework management board**

### *1.2.6. Costs estimated for the running of an EU wide ICT framework managed by an Expert Group*

In the context of the creation of an EU wide ICT Certification scheme, costs estimated for the running of an EU wide ICT Framework managed by an Expert Group have been also considered.

The costs for the **EU institutions**, **ENISA** and **Member States** coincide with the establishment and maintenance of this European Framework. In particular, the European Commission would have to place resources to support the establishment of the framework, notably for the adoption of the European schemes by means of delegated acts or implementing acts. It is estimated that this would require three FTEs working full time basis (e.g. two administrators and one assistant).

The EU institutions would also bear the costs related to the set up of the Expert Group. Typically, the Commission allocates 600 Euro per expert who will qualify for travel reimbursement. Since each Member State will appoint a representative, the total cost of the group is estimated to be in the region of 16,000 - 17,000 Euro per year.

ENISA is expected to bear the bulk of the costs related to both the functioning and maintenance of the framework, as it will be in charge of a) preparing the candidate schemes and b) issuing guidelines and c) providing the secretariat for the Group. The institutional costs related to ENISA are included in the economic estimates for ENISA (see Annex 6).

As an alternative to ENISA, it has been estimated that establishing a new body with the appropriate expertise in such a complex area would take between 5-7 years. Approximately, the costs of setting up a new European body amount to EUR 21,9 million. ENISA as the EU agency for cybersecurity with strong links with Member States has been considered to be best placed to ensure a coordinated and efficient approach to any European effort on security certification, for example by bringing all relevant stakeholders together, coordinating their work on certification schemes, preparing certification schemes and provide technical expertise.

Member States appointing a competent certification authority are expected to bear costs that would approximately amount to 1,600,000 Euro per year. This estimate include costs related to personel (e.g. min. three), equipment, subcontracting, operations (incl. training conferences) as well as set up of evaluation facilities. The operational management of a certification authority would also require investments for carrying out enforcement and supervision activities. Costs related to these activities are in the region of 290,000-300,000 Euro (per year). Generally, the overall impact will be significantly lower (or neutral) on Member States that are already part of the SOG-IS MRA and that have a supervision authority already in place.

This Option would not impose additional costs for the industry in the short term, namely because certification will remain essentially a voluntary tool. As is the case today, businesses will remain free to choose whether to certify their products or services. By contrast, the possibility to obtain an EU wide certificate would certainly act as a cost reductor for those firms that already certify their products or as an incentive for those that are willing to do so.

Since the process involved in future European schemes would depend on the associated level of assurance, cost and duration of certification would be more proportionate compared to the current SOG-IS MRA, built on the lengthy and bureaucratic CC methodology.

## 5.7 Summary of the Interviews with Experts on Cyber Resilience of Critical Infrastructures

The following paragraph summarize the information gathered through interview activities to selected participants from these Critical Infrastructures Sectors:

- Finance
- Transportation
- Energy
- Telecommunication
- Healthcare

Questions were asked in order to cover the following areas of interest:

- Evidence of fragmentation
- Labelling and information asymmetry
- Advantages of adopting cybersecurity certification
- Cyber resilience of Critical Infrastructures
- Impacts of an EU wide ICT Security Certification and Labelling Scheme
- Costs related to Certifications

Almost the totality of interviewees from different critical infrastructures sectors agree that there are many advantages adopting security certified ICT components/products for Critical Infrastructures. For example, a security certified product allows the entrance to several markets that have particular requirements and gives advantages for the transparency of the information for the customer or the regulator. However, an interviewee from Finance Sector stressed that being compliant does not mean being safer. In fact, the Finance Sector is one of the most regulated sector in the world and operators need to be compliant with lots of National and International Requirements.

The fragmentation across Europe related to National and International ICT Security Certification Schemes is highlighted by many interviewees. One of the Scheme mentioned by interviewees is Common Criteria but it is stated that this Certification Scheme does not work and it is little used to certify critical infrastructure products or components. Moreover, the certification processes are too difficult to go through because there is too much bureaucracy and paper forms to fill and the related costs are too high. An interviewee from Communication Sector said that in 2016 they requested 20 Common Criteria certifications with a cost of several hundred thousand euros each, including the external resources, laboratories etc.

Two clear examples of fragmentation are related to the French National Certification Scheme developed by ANSSI and the German National Certification Scheme developed by BSI. These two National Certification Schemes do not recognise each other. Another example mentioned is the National Certification Scheme recognised only in UK. An interviewee from Communications Sector said that his company needs to be certified on a variety of schemes in order to provide their service. In UK, there is the CAS(T) scheme, which is a telecom specific version of ISO27001 and that is a fundamental security certification for any product and service that is sold. Furthermore, the Public Services Network need to be certified every year as a prerequisite. It will not be possible to sell services in UK, without certifying them. For the same company, costs related to these certification are very high. For example, for one of their network platform the overall budget was of 500 thousand UK pounds. It includes 39 different services, whose price range from 10 to 15 thousands UK pounds each. CAS(T) Certification, an equivalent of the ISO 27001, it is issued by the National Cyber Security Council and it is valid only for the UK. Therefore, it is more UK centered and not European. Furthermore, there are actually a lot of standards for products' security certification. There are at least four schemes that are run by the UK National Technical Authority. They range from test marking, encryption etc. and there is no doubt that the cost of certification would be a barrier for vendors who want to enter the UK market.

A representative of an association of critical infrastructure stated that in Italy there isn't any mandatory certification but it is necessary to be compliant with Standards and National requirements. For example, as stated by interviewee from the Communication Sector, there are lots of products and components such as firewall, IPM, intrusion detection systems, routers with different criteria and standards that are required. In some cases, multiple certifications are necessary because other markets require them. For example, in

France, it is requested an authorization issued by the Prime Minister Office for network devices used in Critical Infrastructure. It is common for government to require certain standards for Critical Infrastructure and security products and services.

In the Finance industry services must have secure encryption and the use of Hardware Security Module (HSM), which are incredibly expensive. In order to use a HSM component, the cost is around 20 thousand euros and it is a cost for a single component, not for the whole device.

The fragmentation of ICT Security Certification Schemes combined with the increase of National Approaches across Europe are defined by interviewees a real market problem. Without a European wide Certification Framework, it would be very difficult to sell products in more than one European Country especially for small and medium companies. It is important however that the requirements of the certification are appropriate.

Critical infrastructures are by definition more critical than IoT, in general. However, the fragmentation is a common theme for both of them and it is unhelpful. Interviewees stated that the best solution to solve such fragmentation would be a moderate option that keeps in consideration both the European Market and each jurisdiction. According to representatives from Telecommunication Sector, it would also be positive if European Commission, instructed by ENISA, could define a set of best practices.

Regarding the lack of information related to security requirements of ICT products and components, according to all interviewees, an EU wide Certification and Labelling Scheme could be a valid instrument to raise the awareness and trust of customers. Interviewees stress that customers should be divided in companies and end-users. Companies are generally more aware on security requirements of ICT products purchased than the end users are. This is due also to the different nature, cost and complexity of the product that are purchased. There are medical devices that are expensive and complicated machines, which can be bought only by operators (for example, Tomography machines cost approximately one million euros). Before an operator buys such an expensive machinery, surely it will ask for more information about security requirements than a normal user that wants to buy a medical smart device that measures the level of glucose.

For critical infrastructure operators it is crucial to have the correct information about security tests made on certified products or information related to security requirements. As argued by an interviewee of Communication sector without a certification applied it is difficult to know if the information provided to the customer/end-user are true and complete. Each company could claim that their product is secure but it is better to have third parties to test it independently. Without any information related to security requirements of ICT/IoT products, the choices are based merely on the producer name. The company brand from which consumer purchases the components is like a security guarantor. For instance, buying from Schneider Electric and Siemens is probably more reliable than purchasing from a Chinese producer. There is, however, an issue to point out: most of systems and products on the European Market have embedded components that come from China where the security standards are less available to check. An appropriate EU labelling Scheme for ICT/IoT products could reduce these problems. Interviewee from Communication Sector said that, during the last year, his company discussed on the idea of IT trust labels for devices. They believe that a Labelling Scheme could be a more effective solution, especially for critical infrastructure. Also for a representative of Transportation and Logistic sector, the current situation with the lack of transparency of security requirements could still be improved. Making the information more available and clearer would definitely help the operators and avoid certain situations. If the label would be reassuring for the customer, it would also increase the trust in the company.

The totality of the interviewees agreed that a European cybersecurity certification Framework that support the mutual recognition of cybersecurity certification would have a positive impacts. However, it is important to establish in a proper manner what are standards, minimum security requirements to adopt and the evaluation processes of the laboratories. For an expert on cyber resilience of critical infrastructures, having multiple certification laboratories is very expensive. It is required to prepare the maintenance staff of these structures and, with an EU wide Certification Scheme, it would be possible to reduce these laboratories. It will be therefore possible to reduce costs related to laboratories on the long term.

Representative from a Transportation and Logistic association claims that an EU wide Certification Scheme would not only increase the security levels of all Member States but it would also be good for the European market. Even in this case, however, it is stated that the EU wide Certification Scheme has to be made in a proper manner: the certification needs to be designed based on the needs of the industries and the Member States. Moreover, the mutual recognition across EU might even have positive effects globally. An EU wide Certification Scheme could attract other non-European countries to join the mutual recognition. States like US and Canada and many others might be interested in the future to join such mutual recognition. All interviewees stated that it is also important that an EU wide Certification scheme would not be a mandatory scheme.

Another example, related to cybersecurity and the actual European ICT landscape, comes from Cloud Computing Services. Interviewees from Finance, Energy and Telecommunication Sectors stated that there is a barrier from using Cloud Services considering that, without clear and mutually recognized security requirements, companies have not perception of data stored in a secure way, especially according to the various jurisdictions. Most of the banks are struggling with this challenge. There are many problems because the European data might be stored in South America, or in another Country, under a different jurisdiction and with different perception of security. If Cloud Services would be certified under an EU wide Certification Scheme, it would be easier to be compliant and more confident about the respect of common security requirements.

## ***6. Work Plan***

This chapter of the Interim Report is based on the submitted Inception Report, and briefly summarizes how activities were undertaken in the first reporting periods and the extent to which they coincided with Tasks as planned. Furthermore, also key issues and how they were tackled are included.

The timetable represented here below (Overall Gantt chart) illustrates the general scheduled work plan for carrying out the whole project, as agreed within the Inception Report, with the red line indicating where we currently stand:



## Overall Gantt Chart

Sub-Task	Description	May					June					July					August					September			October	
		W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21				
<b>Task 0 – Project Management</b>																										
0.1	Organisation and management of project meetings	IM					FIM																			
0.2	Submission of deliverables and quality control	IRd	IRf		FIRd	FIRf		SIRd	SIRf	FRd	FRf															
0.3	Regular reporting to the EC																									
<b>Task 1 – Gather the evidence base</b>																										
1.0	Project set up		IRf																							
1.1	Desk Research & Field Work																									
	Literature / Input analysis provided by the Commission																									
	Desk Research																									
	Stakeholders re-mapping																									
	Interviews / Online Questionnaire																									
1.2	Mapping and assessment of existing certification and labelling schemes																									
1.3	Problem definition and assessment																									
1.4	Analysis of the baseline scenario and its evolution				FIRd	FIRf																				
<b>Task 2 – Assess the impact</b>																										
2.1	Classification and analysis of the impacts of each policy option																									
2.2	Comparison of options and elaborating the preferred one						SIRd	SIRf	FRd	FRf																
2.3	Desk Research; interviews to new stakeholders; definition of three case studies																									
<b>Task 3 – Other specific tasks</b>																										
3.1	Economic annex explaining the analytical model																									
3.2	Support in answering to specific requests coming from the Board																									
3.3	Elaboration of the intervention logic																									
3.4	Follow-up of the submission of the IA to the RSB																									

## 1.1. Update on Project Tasks

We have been following clear and logical procedures at all stages of the engagement until now. Below we outline, in reference to each of the foreseen Tasks, main activities carried out, including those methodological elements that characterized these Tasks. Furthermore, at the beginning of each paragraph describing the Task, we have detailed each one of them in a number of more operative Sub-Tasks, indicating for each of them their implementation status.

### 1.1.1. Task 1: Evidence Gathering and Analysis

Macro-Task 1 will be broken down into five sub-tasks (1.0, 1.1, 1.2, 1.3 and 1.4) each one containing the various activities indicated with letters in the ToR. Task 1 will involve the following sub-tasks:

Task 1: Evidence Gathering and Analysis	Implementation status
<b>Sub-Task 1.0: Project set up</b>	Completed
<b>Sub-Task 1.1: Desk research and Field work</b>	Completed
<b>Sub-Task 1.2: Mapping and assessment of existing certification and labelling schemes</b>	Completed
<b>Sub-Task 1.3: Problem definition and assessment</b>	Completed
<b>Sub-Task 1.4: Analysis of the baseline scenario and its evolution</b>	Completed

Here below the implementation timetable referring specifically to project Task 1, dedicated to Evidence Gathering and Analysis.

The output consisted of additions and integrations to what has been described in literature provided by the commission (e.g. JRC report, ENISA questionnaire), a desk research activity, an ongoing activity which consists in interviews of the main stakeholders mapped (mainly Certification Authorities, smart meters and semiconductors representatives). Furthermore it has been conducted a depth analysis of the problem definition and the baseline scenario and its evolution, using the output coming from the above mentioned evidences gathered.

### Task 1 Timetable – 5 Weeks

Sub-Task	Description	May			June				July
		W1	W2	W3	W4	W5	W6	W7	W8
	<b>Task 1 – Gather the evidence base</b>								
1.0	Project set up		IRf						
1.1	Desk Research & Field Work								
	Literature / input analysis provided by the Commission								
	Desk research								
	Stakeholders re-mapping								
	Interviews/Online Questionnaire								
1.2	Mapping and assessment of existing certification and labelling schemes								
1.3	Problem definition and assessment								

1.4	Analysis of the baseline scenario and its evolution				<b>FIRd</b>	<b>FIRf</b>			
-----	---	--	--	--	-------------	-------------	--	--	--

### *Sub-Task 1.0 Project set up*

As part of the Project set up, PwC & FUB delivered on the 17<sup>th</sup> of May 2017, the Draft Version of the Inception Report to the DG CNECT Team one day before the inception meeting. The goal of the Inception Meeting at week 1 was to scope the methodology, resources and objectives, which have been initially proposed in the technical offer and thanks to a preliminary data collection. This was necessary to set out, share and validate the approach to be followed throughout the whole duration of the study, laying out the grounds, in particular to the mapping and assessment of existing security certification and labelling schemes, the problem definition and assessment as well as providing the discussion over the policy options.

Following the Inception Meeting, the Inception report has been finalised taking into account all observations and comments raised at the meeting and delivered on the 19<sup>th</sup> of May 2017.

### *Sub-Task 1.1: Desk research and field work*

The goal of the data gathering activities was to find quantitative data or estimates, experts' views, and any kind of useful information on:

- State of play of certification and labelling frameworks by Member States, including level of diffusions, their key features (i.e. self-regulation vs. mandatory frameworks), level of success and their added value
- Evidence of obstacles to cross-border trade and market fragmentation stemming caused by fragmentation in national certification framework
- Costs (i.e. cost and duration of certification procedure) and benefits (for final users and as positive externality for the Digital Market Strategy) of certification frameworks (see later our typology)

DG CONNECT has provided a list of sources to be examined that include also the results of workshops organized by DG CONNECT with stakeholders in the previous months. In addition to the sources provided and listed above, one market study elaborated by PwC integrated.

During the first preliminary meeting, on the 8<sup>th</sup> of May 2017, and the kick off meeting, on the 17<sup>th</sup> of May 2017, the DG CNECT Team has highlighted the need to have within the Draft Interim Report the analysis of all the evidences supporting the impact assessment. It was therefore asked to focus on the documentation provided by DG CNECT and for this reason the activities to be carried out has been reorganized as follows:

1.1.0. Literature / Input analysis provided by the Commission;

1.1.1. Desk Research;

1.1.2. Re-mapping of key stakeholders not yet engaged in past activities and organization of related interviews;

1.1.3. Interviews/Online Questionnaire.

Since the beginning of the project, we have been working to identify and validate a list of the stakeholders who are directly or indirectly impacted by the project. The list has been updated and enriched several times during the first weeks. An updated release of the stakeholders map is included already now in Annex.

This fundamental database represented a key element to identify Certification Authority agencies and the representatives of the main industrial sectors participating to the interviews and questionnaire, to identify evidences supporting the analysis. When identifying key stakeholders, we have been taking into account the following:

- Geographical coverage (EU 28 MS),
- Coverage of the various types of stakeholders (Certification Authority Agencies, Industries, etc.)
- ICT vendors,

- 
- Policy makers.

To get more resources in support of *Literature / input analysis provided by the Commission*, the Consortium requested to have access to a study on cloud computing certification, the study is not completed and the Consortium had a preview of the ongoing activities. Furthermore, within the Report have been included preliminary data coming from the study on the Cyber Security Industry Market Analysis (CIMA), conducted by PwC and LSEC. This study is not yet completed and the data included by the Consortium within the present report are the very first information shared and updated at the 6<sup>th</sup> on June 2017.

As regard the results of the 2017 Enisa Survey, the DG CNECT Team shared the results with the Consortium and these results are part of the analysis included within the previous chapters.

The chapter of this report, named Stakeholders' support, contains a synthesis of the interviews conducted so far and, it gives an overview of the point of view of the main stakeholders involved. In addition to the interviews, the Consortium has prepared a Questionnaire (see Annex 7.2) sent to all stakeholders mapped during the first two weeks of the project, which aimed at gathering more evidences. The due date to submit the said Questionnaire was the 19<sup>th</sup> of June, the Annex includes also the results gathered.

### *Sub-Task 1.2: Mapping and assessment of existing certification and labelling schemes*

Evidence on the current state of the art in the 28 EU countries and selected extra EU countries has been identified and provided, performing a systematic research of secondary sources on the following:

- Available materials (from e.g., EU project CRISP, ENISA, BSA) that formed the initial reference for relevant entities in cybersecurity (and, hopefully, for the derivation of the cybersecurity certification status) in EU (and outside).
- Missing data gathered on the basis of explorations by the above mentioned questionnaire and interviews submitted to selected stakeholders in specific and impacted industry sector (mainly smart meters, semiconductors, Certification Authorities, etc.)

As highlighted by the DG CNECT Team during the Inception Meeting, on the 8th of May 2017, the specific theme of labelling will be discussed in September.

### *Sub-Task 1.3: Problem definition and assessment*

Sub-Task 1.3 has been developed performing the following phases:

#### **Analysis of the state of play and why EU intervention is needed (or not);**

A preliminary qualitative assessment of the current fragmentation and its costs has been developed during these weeks, to perform the test prescribed in impact assessment to ascertain whether EU action is required. Practical examples and specific cases to prove the market fragmentation have been gathered and it is presented within this report. The activity is ongoing and it will be completed within the 19<sup>th</sup> of June 2017.

#### **Further Development**

Based on the documents/data/information that the Consortium have analysed, it has been developed and improved the evaluation of the core problem and its whole definition.

### *Sub-Task 1.4: Analysis of the baseline scenario and its evolution*

The approach used to develop scenarios started from the definition of gaps, needs and state of play. The trajectories that the State of Play Model pointed out, as well as the analysis of barriers and needs, interpreted in terms of how they can evolve in terms of trends. The scenarios, thereby, investigated the type(s) of future(s) to which these trends may lead following the various steps explained in the following.

The trend analysis followed five steps:

- 
1. **Identify the main trends.** The trends has been derived from the baseline and state of play, which also shaped by the general description framework.
  2. **Classification of the trends.** This step required that trends have been clustered using an uncertainty - impact matrix. The rationale is that trends having a high uncertainty and high impact may result in contradictory and alternative futures and thus feed into different scenarios. On the contrary, trends having a high impact and low uncertainty should result in one type of future that has been forecasted. Trends with expected low impact are irrelevant and has not be considered.
  3. **Organization of trends.** The trends classified as having a high uncertainty and high impact has been organized and clustered into a limited number of key uncertainties that defined a number of key dimensions (possibly two). These dimensions are the variables of the scenarios axis. In doing so trends related to each other will be merged into key uncertainties having a high impact.
  4. **Derive concerted scenarios.** By combining the key dimensions of uncertainties (each one taking an extreme value), a number of scenarios has been derived. Each scenario has been given a typical, easy-to-recognize, and understandable name.
  5. **Develop scenario stories and description.** The last step aimed at enabling communication of the scenarios. An easy to read and understandable sketch or story will be of each scenario, as well as the values taken by the main aspects (contextual macro-level environment, transactional environment, technology, etc.)

### 1.1.2. Task 2: Assess the impact

During Task 2 will be provided quantitative and qualitative empirical evidence of the likely economic, social and environmental impacts of each of the identified preliminary options. Task 2 has been broken down into two sub-tasks detailed as follows:

Task 2: Assess the impact	Implementation status
Sub-Task 2.1: Classification and analysis of the impacts of each policy option	Closed
Sub-Task 2.2: Comparison of options and elaborating the preferred one	Closed
Sub-Task 2.3: Desk Research; interviews to new stakeholders; definition of three case studies	Closed

The Sub-Task 2.2 is ongoing considering that, during the interviews, the Consortium has started to gather, from the main stakeholders, data and information on the options proposed by the European Commission.

Here below the implementation timetable, referring specifically to project Task 2, dedicated to assess the impacts:

#### Task 2 Timetable – 10 Weeks

Sub-Task	Description	June				July				August				September				October		
		W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21	
	<b>Task 2 – Assess the impact</b>																			
2.1	Classification and analysis of the impacts of each policy option																			
2.2	Comparison of options and elaborating the preferred one					SIRd	SIRf	FRd	FRf											
2.3	Desk Research; interviews to new stakeholders; definition of three case studies																			

#### Sub-Task 2.1: Classification and analysis of the impacts of each policy option

As agreed with the European Commission DG Connect Team, this activity is currently driven and performed by the Commission and the Consortium is supporting through the evidences gathering and an in depth analysis of the information gathered through the interviews conducted.

Within this inception report, it has been drafted a previous potential impact analysis for each policy option identified by EC.

#### Sub-Task 2.2: Comparison of options and elaborating the preferred one

The overall objective of the comparison of options is to provide an overview of the positive and negative impacts of each policy option with regards to the objectives. This comparison, using a multi-criteria analysis, will help us to compare the different policy options in terms of effectiveness, efficiency and coherence concerning the delivery of the policy objectives as well as prepare evidence and recommendations for decision-making.

The comparison of policy options is consisting in:

- Summarising positive and negative impacts for each policy option;
- Comparing policy options in terms of effectiveness, efficiency and coherence according to the results of task 1;
- Ranking the options by order of preference and recommend a preferred option.

### *Sub-Task 2.3: Desk Research; interviews to new stakeholders; definition of three case studies*

In order to gather more information to be used for the impact assessment, the Consortium has organized a second phase of direct interviews and a second online questionnaire specifically designed and structured for Critical Infrastructures (which include organizations coming from transportation, healthcare, energy, finance, telecommunication sectors). Considering that the questionnaire has been submitted at the end of July, a complete overview of the results would be consultable in the first week of September. As regards the interviews the main results have been included within the present report.

The report includes three case studies specifically defined through the interview conducted and an additional desk research. The case studies regard:

- Smart Meters industry
- Alarm Systems industry
- Cloud Computing services

#### *1.1.3. Task 3: Other specific tasks*

During this Task 3 we have to provide additional elements/services in order to support the Commission through the following actions:

1. Provide the economic annex referred to in the Better Regulation Toolbox (Tool #8), explaining the analytical models used in preparing the impact assessment;
2. Assist the Commission in establishing an adequate implementation plan for the preferred policy option;
3. Assist the Commission in the elaboration of the intervention logic linking the identified problems with the problem drivers and the policy options and in the drafting of the main charts and tables to be included in the impact assessment;
4. Support in the follow-up of the submission of the impact assessment study to the Regulatory Scrutiny Board (RSB) of the Commission (in particular in helping to respond to questions from the RSB).

The following sub-tasks:

<b>Task 3: Other specific tasks</b>	<b>Implementation status</b>
<b>Sub-Task 3.1: Economic annex explaining the analytical model</b>	<b>Ongoing</b>
<b>Sub-Task 3.2: Support in answering to specific requests coming from the Board</b>	<b>Closed</b>
<b>Sub-Task 3.3: Elaboration of the intervention logic</b>	<b>Closed</b>
<b>Sub-Task 3.4: Follow-up of the submission of the IA to the RSB</b>	<b>Ongoing</b>

Here below the implementation timetable, referring specifically to project Task 3, dedicated to additional elements/services aimed at supporting and assisting the European Commission:

### Task 3 Timetable – 15 Weeks

Sub-Task	Description	May		June			July				August				September				October			November			December				
		W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21	W22	W23	W24	W25	W26	W27	W28	W29	W30
	<b>Task 3 – Other specific tasks</b>																												
3.1	Economic annex explaining the analytical model																												
3.2	Support in answering to specific request coming from the Board																												
3.3	Elaboration of the intervention logic																												
3.4	Follow-up of the submission of the IA to the RSB																												

### Sub-Task 3.1: Economic annex explaining the analytical model

With specific reference to the economic impacts, in the present subtask we are developing an economic annex to the impact assessment report with detailed explanations on the analytical models used in preparing the impact assessment.

More precisely, for each of the analytical model used we are defining an explanation box with technical explanations (in accordance with the ToR - Section 5.1 “Deliverables”) containing, at least, the following main information about the model:

- a brief description of the model;
- the model developer and nature (public/private/open source) of the model;
- model structure and modelling approach with any key assumptions, limitations and simplifications;
- intended field of application and appropriateness for the specific impact assessment study;
- model validation and peer review with relevant references;
- the extent to which the content of the model and input data have been discussed with external experts;
- explanation of the likely uncertainty in the model results and the likely robustness of model results to changes in underlying assumptions or data inputs;
- explanation as to how uncertainty has been addressed or minimised in the modelling exercise with respect to the policy conclusions;
- the steps taken to assure the quality of the modelling results presented in the IA;
- a concise description of the baseline(s) used in the modelling exercise in terms of the key assumptions, key sources of macroeconomic and socio-economic data, the policies and measures the baseline contains and any assumptions about these policies and measures.



---

### *Sub-Task 3.2: Support in answering to specific request coming from the Board*

In order to assist DG CNECT in answering to the Board comments and requests, we have supported the team in respond to the main comments received. To achieve this purpose the Consortium contacted again some of the main stakeholders and add information through desk research activity.

### *Sub-Task 3.3: Elaboration of the intervention logic*

Underlying causes (or "drivers") of the problems identified in the task 1 "Evidence Gathering and Analysis", the present subtask supported in the elaboration of the "intervention logic" as the link between problem-drivers and policy options.

The intervention logic model that we have developed to justify the public policy action is a method used to explain of what the intervention - the policy proposals - is meant to achieve (the objectives) and how it is supposed to achieve it (the tools). The intervention logic regroups all the activities, expected effects and assumptions of an intervention. It also presents in a clear way how the policy will lead to the intended effects in the present and future context.

Developing the intervention logic, we have taken into account that it may evolve over time according to the political, economic or social context. This implies that the intervention logic model may need to be reconstructed several times, for successive periods to fit in with developing events.

During this sub-task, the intervention logic has been detailed for the policy option that results as the preferred option considering the ranking.

### *Sub-Task 3.4: Follow-up of the submission of the IA to the RSB*

After the draft Impact Assessment has been produced, the Regulatory Scrutiny Board (RSB) will scrutiny it in order to assess the quality and provide recommendations on how this draft report should be improved by the Commission services. As part of the Commission's renewed commitment to better regulation, a new Scrutiny Board has been established, replacing the Impact Assessment Board, with the aim of strengthening the existing system of quality control.

The new Regulatory Scrutiny Board will scrutinize the quality of all impact assessments, major evaluations and fitness checks of existing legislation and issue opinions on the draft of the related reports in line with the relevant guidelines. According to the Commission's Working Methods 2014-2019 any impact assessment should be accompanied by a positive Board opinion before an initiative can proceed.

Our support in this task will consist in helping to respond to RSB questions concerning the impact assessment study already submitted and in supporting the commission services in the follow of the RSB recommendations considering that the activities have to be finalized within the end of September.

#### *1.1.4. Task 0: Project Management*

This Task is focused on the provision of ongoing project management services throughout the duration of the project. In detail, project management activities are involving the following three Sub-Tasks, together with the production of most of the foreseen project Deliverables:

- **Sub-Task 0.1:** Organisation and management of project meetings
- **Sub-Task 0.2:** Submission of deliverables and quality control
- **Sub-Task 0.3:** Regular reporting to the EC

Here below the implementation timetable, referring specifically to project Task 0, dedicated to project management and coordination activities:

### Task 0 New timetable 1 – First 15 Weeks

Sub-Task	Description	May			June				July				August			
		W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
	<b>Task 0 – Other specific tasks</b>															
0.1	Organisation and management of project meetings	IM						FIM								
0.2	Submission of deliverables and quality control	IRd	IRf				FIRd	FIRf	SIRd	SIRf	FRd	FRF				
0.3	Regular reporting to the EC															

### Task 0 New timetable 2 – Second 15 Weeks

Sub-Task	Description	September				October	
		W16	W17	W18	W19	W20	W21
	<b>Task 0 – Other specific tasks</b>						
0.1	Organisation and management of project meetings						
0.2	Submission of deliverables and quality control						
0.3	Regular reporting to the EC						

#### Sub-Task 0.1: Organisation and management of project meetings

The kick-off meeting took place in Brussels on the 17<sup>th</sup> of May 2017. Furthermore, in order to ensure frequent communication with EC Team throughout the entire project, conference calls have been scheduled during the first weeks with EC Project Manager in order to discuss project activities, progress on deliverables and any other key issues.

The main project Reports already presented, include the Inception report (D1), delivered at the beginning of engagement activities (on the 19<sup>th</sup> of May).

#### Sub-Task 0.2: Submission of deliverables and quality control

All deliverables are going through a rigorous quality review process covering both scientific excellence and standard of English. Feedback received during Project Meetings has been and will be considered and the reports duly amended.

#### Sub-Task 0.3: Regular reporting to the EC

The Team Manager will lead regular reporting on behalf of the entire team to the Commission, primarily through day-to-day email exchange as well as regular project status report via conference calls.

#### Meetings and Reports

A number of meetings are foreseen to ensure discussions on the most important project issues. Meetings will be relevant to each deliverable.

---

The main project Reports already presented, include the Inception report (D1), delivered at the beginning of engagement activities and the First Interim Report (D2), the Second Interim Report (D3) and the present and Final Report. The final study report summarizes how activities were undertaken and the extent to which they coincided with tasks as planned. Key issues and how they were met will be included. The Final study report will show key conclusions and all information gathered so far.

---

## 7. Annex

### 7.1 Minutes of the interviews

June 7, 2017

#### *Interviews results from representative of a National ICT Certification Authority*

**1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?**

In all EU MSs, a security certification is requested in the digital signature context, namely for secure signature/seal devices as defined in EIDAS regulation<sup>6</sup>. As specified in EIDAS secondary legislation<sup>7</sup>, this is a security certification according to "Common Criteria EAL 4+" with given Protection Profiles. The corresponding duration and cost are in the order of 18 months and 100K euros. Notice that, in Italy, a procedure has been established to cover cases where the Protection Profiles mentioned before cannot be used. The Italian procedure is still based on Common Criteria EAL4+ as well.

**2. Do you know cases in the EU, where national approaches for the security certification of any ICT products/services have been/are being established?**

Yes. In Italy, based on the national decree DPCM 17 February 2017<sup>8</sup>, it should be established a National evaluation and certification centre for verifying security and non-vulnerability conditions for products, devices and systems for networks, services and critical infrastructures.

**3. Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?**

Yes. The provided information is usually not reliable enough. Notice that, to improve the situation, a security certification is a necessary but not a sufficient condition. A significant solution would be to have a security certification against security requirements established by super partes bodies and possibly recommended by statutory authorities.

**4. Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

---

<sup>6</sup> Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014.

<sup>7</sup> Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal of the European Union L 109/40, 26 April 2016.

<sup>8</sup> Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, Gazzetta Ufficiale n. 87 del 13 aprile 2017 (Italian Prime Minister Decree, 17/02/2017, Directive on guidelines for national cyber protection and cybersecurity, Official Bulletin n.87, 13/04/2017)

---

Yes. Clearly, a recognition agreement would eliminate the need and cost of re-certification in the domain covered by the agreement.

**5. In the context of the possible creation of a European ICT security certification Framework, building on existing ICT certification mechanism, such as SOG-IS MRA, what do you think are the estimation of costs needed to run a European Certification Board?**

I expect not negligible costs. At least, the following costs should be considered: costs to produce/maintain the relevant competencies in the Framework (e.g., security specification, evaluation, certification), costs to call/launch ad hoc projects on relevant security requirements and corresponding security certification requirements, and costs for logistics.

*Interviews results from representative of a National ICT Certification Authority*

**1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?**

Yes. In Italy, a security certification is requested for secure signature/seal devices. In fact, due to EIDAS<sup>9</sup>, this applies to all EU countries. As specified in rules for EIDAS implementation<sup>10</sup>, the security certification has to be executed according to "Common Criteria EAL 4+" with given Protection Profiles. Duration and cost can be estimated in about 12 months and in the range of 50K-100K euros.

There is also a second example. In Italy, a public local authority (Provincia di Trento), in a public procurement procedure<sup>11</sup> has recommended the security certification of a video surveillance system according to Common Criteria (low assurance, i.e., EAL 1). Duration and costs of this security certification can be estimated in about 6 months and 20K euros.

**2. Do you know cases in the EU, where national approaches for the security certification of any ICT products/services have been/are being established?**

Yes. In UK, an approach known as CPA (Commercial Product Assurance) has been established for COTS products to be used in low risk environments. This approach has been derived by the Common Criteria (for low assurance certification).

Moreover, in France, an approach known as CSPN (Certification de Sécurité de Premier Niveau) has been established.

This is a black box testing approach for low assurance certification requirements and the evaluation/certification process has limited duration and costs.

**3. Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?**

Yes. In fact, for many products of large diffusion (e.g., the smart phones), no information is provided about the relevant ICT security properties, and the user is left alone with many questions and no answer. A security certificate would improve the situation making some significant information available, and reliable as well.

**4. Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

---

<sup>9</sup> Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014.

<sup>10</sup> Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal of the European Union L 109/40, 26 April 2016.

<sup>11</sup> Further details are not available

---

Yes. As in similar cases, the mutual recognition agreement would eliminate the cost of certification duplication, at least within the validity (range of products, set of countries, etc.) of the relevant agreement.

**5. In the context of the possible creation of a European ICT security certification Framework, building on existing ICT certification mechanism, such as SOG-IS MRA, what do you think are the estimation of costs needed to run a European Certification Board?**

I would estimate medium costs. At least in the case where already available structures (e.g., EU Agencies), tools (e.g., SOGIS-MRA), and standards (e.g., Common Criteria) were exploited to the maximum extent. Costs could be in fact reduced to those needed to coordinate and/or extend pre-existing structures and/or tools and/or standards.

*Interviews results from representative of a National ICT Certification Authority*

**1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?**

Yes. A security certification is requested in the EU digital signature context. According to EIDAS<sup>12</sup> and the corresponding technical rules<sup>13</sup>, a secure signature/seal device has to be certified according to Common Criteria EAL 4+ with given Protection Profiles. Duration and cost of this security certification depend on the type of secure signature device (either smart card or HSM- Hardware Security Module) and on the maturity of the security certification market. My estimates hold for countries where the relevant market is consolidated<sup>14</sup>. For the smart card type, the duration of the evaluation/certification process is of some months; whereas, for the HSM type, the duration is of some years.

Another example is available for Italy, where, in a public procurement procedure defined by Provincia di Trento (Italian local authority), a video surveillance system has been recommended to be provided along with a Common Criteria - Low Assurance security certification<sup>1</sup>.

**2- Do you know EU cases where an ICT product/service vendor due to requested or recommended additional security certifications (see previous question) in order to enter the market of another MS, has given up in entering that market?**

As concern questions 2, 3 and 4, relevant cases were possible before the establishment of EIDAS regulation

**3- Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?**

Yes. The typical case is that the relevant information is not provided at all. In fact, in EU, we are very far from the case where, as far as ICT security is concerned, a product is provided along with a set of reference information for the customers which allow to understand, e.g., how the product can be/cannot be used. The current concept of product information to be provided to a product user do not cover at all the ICT security domain.

**4- Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

Yes. At least in the countries and for the products (positively) affected by the agreement, multiple security certifications would no longer be needed.

<sup>12</sup> Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union L 257, 28 August 2014.

<sup>13</sup> Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal of the European Union L 109/40, 26 April 2016.

<sup>14</sup> Further details are not available



---

**5- In the context of the possible creation of a European ICT security certification Framework, building on existing ICT certification mechanism, such as SOG-IS MRA, what do you think are the estimation of costs needed to run a European Certification Board?**

I would expect low costs, since already available structures/components (e.g., EU Agencies) could be exploited for the Framework realisation. I'd suggest the Framework to consider the possible infeasibility to take a unique approach (e.g., unique evaluation/ certification criteria) to security certification. In fact, based also on the operating context, ICT products/services usually have large variability in terms of severity of security requirements severity and assurance level of the corresponding certification processes, and this is probably better addressed by several suitable solutions.

---

**June 8, 2017**

*Interviews results from representative of a National ICT Certification Authority*

**1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?**

The interviewed is aware of cases where an ICT product service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given Member State: the interviewed provided examples where a Common Criteria certification is EU-wide requested (e.g. the case of digital tachographs) and where the same certification is requested (e.g. the case of the electronic Identification Authentication and Signature, eIDAS, regulation).

The duration of such certification is around 6 months and the costs can be estimated between 50 and 100 thousands Euro.

**2- Do you know EU cases where an ICT product/service which is equipped with some certificate security certificate is requested or recommended (e.g., preferred within public procurement) to get additional security certificates in order to enter the market of any MS?**

The interviewed provided information of the smart meter case where the product is requested to get additional security certificates in order to enter at least the German market. In order to provide information to the fragmentation, the interviewed explained the health card example in Germany where a certification of the health cards is required by the National Approach; unfortunately the interviewed was not aware of the cost of the certification for the cases of smart meter and health card.

**3- Do you know cases in the EU, where different certification approach from two different countries are deemed equivalent to establish the security of a same product (through Mutual Recognition Agreements)?**

Regarding the approach of a mutual recognition arrangement, the position of the interviewed is that such approach will have positive impact on the costs of industry. On the other hand, regarding the possibility to establish a European certification framework, the interviewed commented that costs are still not predictable because it depends on the tasks and on the mandate of the European Certification Board in charge of managing the framework.

*Combined answers from two interviewees from a National ICT Certification Authority*

**1. Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?**

The interviewed provided several cases where there is a requirement on certification of an ICT product.

Regarding the Hardware Security Module (HSM), a product that falls in this category has to be certified against the common criteria standard in order to access to the French market. HSM common criteria certification can last 6 to 9 months and the cost can be estimated on around 200k euros.

Another example where common criteria certificate is required, in the EU, is the Secure Signature Creation Devices (SSCD): like the previous example, a certification process can last 6 to 9 month and the cost can be estimated in around 200k euros.

The interviewed provided then information on the case of detection sensors where a qualification against the French national approach CSPN is required by national law. In this case, the duration of the qualification is 2 months and the costs is around 35k euros.

Regarding network devices related to the creation and management of VPNs (Virtual Private Networks), requirements are defined in France and in the EU on certification based respectively on a national approval (which is Common Criteria based), and on a EU approval process: the French national approval process for VPNs will last from 6 to 9 month and the costs are estimated around 80k euros. The EU approval process is free of charge and takes 2 months to be completed.

**2. Can you provide a case where the certification of an ICT components component is accepted in one country but it was not accepted in another EU country as another certification was required? In that case, did the company undertake a second certification or did it restrain itself from entering the market of that second country?**

With reference to the previous examples, the interviewed noted that for HSM an initial certification of the crypto module is requested (FIPS), and the SOGIS members, via CEN, request for additional Common Criteria certificates with related vulnerability analysis.

For SSCD products, there are examples in SOGIS Member States where, if the original common criteria certification is not sufficient for national needs, the product has to undergo again the certification process.

VPNs related network products are a good example to demonstrate that in absence of an EU common certification approach, some national schemes may have the need to define their own framework requesting another certificate: even if the product is certified against a "collaborative" protection profile, cPP (meaning that the PP has been harmonized between International Mutual Recognition Arrangement members), and even if the product is certified against the FIPS requirements, the additional certification CSPN (and in some cases a completely new common criteria evaluation) is required to access to the French market.

Other example can be provided for other ICT products like Firewall.

**3. National certification approaches**

The interviewed confirmed that some vendors of HSM, SSCD or other EU regulated products, after completing the certification process in non EU countries (e.g. USA, but there are also examples of

products certified in UK and Sweden), quit the common criteria certification required in the EU because, in most of the cases, evidences required at security level for the evaluation process cannot be made available outside the country of origin.

The interviewed provided examples of national approaches for low-level assurance with the CSPN in France, and the parallel approaches in Germany and Netherlands. The interviewed commented that alternative certification programs have been established to complement existing ones, in order to allow more entries into certification (case of CSPN), or to fill the gap of non-existing certification solutions.

**4. Do you know cases in the EU, where different certification approach from two different countries are deemed equivalent to establish the security of a same product (through Mutual Recognition Agreements)?**

The interviewed thinks that a mutual recognition agreement of certification schemes existing in different countries have indeed a positive impact on industry costs. Based on the SOG-IS MRA, France can for example certify an e-passport application on a chip that was certified in another SOG-IS qualified member by just composing on the chip certificate. It applies as well for all smart card based products.

For eIDAS, any SOG-IS certificate on a HSM or SSCD will be considered as immediately valid for French procurement, as it probably is for all SOG-IS MRA members.

A very quick estimation of manpower needed to run an European Certification board is not that obvious, however if we consider the existing SOG-IS MRA and EU Authorities (ENISA, JRC), we could suggest that a permanent secretariat of 3 to 5 people could support the MSs to:

- Organize the appropriate exchanges of strategies to address the certification needs in the EU and establish roadmaps
- Approve the certification methods considered applicable for EU certification and recognized by all MSs
- Offer a front office for new certification needs expressed by vertical sectors
- Publish certificates and promote certification activities

**5. Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?**

Unless a product or service has been certified, interviewed answered that there is no proper evidence that a product or service is secure enough for its customer.

Only a certification allows to deliver a certification report that identifies the assessed security level and associated documentation (user guidance, especially) to customers (who have to carefully examine these evidence to make sure the product/service is adequate to their security needs).

**6. Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

Therefore, there is an urgent need to establish a proper EU framework that will analyse, select and improve, where necessary, the acceptable approaches for EU wide certification, and will rationalize the certification decisions for both MSs and industry.

Harmonizing will only be possible through technical exchanges between the MSs schemes, which obviously relies on open certification approaches.

*Interviews results from representative of a Semi-conductors industry*

**1- Do you know EU cases where an ICT product/service is requested or recommended to be equipped with a given security certificate in order to enter the market of a given MS?**

An illustration of present certificates needed for ICT products is the Italian passport, which has a chip certified for example in Netherlands, produced in Germany and approved by the national statement of Polygraph of Italy.

Another example given was related to the banking sector and especially for the bankcards. All bankcards in Europe must be certified in two ways: credit cards or debit cards.

Passports, bankcards and many documents must be certified under European Regulation but there are also National Regulation to be considered that could require additional certification. For instance, in Italy there is the CNS (Carta Nazionale dei Servizi) Card that is certified under the Italian Government. In Germany there is a similar program called Telematik-Infrastruktur. Another example of ICT products that must be certified are all cards reader for hospitals.

All laptops using Microsoft, Office, Windows software needs TPM (Trusted Platform Module) which is the name of the requirement for building a microchip which aims at guaranteeing the encryption of the email of personal computers and laptops. All pc, laptops must have certified microchips and the certification is uniquely recognized worldwide. The chip of a laptop could be produced in Germany and the motherboards produced in China but all components must be certified.

**2- Do you know EU cases where an ICT product/service which is equipped with some certificate security certificate is requested or recommended (e.g., preferred within public procurement) to get additional security certificates in order to enter the market of any MS?**

One problem of fragmentation for ICT Certification is that one product needs to be certified more times for each single component: the hardware of one product needs one dedicated certification, the software integrated of the same product needs another certification and, for example, the chip a third one. This is a real problem for the semi-conductor industry.

Fragmentation is related to the existence of multiple national and sectorial certification schemes not mutually recognized especially in reference to National programs and regulations. The Italian health care cards are completely different from French health care cards, because they have different data, different functions and different type of certifications.

**3- Do you know EU cases where an ICT product/service that has been requested or recommended to be equipped with additional security certifications (see previous question) in order to enter the market of another MS, has actually gone through the certification process?**

For example, Taxi cards have to be certified within individual National specific programs (one example is the Dutch program) but in Italy there is no such a program established. Within the Member State there are too many National programs which are not harmonized. The fragmentation exists in terms of specific products and specific regulation of member states.

Software, Hardware and chip are certified with different levels of certification according to EAL Common Criteria.

**4- Do you know EU cases, where a customer is not provided with enough/reliable information about the security properties of any ICT products/services?**

---

It is paramount to distinguish customers from users when trying to assess whether there is an information asymmetry with behavioural impacts. The final consumer is not well informed on the security properties of ICT products/services, this is due to a lack of awareness through labelling. From the point of view of industry and government customers, the information in labelling schemes is likely to have an impact on its behaviour and purchases.

An example can be found in cable TV that need to be connected to a router for internet connections, these products do not respond to specific security requirements and are vulnerable to hacker attacks. On the other hand, consumers are not aware of this kind of deficiencies, so they continue buying products without considering security requirements.

**5- Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

Benefits of Mutual recognition agreement within Member States comes from more than 20 years of experience.

**6- Do you think that the extension of the SOG-IS MRA to all Member States could be a viable policy options?**

The extension of SOG-IS agreement to all MS is not a valid policy option that must be considered because there are Member States which are too small and do not have a Certification Authority. Not all countries have the ability to join the SOG-IS agreement.

*Combined answers from two interviewees from Smart Metering Industry*

- 1. Do you know EU cases where an ICT product/service which is equipped with some certificate security certificate is requested or recommended (e.g., preferred within public procurement) to get additional security certificates in order to enter the market of any MS?**

The fragmentation meant as the existence of multiple national and sectorial certification schemes not mutually recognized exists especially talking about National specific programs. There are currently three certification that are ongoing: one in UK, one in France and one in Germany. Our company currently knows this three different certification scheme and do not knows if other initiatives are ongoing. There are at least three Member State that request different certifications and they do not accept each other certificates, so for each country it is request a different certification.

All the three Countries (France, UK, and Germany) have their own scheme: in the UK is called CPA (Commercial Product Assurance) that it is a scheme that is applied for smart-meters but also for other products. In France it is request the CSPN (Certification de Sécurité de Premier Niveau) certification scheme and in Germany there is a certification scheme based on Common Criteria. Another kind of fragmentation is then also happening on the evaluation side. There are only limited number of Conformity Assessment Body that are able to certify against the requirements of different schemes. In this way, a certain kind of market entry barrier is created.

- 2. Do you see the emergence of multiple national or sectorial certification schemes as a likely scenario in the future, especially in view of the growing cybersecurity risks?**

If MS continue to do not accept each other Certification schemes, each MS will continue to improve its own Certification scheme. Our company started many activities with DG CNECT in order to prevent a situation with 27 different national certification schemes in Europe.

- 3. Do you think the extension of the SOG-IS to all member states represents a valuable policy option? Can you please elaborate what do you think are the criticalities and positive aspects?**

In Germany, smart-meters needs to be certified against EAL-4. It is not very easy to evaluate again smart-meters for example in France or somewhere abroad. The competition is limited. Moreover, Smart-meter industry is beginner in security. A European certification scheme beyond the SOG-IS, would be great and it would increase the competition. Actually, the processes, the procedures and the bureaucracy for certification is too much for smart-meters industry and security industry.

- 4. What do you think in this context would be the difference between the SMEs and the Large Sized Enterprises? Do you think that the size of the Company may impact its ability to access in another market and then having additional certification?**

The cost of certification is about 1 million and the SMEs are out of this gain. In Germany, only one of the biggest smart-metering companies is starting a certification and all the other companies are present only in the German market.

- 5. Do you think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (e.g. more stringent testing/assessment standards for more sensitive products/applications and less stringent for less sensitive products/applications)?**

---

It would be great to have one methodology on how you affect the risk, how you define security requirements and how you go through certification and a recognition across Europe. It is very important to have flexibility in certification scheme, determine on the risk connected to the product evaluated and the risk connected to the location of the product.

**6. Do you have an estimate about cost and direction of these certifications?**

Looking at the German scheme, the cost of certification is very expensive. The cost of certification is about 1 million euro and the SMEs are out of this gain. For BSI "Smart Meter Gateway" certificate the cost is much more than one million. Our company also checked with meters manufacturers the price for smart meters certification and in UK is almost 150K euro. In Germany, only one of the biggest smart-metering companies is starting a certification and all the other companies are present only in the German market. In France, the cost of certification is something between Germany and UK. The cost it is similar to the UK, so it is about 150K euro or more. In terms of cost, it is also important to note that the evaluation processes are different between MS.

**7. Can you provide a case where a customer/user is not provided with enough/reliable information about the security properties of any ICT products/services? What is the problem for consumers: that information 1) is not is not provided at all 2) is not reliable 3) is not enough**

Concerning the Labelling topic, the representative of the Smart meter industry underlined that it is fundamental to distinguish the kind of customer. The suppliers buy millions of meters and they have good understanding of security specifications of the products. For Business-to-Business products, the labelling aspect is not much relevant. On the other side, the public opinion is more concentrate on privacy issues (e.g. personal data) and the transparency of data collected by smart-meters. In UK, smart-meters have a display connected to the meters and consumers can simply read data on this display. The consumer decision to buy a product is more on the utility of the product than security aspects. It is important to differentiate which devices needs to be certified and which devices needs to be labelled.

**Additional Remark**

Working with ENISA, it would be important to understand and harmonize the security language of the energy sector, in order to understand each other, both energy and smart-meters sectors. It is important to combine the approach of DG CNECT with the approach of DG ENERGY.



*Interviews results from representative of Smart meters industry*

**1- Can you provide a case where the certification of an ICT component is accepted in one country but it was not accepted in another EU country as another certification was required? In that case did the company undertake a second certification or did it restrain itself from entering the market of that second country?**

We need to distinguish between ICT and ICS (Industrial Control System) products, since the two categories have different requirements and currently this is not so clear to the certification environment. In France exists the CSPN certification (a kind of light common criteria), which is a low level assurance approach, initially used for ICT products but now moving in covering also ICS and critical infrastructure products.

Relating to product to be used in critical infrastructure, we are not aware of any other request for products certification in other EU countries.

In our product range, we have not seen any overlapping in product certification relating to activities in other countries. Not even in the field electrical infrastructure used by the military world.

We are not aware of cases where a vendor renounced to certificate its products in other countries due to different certification requirements for the same product.

We are aware that, in Germany, BSI is investigating on a low-level assurance framework which is in line with the French CSPN approach.

**(Additional question) Based on your experience, what is your view of costs and durations of certification processes?**

The French Certification Authority defined the framework CSPN which a light version of common criteria. CSPN certification costs about 50k euros and the duration is around 6 months. Behind these costs, there are a number of activities to be performed by the vendor to fulfil CSPN requirements and such activities are estimated to cost around 300k euros.

France has in place other types of certification framework (for COMSEC and for system integrators). It is very important to apply international standard to harmonize requirements between Members States and to give the vendor the opportunity to be competitive at international level. In the ICS world, we are aligned with the standard ISO 15443.

We are a European and international industry. We have to follow different certification approaches in different countries. Common Criteria are much more expensive for us: just as an example, the cost of a Common Criteria certification is not less than 500k euros. We do not feel that the Common Criteria approach is the good solution, at least for ICS.

**(Additional question) As for security certification, do you proceed on voluntary basis or on a request/recommendation basis?**

We think that certification is a driver to improve the level of security, and this applies not only in Europe. There are also requirements like the French one to apply to CSPN. However, the choice to undergo the certification of a product is of course market driven.

**2- Do you think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (e.g. more stringent testing/assessment standards for more sensitive products/applications and less stringent for less sensitive products/applications)?**

Devices that are more critical should have a higher level of security. Definitely some products have a very low risk. On top of some certifications, it would be good to consider self-declaration: in some area, there is a high attention on vulnerability assessment approaches. For me it is much more important to

---

have certification based on procedures in charge to the user managing the critical infrastructure. A certification has also to be considered in a system model: if the product is not used or configured in a secure way, there are vulnerabilities in charge of the critical infrastructure owner. We need a sort of way to certify requirements and we need to be able to specify which components are more critical and need a higher security assurance than others. One way to do that could be the self-declaration approach.

**3- Can you provide a case where a customer/user is not provided with enough/reliable information about the security properties of any ICT products/services? What is the problem for consumers: that information 1) is not provided at all 2) is not reliable 3) is not enough**

I do think that information provided to customer is not enough at least for critical infrastructure owners. Today we, as vendors, have in place cyber security programs to fulfil the information needs of critical infrastructure operators.

**4- Would you be in favour of the introduction of a common label signalling that the products have been certified within a certification scheme in accordance with EU rules?**

I definitely think that, even with the label, the customers need to understand what the label means and there is the need for some information behind. I mean there should be a transparent information about how this process of certification has been carried on.

**5- Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

We agree that a certification recognised between member states is required. We prefer to have a certification that is done in one country and is recognized in others Member States. We also prefer to refer to international standard to remain competitive at international level.

**6- Do you think the extension of the SOG-IS to all member states represents a valuable policy option? Can you please elaborate what do you think are the criticalities and positive aspects**

We feel that Common Criteria and SOGIS are not the right solution for ICS at the moment. Common Criteria costs 500k and lasts more than one year. This is a problem for a vendor. Common Criteria is a good approach for some kinds of components and products. In situations where the lifecycle of a product is more than 20 years, we have to find approaches at a system level based on procedures and self-declaration. ISO 15443 is an example of standard that we think is adequate for ICS context.

**7- Concerning an EU wide certification framework, do you think it would have a positive impact on costs for your industry? Can you please elaborate what do you think are the criticalities and positive aspects?**

In ICS context, we think that other levels of the system have to be certified as well, not only the product level. We need to make sure that the certification takes into account the different actors involved in the whole process. Some nations may have different needs on ICS and ICT requirements too. The application of a specific international standard has been debated, not only the framework. For non-critical devices, we also find that the solution could rely on a self-declaration process.

**8- In your opinion, what role the EU Agencies (such as ENISA) might have in the management and the operational tasks of an EU wide cybersecurity certification scheme?**

---

I think ENISA could play a role within industry to help to understand the concerns of the different national agencies. ENISA can play a key a role to harmonize Members States' Agencies on definition of national requirements and assurance, and assuring that the solution meets the needs of industry. ENISA should also cooperate with standardization institutes.

**(Additional question) Would your company be willing to actively contribute to the realization of the said EU framework?**

Industry would be available to contribute to the realization of the EU Framework. We are involved in cyber security taskforces and industry experts from these taskforces would be happy to participate. We also produced a policy paper that shows the position of pan-European vendors about relevant requirements.

*Interviews results from representatives of Conformity Assessment Body*

- 1- Can you provide a case where the certification of an ICT component is accepted in one country but it was not accepted in another EU country as another certification was required? In that case, did the company undertake a second certification or did it restrain itself from entering the market of that second country?**

My organization has in fact certified some products with vendors who have been successively requested to re-certify the same products. This was needed to enter the market of another country. Notice that the problem is not the recognition of certificates (Common Criteria), but the suitability of a certificate against country specific requirements (e.g., assurance level (Common Criteria EAL) and/or security requirements (Common Criteria SFRs). Vendors expect certificates to be valid for all customers, but most of the times this is not the case because of country specific requirements. This applies especially for governmental customers. Most of the problems arise from the semantics and the content of certificates (Common Criteria) and not from the lack of certificate recognition.

There are cases where a vendor, having already certified its product, has applied for a second certification to enter the market of the requesting country.

I do not know about cases where a vendor renounced to apply for a second certification.

- 2- Do you think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (e.g. more stringent testing/assessment standards for more sensitive products/applications and less stringent for less sensitive products/applications)?**

In some cases, end users are addressed with wrong needs and the concept of a single view on assurance is not useful at all (an example is the mandatory usage of cPP (collaborative Protection Profile) within CCRA to get certificate recognition for assurance level greater than EAL2). Certification has to be very flexible to provide what the market is asking for. ISO 15408 (Common Criteria, in fact) has sufficient room for flexibility.

- 3- Are you aware of national approach to security certification of some products which are being established in some MS? Do you expect new approaches established in the near future?**

No.

- 4- Can you provide a case where a customer/user is not provided with enough/reliable information about the security properties of any ICT products/services? What is the problem for consumers: that information 1) is not provided at all 2) is not reliable 3) is not enough**

I think there is a general lack of understanding of the security properties of a product from the user/customer. The information is not really provided.

- 5- Assume a labelling framework where a product can be security labelled after a successful security certification. Would this approach improve the situation?**

The problem with such a label is that it could lead to more confusion. If the label is too simple, the user could misunderstand the corresponding information. If the label is too complex, the user could be unable to understand the corresponding information. To be useful, the label should be well balanced.

- 6- Do you think a mutual recognition agreement of certification schemes existing in different countries may have a positive impact on industry costs?**

I think we definitively need a pan European solution to security certification in view of a single market. This solution could be in the form of MRA or of a European legislation. MRA are slow and difficult to

---

manage, and they could in fact be ruled (or more or less controlled) by some nations only. I would prefer a European legislation applied to all member states.

**7- Do you think the extension of the SOG-IS to all member states represents a valuable policy option? Can you please elaborate what do you think are the criticalities and positive aspects**

The fact that the SOG-IS does not include all member states is a real problem: it is a must to expand SOG-IS to all members states.

**8- Concerning an EU wide certification framework, do you think it would have a positive impact on costs for your industry (ITSEF)? Can you please elaborate what do you think are the criticalities and positive aspects?**

I think we need that: as an ITSEF, the framework is fundamental to my organisation. Note that 80% of our customers come from countries outside Europe. The rest are national vendors: certification in Europe is too much based on national reference (vendors in one country certify in that country). In general, there is no single market in EU.

**9- In your opinion, what role the EU Agencies (such as ENISA) might have in the management and the operational tasks of an EU wide cybersecurity certification scheme?**

Current schemes, which are governmental, do not really have resources and capabilities to suitably certify according to the current market requests. EU certification framework need to consider capabilities and to open the door to private certification activities. There is room for European Agencies (like ENISA) but there is also the need to find a role for private certification bodies and companies. I do not think a successful design can be done with just certification bodies: the EU certification framework has to open other realities such as ENISA, representatives from industry, etc.

*Combined answers from two interviewees from Smart Metering Industry*

- 1- Based on your knowledge, is the smart meters industry a highly regulated sector? Across Member States, are there existing security provisions and standards indeed override the need for labels and certification?**

We will both answer to this question. In the current situation there are few countries that are asking for a security certificate that are UK, Germany and France. Their process of certification is based on national requirements that they started to write. In the UK they are called security objectives. Based on these requirements and objectives they defined a security certification approach at a national level. So far, I haven't seen any reference to any international standards because these standards are still quite high level and very general. They are not suited for a certification. That's why there are national definitions based on which national certification takes place. It's mainly that you have to repeat three times different methodologies to prove that you have secured your device, which means that you'll have to face three times more costs. This is not possible.

- 2. If France, Germany and UK did not introduce the national requirements, what would smart meters operators be required to do as security measures?**

The motivation for the industries to invest and to innovate on this topic is limited because of the market structure. Another thing is that the liability for damages for operators in different countries is not even when they comply with the legal environment. I would like to stretch that the three methodologies that France, Germany and UK use are all standards, which is not a problem. The problem is that there are too many standards. Another problem is a problem of European accordance of minimum requirements of documentations and tests results, for the same functionality and in the same language, ready and accepted by the different authorities of different countries. This is an important message that should pass to the Commission.

- 3. So, the introduction of these three different standards made operators to go through other tests three more times, by adding more costs?**

Yes, It also block the innovation. The additional costs could be invested in other innovations.

- 4. We talked about the different standards from Germany, France and UK before and it was said in the previous interview that the costs for the German certification is approximately one million. Is that correct?**

Yes, and it would include the indirect cost, which is the non existent market. Companies invested for six years and they do not have anything back so far.

- 5. For France and Uk, it was said that it could reach almost 150 thousand euros. Is it right?**

Yes, it was in the Smart Meter sector. We received these information from the meters manufacturers so it's specific for the Smart Meter Certification. This information is related to the Uk. For France it should be a similar range, around 150 thousand euros for one certificate.

- 6. For which reasons is there such a wide range of costs? Are there big differences between these Smart Meter industries? Is it related to the different approaches in these three countries?**

The approach in France is for instance more focused on testing in a fixed time: given the products and the deadline for certification, all the security tests have to be completed during that time. At the end of the fixed time, you receive a report on whether it is working fine or not. In the German approach, they have a higher level of certification. The standards are the same but they have higher levels of tests for the certification. How thoroughly you can test the device is the difference. The Germans are using the Common Criteria as standard. They started in 2011 to use these security certification standards as

requirements. They also added requirements for privacy and security as well as other processes to maintain these standards during the lifecycle. The testing methodology is end to end: for instance for software coding you need to have your own site, where only authorized coders and cleaners can enter the room. On the other hand in UK and in France they put just a security assessment on one product, while in Germany the whole infrastructure need to be tested and certified. The basic functionalities and requirements are the same but it doesn't mean that at other levels the German certification might be more efficient. There are in fact different architectures for different smart meters. For instance, the French ones won't work in Germany. The data and the controlling is different. Same is for UK. However the basic function requirements are the same.

**7. Would the higher costs for certification in Germany be a barrier to the market for small and medium industries? If the architectures are different, wouldn't a European certification framework also require different standards?**

There is clearly a difference in attitude in different countries. There will be for sure some countries that believe that their approach is better than any other one. They will have different architecture and different security measures like in Germany. What would be interesting is to see how the market would respond to this. German Manufacturers will probably follow this standard but other European producers will probably prefer other countries. It is our expectation however that the majority of the European States would agree with the European approach for certification. They will accept certifications made by other European countries. If a particular Member State would require additional test, they should be able to demand it. The basic requirements on security are very similar in all the European countries. If we say that 80% of the requirements is the same for all countries, then there will be only a 20% of the standards that should be covered in order to enter the market of another European Country. This would be more attractive economically and financially. It would in fact be a basic certification for everybody and, maybe, even Germany would accept that basic requirement since it might be the same.

**8. Another advantage might be that the money that won't not be spent for other national certification, they could be invested in the cyber security sector. Is it correct?**

Yes, absolutely. For instance, for my company, I won't have to find several solutions for each country for security and there for invest the money of those costs in development of other cybersecurity measures, that require constant updates. Maintaining certain levels of security in various different countries would also be way more expensive and difficult than if they were in European certification framework. On a national level, the ICT guys are imposing their visions on the Energy guys and their approach is not very successful. At the same time, the Energy guys are ignoring all the risks. They are not reliable.

**9. I would like to deepen the aspects related to the small and medium enterprises. Considering the previous hypothetical situation of an 80% of states that will use the European standards, do you think that smaller and medium enterprises would be favored to penetrate in these countries?**

Basically, with a European framework the barrier for the market entry would be easier. It's hard to define if they would be able or not to enter the market because it will depend on that 80% of common costs. For sure, it would lower the barrier so they would have more chances to do it. For the markets that won't accept the certification would still have problems. There might be two sides of the company. In a very fragmented market, there might be few national champions with certain innovations but bigger player might eat them but this is not related to the security certification. In Germany 5 out of the seven companies that are putting their products on the certification are smaller companies. Only one player is global. The challenge however is that in the Smart Meter sector, the product cannot leave the German market, at the moment.

*Interview results from Expert on Cyber Resilience of Critical Infrastructures*

- 1. Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience**

I worked on these issues as I was working for the ERNCIP (European Reference Network for Critical Infrastructure Protection). The aim would be to arrive to a certification framework for the Critical Infrastructure. The discussion on a certification of the components started two years ago or so because of the French and German influence, as well as DG CNECT. If I am not wrong, last year there was even a Call of Proposal in order to fund projects in this field. I'm still skeptical about certifications and benefits that they could have on the improvement of the Critical Infrastructure resilience.

- 2. Do you know cases in the European Union where some ICT components of critical infrastructures, even though already equipped with some security certifications accepted in some MS, are requested or recommended to get additional security certifications in order to access the market of other MS?**

Yes, there is. Certification means to certify towards other referential standards. There is the Common Criteria but it doesn't work and there is proof of its inefficiency. Only by checking their website, it is easy to understand that there are only few products for the critical infrastructures that had been certified by the Common Criteria. Furthermore, the ISA Security Compliance Institute release the ISA SECURE certifications: even in this case there are only few certified components. It's a too little number for such a complex system. They are way too expensive and they don't have a future. These certification processes are too difficult to go through because there is too much bureaucracy and paper forms to fill. Another problem is the definition of Standard. What are the reference ones? In the critical infrastructure domain, it takes too much time –even more than 10 years – to decide them. In France with the ANSII and in Germany with BSI, there is fragmentation. In Italy, on the other hand, there is no requirement and in all the other Member States there isn't any mandatory certification. You only have to comply with the Standards. I come from a background in the Nuclear Sector, where standard compliance to certain standard is mandatory and extremely strict. As for the certification I think that it's only useful for the creation of procedures that turn out to be long, complicated and expensive.

- 3. Do you know ICT products/components/service deployed in critical infrastructures require mandatory cybersecurity certification?**

No

- 4. As for operators that purchase and adopt components and products for the critical infrastructures, do you think that their choices are based on product certifications or on other features?**

I believe that their choices are based merely on the producer name. The company brand from which they purchase the components is like a security guarantor. For instance, buying from Schneider Electric and Siemens is probably more reliable than purchasing from a Chinese producer. There is, however, an issue to point out: most of systems and products on the European Market have embedded components that come from China where the security standards are less available to check. So, how can I be sure that Chinese components respect security standards and certifications that will protect me from risks? For example, the microprocessors of PLC (Programmable Logic Controller) components have Chinese origins.

- 5. Do you know any National Certification Scheme in Europe?**

Besides France (ANSSI) and Germany, I know the existence of the national schemes in UK and the Netherlands.



**6. In your opinion, to what extent does the current (or possible) existence of multiple cybersecurity certification schemes represent a barrier to EU market entry in the critical infrastructure domain?**

Yes, it's definitely a market problem. If the European Commission would be able to apply a European label, components and products with an Italian certification would be able to be sold in Finland. If we could manage to have European standardized framework, the market would benefit from it. It's similar to the food labels. Without a free movement of goods in the EU, there would definitely be market limitations. Without a European Certification, it would be very difficult to sell products in more than one European Country.

**7. In your opinion, would a European cybersecurity certification framework that support the mutual recognition of cybersecurity certification reduce costs for manufacturers of components or service providers used in critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

Yes, sure. Furthermore, having multiple certification laboratories is even more expensive. You need to prepare the maintenance staff of these structures and, with European certification, it would be possible to reduce these laboratories. It will be therefore possible to reduce these costs on the long term.

**8. By adding an information label on the product that certifies the security standards – as it happens for medical devices – do you think that it would be possible to reduce the information asymmetry? Would it be possible for the consumer to compare more products and have more information on its security standards?**

Yes, absolutely. As for the medical devices, we are talking about expensive and complicated machines that are bought by operators, for example Tomography machines that cost approximately one million euros, and not by normal citizens. It is more a Marketing issue: as I use a label to certify my product, it can be sold more easily on the European Market. Should I be surer about its security, though? Not really, as far as I am concerned.

**9. What are the benefits for a certified product? Would a customer buy it more likely?**

It's always a matter of Trade-Off, whether to put a certified product on the market or not. If the certified product is three times more expensive than the not certified one, I am not sure I would buy it. It's an old dilemma if the security costs are a long term investment or not. Through mutual recognition of a certification framework it would be better. However, it should not add any other cost on the producers.

**10. Would you be in favor of a European Scheme of mutual recognition between the member states?**

Yes, I am because of the free market benefits and not because of the possible improvements of security in the Critical Infrastructures. I am positive towards a European Label. The certification, however, should be discussed on different levels: what about the compliance standards? And what about the laboratories? They are different discussions.

**11. Are there any regulations that makes certifications mandatory?**

There isn't any mandatory certification in Europe. There are other private activities such as the Norwegian DNV and the German Thuf but there isn't any mandatory certification.

**12. We are wondering if a certified product might guarantee more openness to the different markets. What do you think about the functionalities of it?**

---

Let's take an example. A PLC is well defined functionally. It is more difficult however for SCADA systems. The certification won't guarantee only their functionalities but also its immunity to external threats and other vulnerabilities.

**13. For these components, the security requirements are very important. Are there security tests of the components?**

After the functional tests, they check the security of the component from external threats through tests in laboratories, like the penetration test. Recently, in the United States, hackers managed to hack in to cheap CCTV cameras, produced in China. They were extremely common because of their affordable price but they had lower security standards. Therefore, Hackers managed to enter their system and block the whole network. Enel is going to sell 24 million Smart Meters. If these devices would have a security certification, we would definitely be safer. On the other hand, if they have vulnerabilities, hackers would be able to enter a network of 24 million devices and turn off the lights of Italy for at least one day. There is a lot that should be done: defining the limits of a certification, what are the standards and what is its contribution to security. I worked with ENISA and I think that we should work more on the meaning of this certification/label and on the real effects that it could have on resilience.

*Interview results from representative of a manufacturer operating for Critical Infrastructures*

- 1- Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience**

There are different advantages and some of them are quite obvious. It allows the entrance to several markets that have particular requirements. It is also an advantage for the transparency of the information for the customer or the regulator. By certifying products, you can step up versus a competitor and be in a better position on the market. For the security of the product itself, it can be helpful but I think that the major advantages would still be related to the transparency of the information and the entry on the markets.

- 2- Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?**

As for critical infrastructure operators is crucial. If you do not have a certification, you cannot know if the information is true. Each company could claim that their product is secure but it is better to have third parties to test it independently. That is definitely another advantage that a certification could represent. However, I still believe that the main one would be the entrance on the market.

- 3- Do you know cases in the European Union where some IT/OT components deployed in critical infrastructures are requested, mandated or recommended to be provided with some type of cybersecurity certification?**

It depends on what products are compelled. It is primarily around security products and services, such as firewall, IPM, intrusion detection systems, routers, so this kind of networking devices, like routers and switches. There are different criteria and standards that are required. In some cases, we do multiple certifications because other markets require them. For example, in France, you need to have an authorization issued by the Prime Minister Office for network devices in Critical Infrastructure. It is common for government to require certain standards for Critical Infrastructure and security products and services.

- 4- Do you have any example of national certification or scheme?**

As a company, we rely a lot on Common Criteria. Getting certifications in each member state is complicated, expensive and time consuming. On standard sides, we follow ISO standards. As for local ones, we have specific requirements by the military law for security devices. In Germany, we have some requirements from BSI.

- 5- In your opinion, would a European cybersecurity certification framework that support the mutual recognition of cybersecurity certification reduce costs for manufacturers of components or service providers used in critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

I am not sure what the framework is exactly trying to achieve, a part for mutual recognition. There are many basic and common requirements at a national level but they can also be certified through the Common Criteria. I am not sure about what Europe can achieve for security issues. I am not against the Commission having a board and controlling the situation but I am a little bit skeptical about the results. There is a problem of fragmentation, especially since more European countries became skeptical on Common Criteria. There is a lot of work for ensuring security of products.

- 6- Do you know cases in the European Union where some ICT components of critical infrastructures, even though already equipped with some security certifications accepted**

---

**in some MS, are requested or recommended to get additional security certifications in order to access the market of other MS?**

Yes, it depends on the type of product and the Member State. Even with the Common Criteria most of the time you have to do other tests because they cover only the basics. Furthermore, certain devices require specific extra certifications such as networking devices. At a national level, for instance, in Germany, for security devices, they have to cover by the Common Criteria but also they have to go through specific tests locally to prove that your devices are reliable. There are also type of products that need to be certified against additional requirements for critical infrastructures in France made by ANSSI.

**7- Can you provide us some information about the costs of certifications?**

Yes, on Common Criteria alone, last year, we had 20 certifications and it costed us around several hundred thousand euros each, including the external resources, laboratories etc.

**8- Do you think that these costs represent a market barrier for smaller and medium enterprises?**

It depends on the type of the companies we are talking about. If you are a Germany encryption company, you have Philips on the other side so you will probably have to look on other markets. Unless you decide to collaborate with the bigger Germany companies. Otherwise, you will probably struggle in finding German customers. From the costs perspective, if you are a smaller company and you are trying to enter on other MS's markets you will struggle.

**9- Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?**

The biggest problem is the fragmentation. There are different kinds of certifications but they guarantee certain standards. Only at lower levels, there might be a problem of lack of transparency on security measures. It is harder to understand if they are secure.

**10- Is there any information or issue on this topic that you would talk about? Something concerning labelling?**

Yes, actually there is. In our company, during the last year, we have been discussing on the idea of IT trust labels for devices. We think that it might be a more effective solution, especially for critical infrastructure. Instead of a common framework, labels might be more useful as a solution for the information asymmetry. Now, most of the end devices for Critical infrastructures are regulated but not checked. A label would be different from a Common Criteria because it would more of an insurance in order to enter the market. The best would be to have both a label for the basic requirements and another one for the specific and higher ones.

July 24<sup>th</sup>, 2017

*Interview results from representative of a European Association for Forwarding, Transport, Logistics and Custom Services*

- 1- Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience**

Yes, there are many. When it comes to security equipment, especially Air Cargo, it is important to have secured components. Security is also very important for screen technology and other IT components as well. A standard security certification of the components is always a good thing. It something that should now exist on a general basis in cargo screen technology. We support in fact a harmonization of the various markets on security standards and certifications. Our only concern is whether logistics is considered a critical infrastructure. Germany considered it as such and it is the most advanced on this issue. However, not all the Member States consider it as such, because in case of a problem with a particular company, you can always ask to another one. However, this point of view does not consider the possibility of a larger cyber-attack, which goes across the whole industry. Not the whole logistic sector should be considered as a critical infrastructure, but there are for sure certain structures that should. Airports are a clear example of this. Furthermore, another entity that we need to deal with, for security standards, are the governments.

- 2- Do you know ICT products/components/service deployed in critical infrastructures require mandatory cybersecurity certification? Do you know European National Certification Scheme?**

No, no that I know of. There might be some, but from the discussion we had on cybersecurity, it never came out.

- 3- Before you mentioned the German approach, do you have any examples of certifications or any experience related to it? Do you know costs and/or procedures that it might require?**

No, I do not, unfortunately.

- 4- In your opinion, would a European cybersecurity certification framework that support the mutual recognition of cybersecurity certification reduce costs for manufacturers of components or service providers used in critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

Yes, I think an EU certification might have a positive effect. We support this kind of policies because we believe that is always preferable to have a common European Scheme. We believe so because it would not only increase the security levels of all Member States but it would also be good for the market. It has to be made properly however. The certification need to be designed based on the necessities of the industries and the member states.

- 5- Do you think that an EU wide Certification Scheme could brings advantages also for smaller and medium companies reducing market barrier?**

Yes, sure. Being able to buy certified products from every member state would help even smaller and medium companies to enter the market. You would be able to buy different components for your network more easily. It is important however that the requirements of the certification are appropriate. It would be helpful also because on the European market the majority of the enterprises are SMEs.

- 6- Based on your experience, do you think that critical infrastructures are at greatest risk because of outdated security practices / policies and limited regulatory oversight?**

We had a lot of discussion about this issue with the European Commission on the current cybersecurity situation and the latest cyber-attacks. As it turned out, most of the companies that had been attacked

---

were underprepared and there was not enough information sharing between them and on what they needed to do. It is extremely important to have updated practices, update processes and updated technologies. This should not happen, once the cyber-attack took place. Operators need to act in advance to prevent them and share information. We think that standardizing security will bring down the costs that could be invested elsewhere. Mandating certain practices will not be the best solution because security requires continuous updates. Rather than prescribing procedures, it would be better to have a constant evaluation of risk assessments through a security check approach.

**7- Do you think that certification and labelling of ICT products/services may contribute to enhance the level of assurance of critical infrastructures? Do you think that certification and labelling of ICT products/services may contribute to enhance the level of information?**

Yes, sure. It would be more effective.

**8- Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?**

Yes, I think that in general they do. It probably depends on individual experiences but I think that they receive the basic security information on the component. I think that the situation could still be improves. Making the information more available and clearer would definitely help the operators and avoid certain situations.

**9- Do you think that this approach of mutual recognition in Europe would have advantages for the different stakeholders of the market? Do you think that it might have other benefits?**

Yes, I think it would be a good solution. It would make the security easier to obtain. The mutually recognition across EU might even have positive effects globally. I think that it would be good if the risk agenda of the EU could attract other non-European countries to join the mutual recognition. States like US and Canada and many others might be interested in the future to join such mutual recognition.

*Interview results from representative of a European Bank*

- 1- Based on your knowledge, what are the main advantages, if any, of adopting security certified ICT/OT components in critical infrastructures? Please consider possible advantages also in the field of attack prevention and/or resilience**

Yes, sure. There are for sure some advantages of using security certified components. I think that a certification adds a lot of value. For instance, I use HSM devices (Hardware Security Modules) that fit with security standards compliance. It allowed us to store critical data on a secure device. It's mainly from compliance assessment that I get advantages. With compliance, it doesn't always mean that is more secure than other devices though.

- 2. Do you know whether the critical infrastructure operated by you adopts some ICT/OT products which come with some types of cybersecurity certifications? In this case, do you have any idea of costs of this certification?**

In the finance industry, as an example, our services must have secure encryption and use HSM, which are incredibly expensive. In order for us to use a HSM component, it is going to cost us around 20.000 euros and that is not the whole device. Devices with five of them like a hot standby, business computing and others are going to cost around 100.000 euros. All of that would be needed just to store key credentials of the encryption.

- 3. Do you know cases in the European Union where some ICT components of critical infrastructures, even though already equipped with some security certifications accepted in some MS, are requested or recommended to get additional security certifications in order to access the market of other MS?**

In the Finance Sector, we have to follow the EU directives for payment services. With other countries, like the US we do not have to do it. I have to be compliant with the 54 jurisdictions of countries we are operating in. These procedures become very prescriptive and we have to deal with many descriptive requirements that sometimes might even be contradictory.

- 4. Do you think that operators of essential services have a sufficient level of information regarding the securities features of the IT/OT products /services they use for the lifecycle of their infrastructures?**

It is not really a lack of a transparency; it is a lack of understanding of security requirements. There is a perception that if everybody performs by following the prescription, it will be secure. However, this is partially true. The problem is that most of the time the prescription doesn't cover everything and they can still be breached. For me, there is a dichotomy between compliance and security. I spend a lot of money and a lot of effort for the compliance, which is not necessary a guarantee for security.

- 5. Do you think that the costs, due to this fragmentation of compliances and the duplication of costs, could be invested in other security solutions?**

Yes, absolutely. For example, there are security organizations that require more people to work on the compliance than the ones working on security solutions.

- 6. In your opinion, would a European cybersecurity certification framework that support the recognition of ICT security certificates reduce costs for operators of critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

If it became too prescriptive, it might be too difficult to comply to, as it happens for the other jurisdictions.

---

**7. Do you think that a soft approach, which only give guidelines to different stakeholders, could be more useful? What kind of approach would you suggest otherwise?**

If you look at the GDPR regulation, it is not prescriptive around the world. I think it would be an appropriate approach.

**8. What do you think about a label on the products with the security information?**

I think it would not make too much difference. As an example at the Data Centers, engineers would configure the devices without physically seeing them. Therefore, they won't be seeing it.

**9. What would be the effect of a European certification scheme on SMEs? Do you think they might have advantages?**

Many of the security products are very technical. Even if there would be a certification, I am not sure that the SMEs would actually understand the security standards and tests of the product. I think that they would not know all the distinctions.

**10. Do you have any information on Cloud Computing? Do you think that this ICT certification in this field would have advantages?**

At the moment we are not using Cloud Computing. There is a barrier from using them because we cannot be sure that the data is stored in a secure way, especially according to the various jurisdictions. Since we are a regulated entity, that is a barrier for us. Most of the banks are struggling with that challenge. There are problems because the European data might be stored in South America, or in somewhere else, under a different jurisdiction. It would also be more expensive because of that.

**11. Do you think that a certification might give more advantages on the security of the Cloud?**

If they are certified it would definitely be more cheap and it would be easier for the security compliance of the different jurisdictions. However, I still don't feel comfortable with them because they are not secure enough by design.



*Interview results from representative of a Telecommunications Company*

**1. Do you know ICT products/components/service deployed in critical infrastructures require mandatory cybersecurity certification?**

I am going to answer you with an insight from the UK perspective. First, we are contractually obliged to look for security certification on products and services for the national infrastructure. They have to be certified on a variety of schemes in order to provide their service to the critical national infrastructure. In the UK, there is the CAS(T)<sup>15</sup> scheme, which is a telecom specific version of ISO27001 and that is a fundamental security certification for any product and service that is sold. Furthermore, the Public Services Network need to be certified every year as a prerequisite. It will not be possible for us to sell it in UK, without certifying them.

**2. Can you provide some information related to costs of the certification?**

Yes, for example for one of our network platform the overall budget was of 500.000 UK pounds. It included 39 different services, whose price range from 10 to 15 thousands UK pounds each.

**3. Do you have an idea if this certification is recognized through Europe or if it is only for the UK?**

I would say that it is valid only for the UK. If we look at the CAS(T), the equivalent of the ISO 27001, it is issued by the National Cyber Security Council. Therefore, it is more UK centered and not European. However, in terms of what it is asked for, it is based on an ISO standard.

**4. Do you have any idea if a certified product in another country has to go through the UK certification process, before entering the market?**

Any product worldwide of this sector, which should be sold in UK, has to go through the certification scheme. There are by use non UK certification that have value like the Common Criteria, but they still need a formal approval to sell it by the UK.

**5. In your opinion, would a European cybersecurity certification framework that support the recognition of ICT security certificates reduce costs for operators of critical infrastructures? Can you please provide your view on other possible positive or negative aspects?**

There are many security standards that we have to comply to and there is one on cyber security resilience coming soon in the UK. If all of the certification bodies would recognize these security tests, we would save a lot of money. We have just started to see the benefits of the interventions to try to facilitate mutual recognition of the national security certification. We support this kind of initiative.

**6. Do you think that the current situation of certification could represent a barrier for European market, especially for the SMEs?**

In the UK, there actually a lot of standards for product security certification. There are at least four schemes that are run by the UK National Technical Authority. They range from test marking, encryption etc. and there is no doubt that the cost of certification would be a barrier for vendors who want to enter the UK market.

**7. Do you think that operators or customers have a sufficient level of information related to the security of their IT devices?**

---

<sup>15</sup> CAS (T) is a certification scheme for clients providing telecommunications services. The scheme supports the government Public Services Network (PSN), which requires all telecoms services procured by public sector bodies.

---

This is a personal opinion but I think that there is a lot of confusion on the meaning of each standard. Most of the people do not understand what the security certification means and what does it guarantee you, on the purchase side. I think that too much information sometimes might create a lot of confusion.

**8. Do you think that a label with the main information might be a solution for this problem?**

I am not sure. I think it depends if they understand the meaning of the label mark on the product. It would be useful to distinguish between two products but I am still skeptical about it. I think it depends on which customer group we are talking about here. I have to say that most of the organizations, who purchase components and products for the critical infrastructure, have the technical knowledge to distinguish between different levels of security protection. In the case of IT devices in general, I believe that –yes- a security label might be useful for consumers. Furthermore, for the case of IoT devices, I think there is still a rationale for a certain type of labelling framework. It's a difficult questions to answer to because it is too general.

**9. Considering the current situation, do you think that the critical infrastructures are at a greater risk because of the fragmentation across the market?**

Yes, I think so. The security level change across Europe and I think it might be problematic for the critical infrastructure.

**10. We are doing a case study on cloud computing. Do you think that the lack of a certification on this kind of service could affect the choice of companies to use it? Do you have any experiences to share with us, related to the Cloud services?**

There are definitely several issues related to the Cloud, including trust ones. It is more difficult because it is not suitable for all certification. I have an example related to critical national infrastructure. Virtualization and Cloud have many benefits for the management of the critical infrastructure but it is important to know every technical aspect and functionality of it.

**11. Do you have any other suggestion or advice for the European Commission on the topics we discussed before?**

Critical infrastructures are by definition more critical than IoT, in general. However, the fragmentation is a common theme for both of them and, as we have seen, it unhelpful. For this reason, we support what the Commission is trying to do. With that said, we think that the European Commission, in her impact assessment, is going in the other direction, for what concerns certain solutions. We would not support the extreme one such as support mandatory requirements. We think that the more moderate attempt, that keeps in consideration both the European Market and each jurisdiction, would be better. I think that it would also be positive if European Commission, instructed by ENISA, could define a set of best practices. As we started working on the IoT with the European Commission, there were different opinions regarding the possibility of a label. We were supportive. In fact, if the label would be reassuring for the customer, it would also increase the trust in the company. There are two issues however. First, it is quite difficult to communicate security levels through a label. Secondly, there would still be some kind of fragmentation. The labelling in itself is good but there should be a proper discussion on how does it communicate.

---

## 7.2 Questionnaire

In order to assist the **European Commission - DG CNECT in gathering evidence on ICT security certification and labelling**, the consortium made an online questionnaire open up to 19<sup>th</sup> June 2017.

The Questionnaire will help the Consortium and the European Commission to build additional specific evidence to the results of the ENISA survey on “EU certification and labelling framework”, which is a key step to **support the design of a European policy/regulation which is close to the needs of the European ICT industries**.

The questionnaire has been designed by putting multiple closed questions and some open questions where the selected stakeholders can more detail some relevant aspect. The Questionnaire template can be consulted here below:

### A. Introduction

This questionnaire is organised by PwC and Fondazione Ugo Bordoni FUB to assist the European Commission in gathering evidence on ICT security certification and labelling. It takes into account the results of the ENISA survey on “EU certification and labelling framework” and aims at building additional evidence. By answering to the questionnaire, you will provide critical support for the collection of data on the impact of vendor’s strategic operations, consumer’s behaviours and what is the most desirable policy option and most conducive regulatory environment for such critical area of activity.

This questionnaire includes multiple-choice and open questions. You can only choose one option for each question. If a question is not applicable to you, or you do not know which option to choose, simply skip that question. Once an option is selected, it can be changed to another option, but you cannot completely remove your response.

All responses recorded, including any personal information you provide, will be kept strictly confidential. Your input will only be used in combination with the responses of others participating in the questionnaire. Our research examines the opinions of groups of respondents. Your individual responses will not be shown to anyone outside the study team.

### B. Registry questions

What is your first name?

What is your last name?

What is your email address?

*Please provide your email if you accept being contacted on the subject of the study*

What is your type of organization?

- Evaluation lab
- Certification Authority
- Public Administration
- ICT Security expert
- Vendor (service/product)
- User (service/product)
- Other

What is your role/profession?

What is the name of your organisation?

What is the country where your organisation operates?

---

## C. Evidence section

### 1. In your opinion what is the best strategy/policy option to increase consumer's trust and confidence in ICT products?

- Implement a bill of rights giving to customers a chance to make claims after having purchased ICT devices
- Adopt a certification and labelling scheme allowing customers to compare in an informed way which products offer the highest level of security
- Hard-law approach, increasing trust through the introduction of disciplinary sanctions
- Financial incentives to vendors encouraging them to regularly replace and/or update old products
- Other

If option "other" is ticked please provide further explanation:

### 2. Do you think security labelling of ICT products/services (whether certified or non-certified) is likely to impact consumers' behaviours despite any price considerations?

- Very likely
- Likely
- Indifferent
- Not likely
- Not likely at all
- Don't know

### 3. Do you think the consumer trust in the security properties of product/service is likely to increase when certifications are performed according to security requirements set by third party entities, as opposed to security requirements being freely chosen by vendors?

- Very likely
- Likely
- Indifferent
- Not likely
- Not likely at all
- Don't know

### 4. To which extent do you think the quality, reliability and exhaustiveness of information on the security property of ICT products is likely to influence consumer/user choice over other type of factors such as costs?

- Very likely
- Likely
- Indifferent
- Not likely
- Not likely at all
- Don't know

### 5. On average what is the range of costs for certifying an ICT service/product?

- < 10.000 €
- 10.000 € – 100.000 €
- 100.000 € – 1.000.000 €

- 
- > 1.000.000 €

**6. On average what is the range of costs of labelling of an ICT service/product (excluding any cost related to the certification process)?**

- < 1.000 €
- 1.000 € – 50.000 €
- 50.000 € – 100.000 €
- > 100.000 €

**7. Can you please provide an example you are aware of a security certification requirement a company had to undertake to access the market of an EU country? (specify at least name of certification, type of ICT product, country) (Include average costs from questions below)**

**Could you provide an educated estimate of compliance costs and time:**

**8. Can you please provide an example you are aware of a security labelling requirement a company had to comply with in order to access the market of an EU country? (specify at least name of labelling scheme, type of ICT product, country)**

**Could you provide an educated estimate of compliance costs and time:**

**9. Can you please provide an example you are aware of a case of national procurement bids/practices restricting open competition in favour of mandatory national certifications? (specify type of ICT product, country, procurement procedures and enforcement e.g. mandatory or recommended)**

**10. How likely do you think a large-sized company which has certified its product in a given EU country would restrain itself from entering the market of a second MS in consideration of additional security certifications requirements?**

- Very likely
- Likely
- Indifferent
- Not likely
- Not likely at all
- Don't know

**11. How likely do you think a SME which has certified its product in a given EU country would restrain itself from entering the market of a second Member State in consideration of additional security certifications requirements?**

- Very likely
- Likely
- Indifferent
- Not likely
- Not likely at all
- Don't know

**12. From your experience, what is the likelihood of an ICT product/service vendor to accept bearing the costs of a second certification/labelling process in order to access the market of another EU country?**

- Very likely

- 
- Likely
  - Indifferent
  - Not likely
  - Not likely at all
  - Don't know

**13. In reference to commercial strategies, do you think a foreign vendor is likely to favour accessing an EU country having in place a mutual recognition agreement (in relation to security certification and labelling) with other EU countries?**

- Very likely
- Likely
- Indifferent
- Not likely
- Not likely at all
- Don't know

**14. In your opinion, in the context of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the management level (e.g. Establish transparent procedures)?**

**15. In your opinion, in the context of the creation of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the operational level (e.g. Identifying needs, cooperation, coordination, alerting)?**

**16. How likely do you think a European ICT security certification Framework would produce the following benefits?**

1) higher consumer trust in the security properties of the product/service

- Very likely  Likely  Indifferent  Not likely  Not likely at all  Don't know

2) higher number of certified/labelled products/services

- Very likely  Likely  Indifferent  Not likely  Not likely at all  Don't know

3) lower time and cost of certification/labelling

- Very likely  Likely  Indifferent  Not likely  Not likely at all  Don't know

4) reduction/elimination of fragmentation (meant as the existence of multiple national and sectorial certification schemes not mutually recognised)

- Very likely  Likely  Indifferent  Not likely  Not likely at all  Don't know

## Results

The Questionnaire results have been collected and analysed. Twenty-five Representatives from different type of organisation gave their contributes to the online Questionnaire. In the graphic below, the percentages of the types of organisation that have completed the Questionnaire are shown:

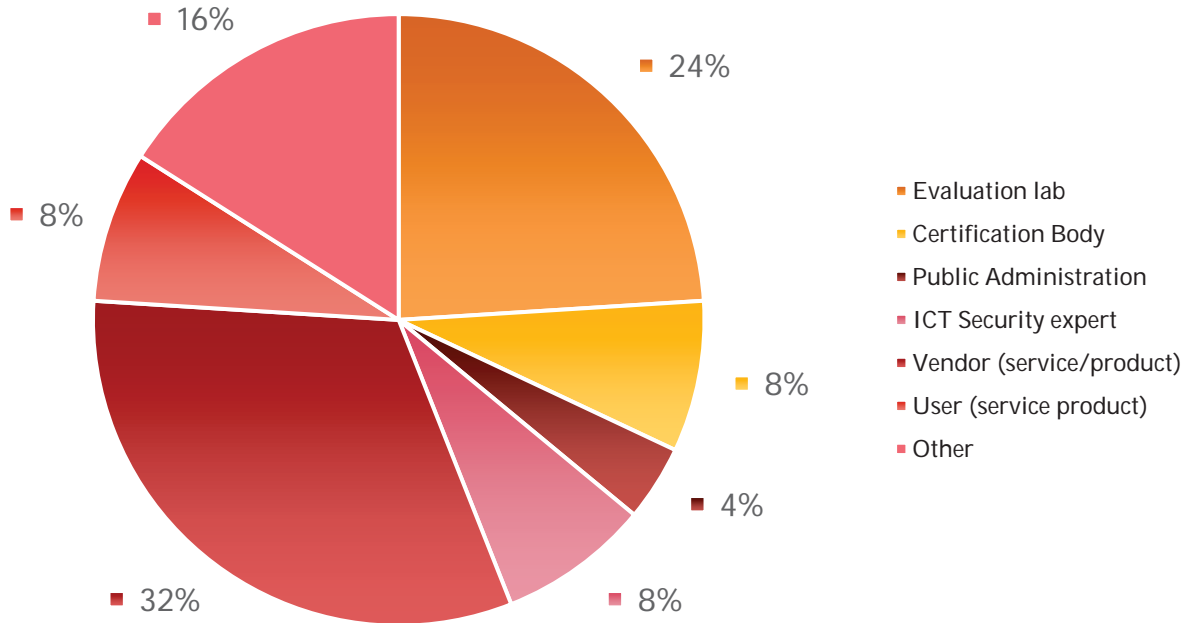


Figure - Type of Respondents

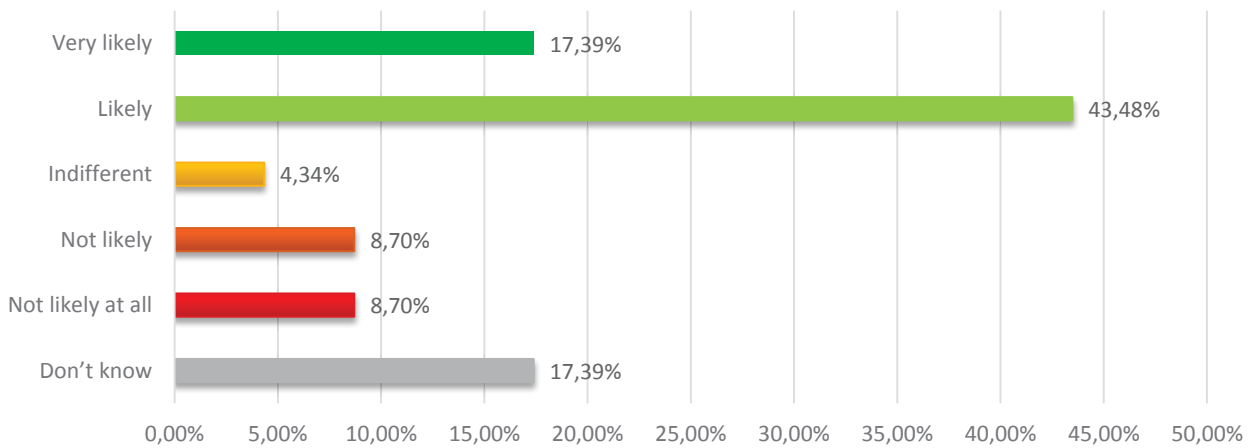
### 1. In your opinion what is the best strategy/policy option to increase consumer's trust and confidence in ICT products?



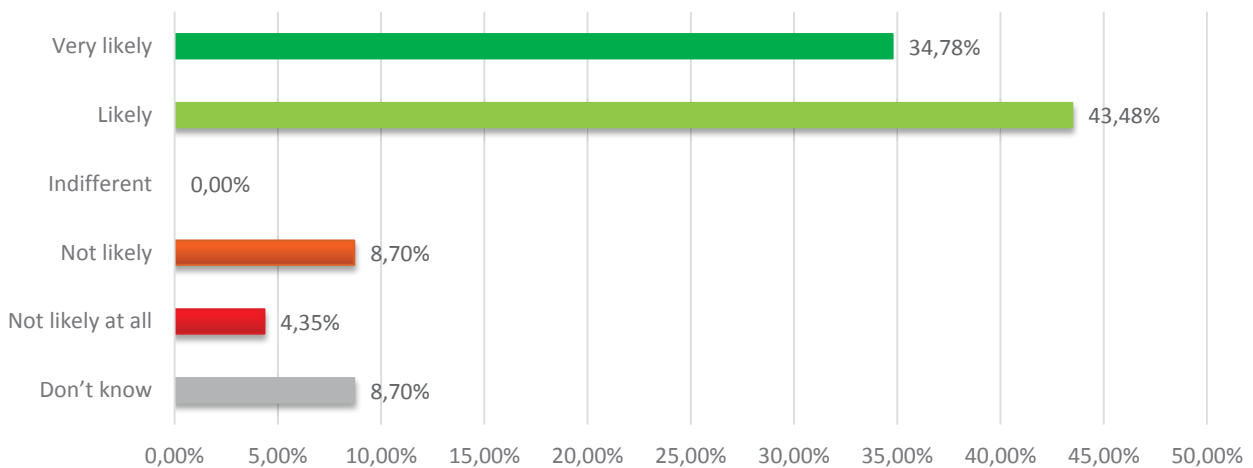
**Explanations provided for the option “other”:**

1. Evidence of conformance with applicable, recognised standards
2. Hard-law approach translating IT security Requirements in Protection Profiles supporting CC evaluation/certification plus financial incentives to vendors encouraging them to certify their IT products/system and maintain the certifications through time
3. A mix of above-mentioned proposals would be the best strategy to increase consumer’s trust and confidence, adopting an EU-wide certification and labelling scheme shall constitute the core of the future strategy of the European Commission. To be efficient, certification and labelling shall apply to all ICT products and services, therefore a hard-law approach is necessary. Remark: With regards to certification, Eurosmart advocates for a scalable approach linked to risk management. Depending on the different security and assurance levels, and on the robustness to be provided, the metascheme could encompass different certification schemes from self-assessment up to Common criteria highest levels.
4. Industry-led best practices (with government input) on cybersecurity baselines -&gt; similar to the NIST Cybersecurity Framework as a model (could be adapted for EU needs) which is based on existing international security standards (and for which certifications are available) are critical in an effort to increase customer's trust and confidence in ICT products. In addition, financial incentives and government procurement power can play helpful roles if applied sensibly.

**2. Do you think security labelling of ICT products/services (whether certified or non-certified) is likely to impact consumers’ behaviours despite any price considerations?**

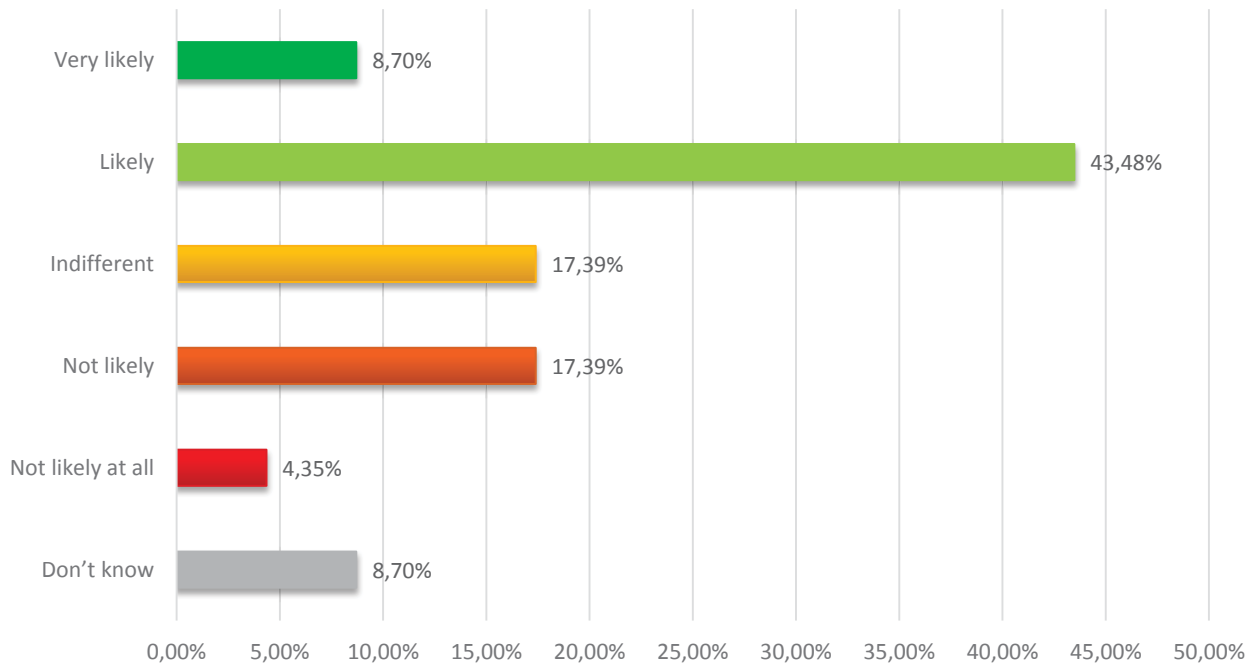


**3. Do you think the consumer trust in the security properties of product/service is likely to increase when certifications are performed according to security requirements set by third party entities, as opposed to security requirements being freely chosen by vendors?**

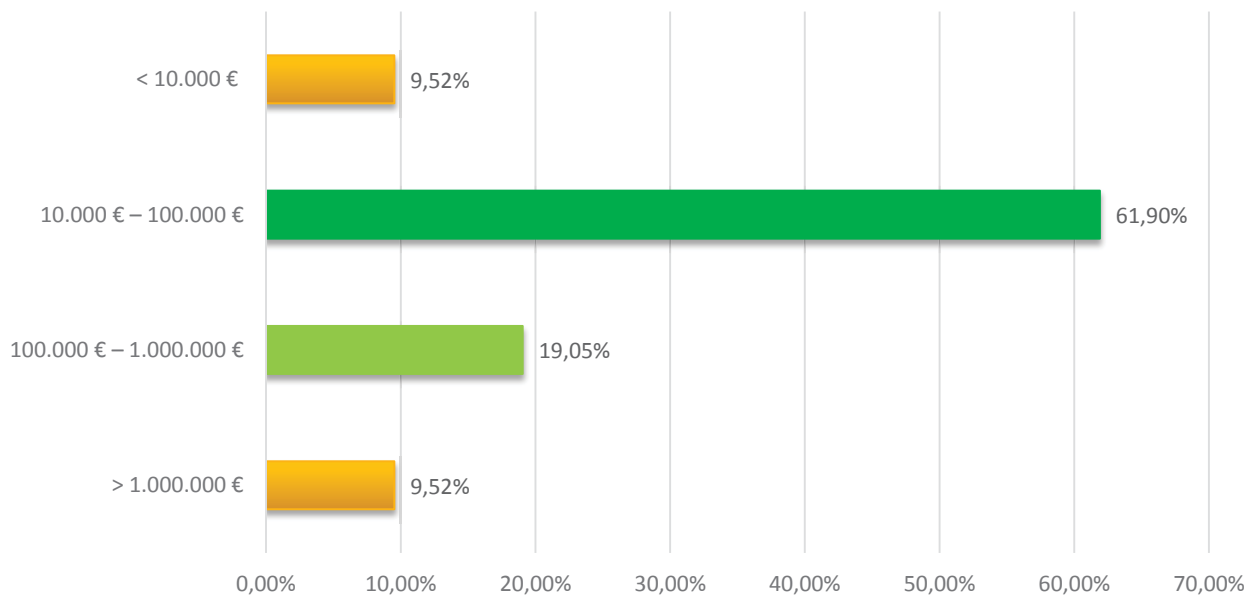




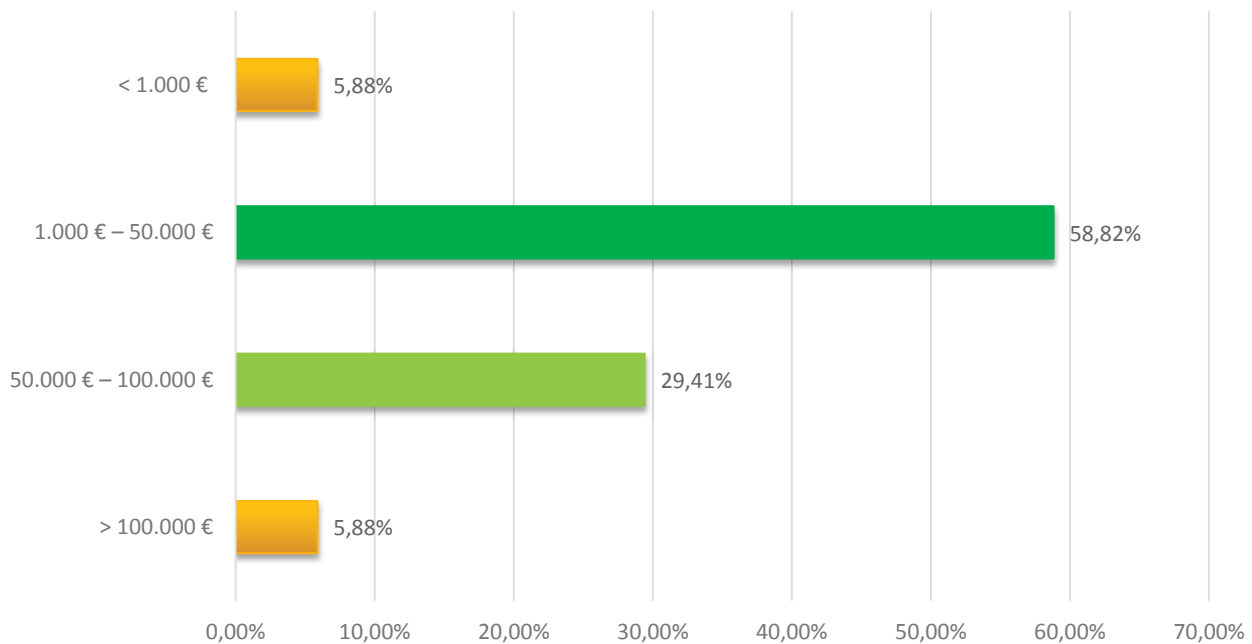
**4. To which extent do you think the quality, reliability and exhaustiveness of information on the security property of ICT products is likely to influence consumer/user choice over other type of factors such as costs?**



**5. On average what is the range of costs for certifying an ICT service/product?**



**6. On average what is the range of costs of labelling of an ICT service/product (excluding any cost related to the certification process)?**



**7. Can you please provide an example you are aware of a security certification requirement a company had to undertake to access the market of an EU country? (Specify at least name of certification, type of ICT product, country) (Include average costs from questions below)**

- "C5" standard is or will be required for public sector procurement of cloud services in Germany (note: C5 compliance is road mapped, but I am not sure if it's been completed yet) EN 301 549 is required for public procurement of ICT products and services ISO 27001 certification provides the basis for our compliance with EU Standard Contractual Clauses under the EU Data Privacy Directive ISO 27001 and 27018 also provide the basis of our compliance with other legal requirements under various privacy laws in the EU, including without limitation NEN 7510:2011 covering health information in the Netherlands and NHS data in the UK. UK G-Cloud is required to sell cloud computing to government customers in the UK.
- Mobile Network Operators require SIM cards to be certified using Common Criteria EAL4+ certification scheme
- ANSSI CSPN in France
- eID card in Germany. Cost are difficult to evaluate as it includes costs of hardware certification and cost of the composite (+/- €500.000).
- French CSPN certification
- Server signing according CEN protection profile
- smart metering, CSPN certification, France
- C-SEC Payment Terminal needed to sell in Germany and UK
- CSPN in France
- Not directly, however I have been assisting several healthcare / medical device manufacturers to implement ISO27001 and GDPR requirements. This has some overlap with the proposed certification
- Security certification requirement is not requested to access the market. Providing of Services (eg trusted services) is required to certify.
- Smart metering Gateway, BSI CC PP EAL 4+ certification
- eIDAS QSCD products

### **7.1 Could you provide an educated estimate of compliance costs and time:**

- Compliance costs are well above \$1M and time is in the 18 months range
- We do not disclose this information publicly.
- For Certification alone it would be 50k€ and 6 months. This does not include R&D costs.
- New common criteria certificates take between 9 and 12 months. For 2 CC certificates for the hardware running in parallel and another one for the composite it takes 1 year ½. It can be faster if hardware is already certified.
- 25k€ and 2 months
- 150000€
- 6 weeks, between 15 to 30 K euros
- 80K and 4 months
- 25 + 10 if crypto
- Very hard, depends entirely on the complexity of the product and the organizational structure.
- Currently only CCEAL4+ is requested as mandatory certification for trusted services. Few months and X0.000€ for smart cards, Many months for HSM and X00.000€ for HSM. Depending on manufacturer experience on Certification.
- 1 Mio / 5 Years
- 60000

### **8. Can you please provide an example you are aware of a security-labelling requirement a company had to comply with in order to access the market of an EU country? (Specify at least name of labelling scheme, type of ICT product, country)**

- See above. Note that most requirements are “soft” – not required by law per se (except for public sector procurement) but a practical reality for customers who want assurances beyond a “trust me” approach by vendors.
- No
- IIF from BSI are German specific.
- No
- Digital Tachograph – Vehicle Unit (PP-0057) & Tachograph Card (PP-0070) & Motion Sensor (PP-0093
- CSPN
- See before, ISO 27001
- NO evidence of labelling requested outside the field of certification
- eIDAS QSCD product certification

### **8.1 Could you provide an educated estimate of compliance costs and time:**

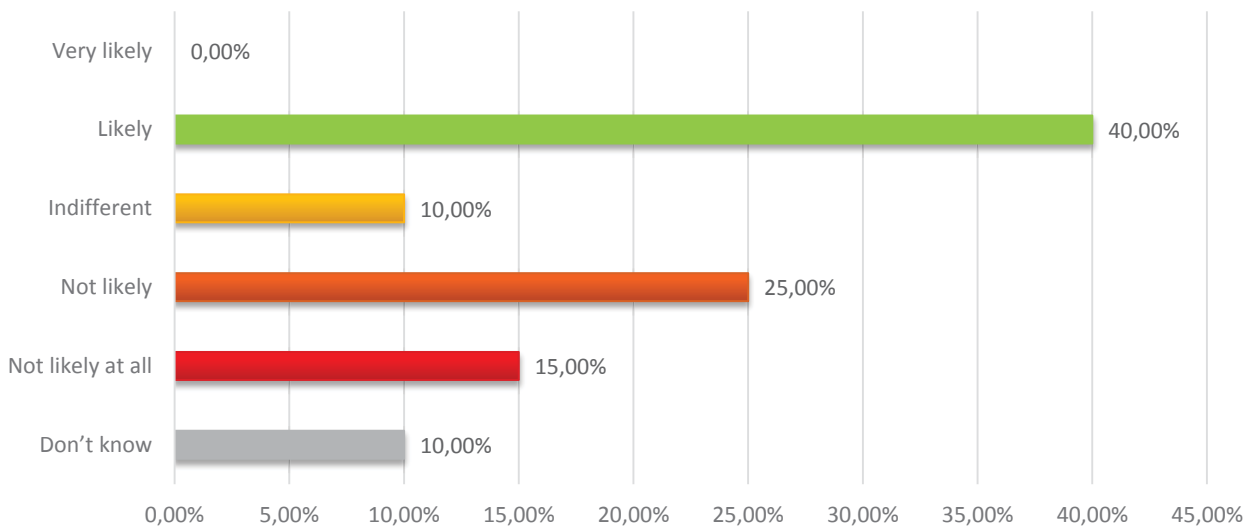
- We do not disclose this information.
- No
- 300000€
- Again, completely product and organization dependant.
- NO
- 60.000 EUR and 3-5 months

### **9. Can you please provide an example you are aware of a case of national procurement bids/practices restricting open competition in favour of mandatory national certifications? (Specify type of ICT product, country, procurement procedures and enforcement e.g. mandatory or recommended)**

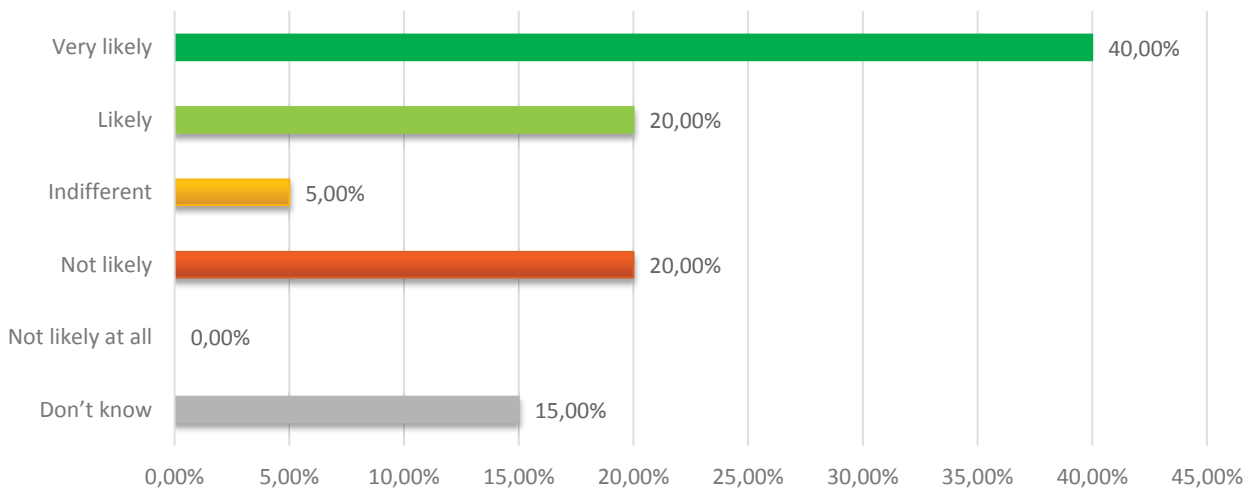
- CSPN in France for Military applications for Electrical Distribution
- No
- Passport, ID card, Driving licence,

- Common Criteria EAL4+, electronic passports
- German ePassports, ID cards, Healthcards, French SIM-cards
- In NL there have been several attempts over time to increase the adoption of open standards in general, not directly security related. All have been quite unsuccessful so far due to resistance from IT departments.
- Surveillance system - Italy - Public procurement - CC Certification
- Smart Metering around Europe / mainly in Germany
- eIDAS product e.g. eID documents and infrastructures. It is mandatory having the eIDAS compliance
- Certification by the Chinese Financial Authentication (CFA) scheme is required to enter the Chinese payment market for card (Secure Element) based payment
- To our knowledge, there is no national procurement practice that restricts open competition in favour of mandatory certification. Instead, most national procurement practices tend to have both open competition and certification requirements.

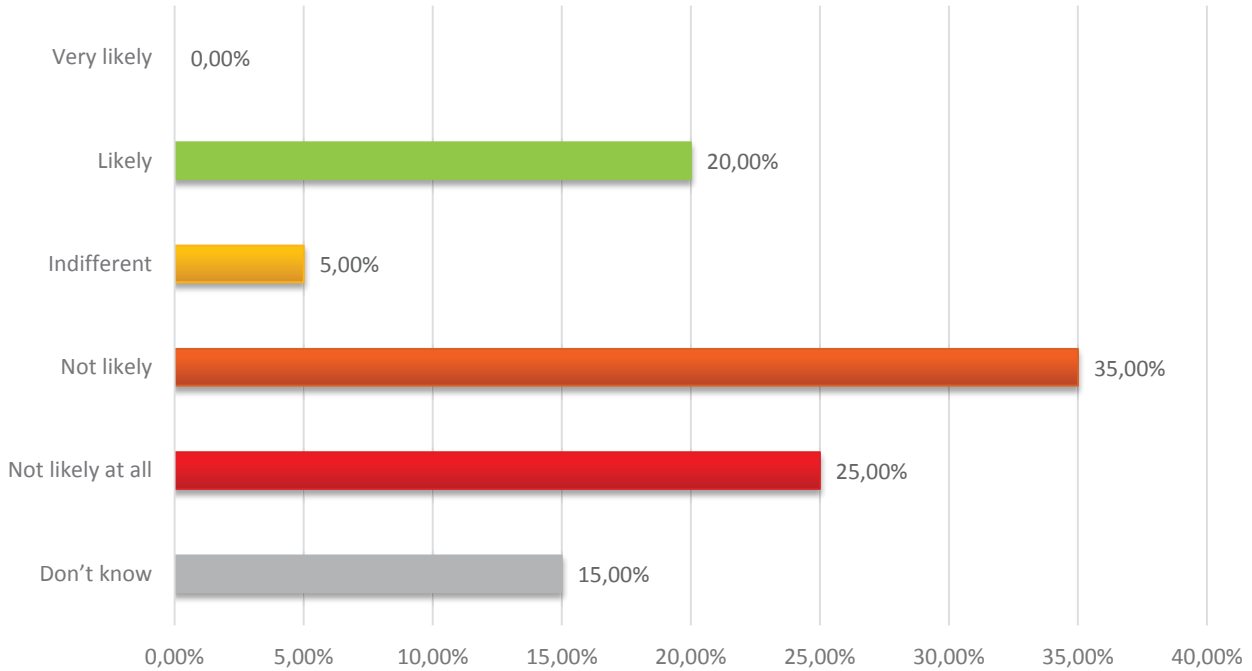
**10. How likely do you think a large-sized company which has certified its product in a given EU country would restrain itself from entering the market of a second MS in consideration of additional security certifications requirements?**



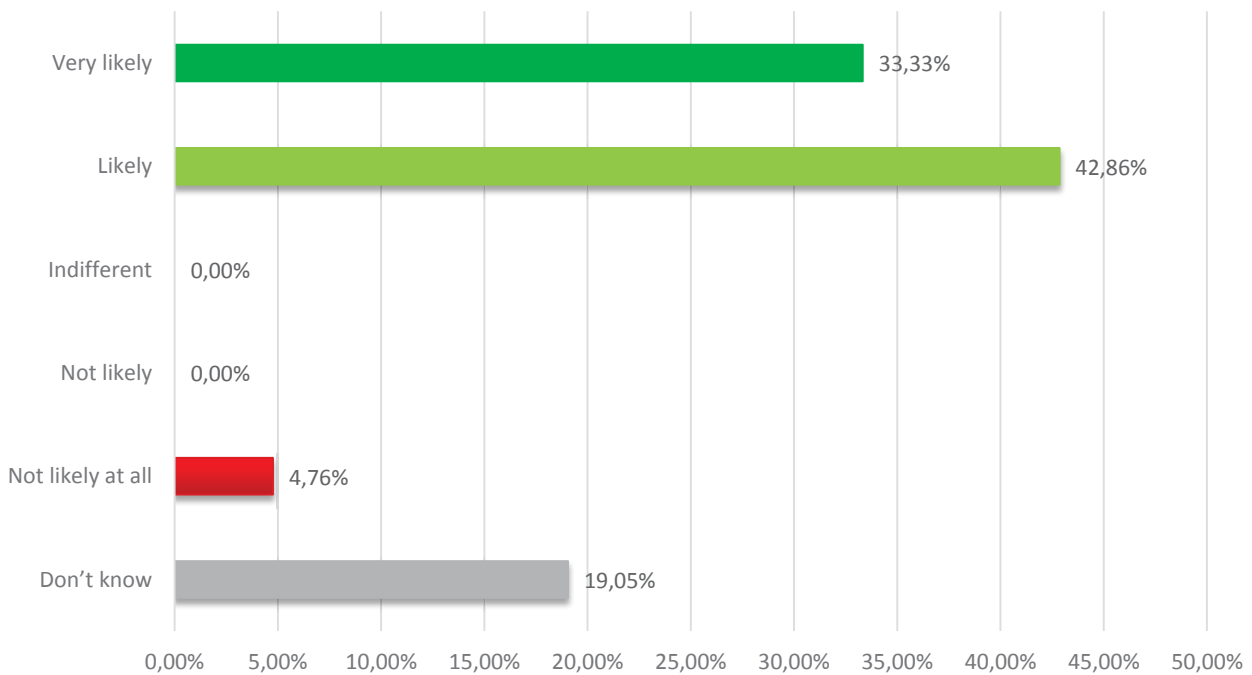
**11. How likely do you think a SME which has certified its product in a given EU country would restrain itself from entering the market of a second Member State in consideration of additional security certifications requirements?**



**12. From your experience, what is the likelihood of an ICT product/service vendor to accept bearing the costs of a second certification/labelling process in order to access the market of another EU country?**



**13. In reference to commercial strategies, do you think a foreign vendor is likely to favour accessing an EU country having in place a mutual recognition agreement (in relation to security certification and labelling) with other EU countries?**



---

**14. In your opinion, in the context of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the management level (e.g. Establish transparent procedures)?**

- Raising awareness, education, etc.
- The EU should ensure that in the context of ICT security certifications that 1) neither the EU nor Member States completely "re-invent the wheel" but instead leverage existing standards and certifications based on international standards. 2) The EU should strive to enable mutual recognition between comparable cybersecurity certifications - again ideally based on existing international standards.
- Governance, co-ordinate mutual recognition
- ENISA could endorse the role of a transversal agency which could be continuously active in identifying and registering expert groups that will be in charge of defining adequate certification levels per sector. ENISA could monitor what is enforced in terms of certification, and could be given a mandate to specific experts groups that would be in charge of defining in details these sectorial certifications.
- establish the same rules for the security certification scheme in the various CS
- ENISA will have a key role
- Coordination of National Security Agencies Technical Referential and procedures
- Identify the products/services, Establish procedures/methodologies, Maintain and harmonize the assurance level and competences (like SOG-IS is doing for Common Criteria evaluations)
- Partner
- Implement laws ensuring support and updates for released devices. And establish clear and transparent implementation procedures.
- define Directives for better integration
- Push for standardisation among member states of such ICT security certifications;
- Third party body as in any other EU Certification Scheme
- Harmonization of security certification requirements (eg security level required) and harmonization of approaches to certification of ICT security features in EU states
- Conformity Assessment Body centrally in order to enhance EU wide competition
- Drive mutual recognition, define procedures and frameworks e.g. Common Criteria

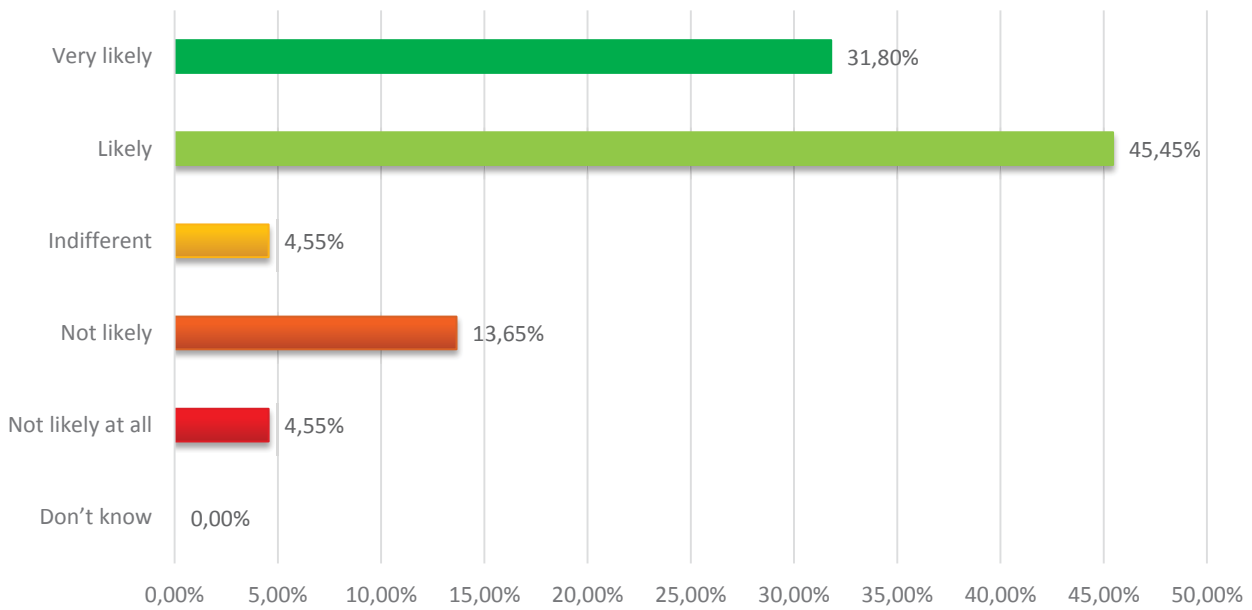
**15. In your opinion, in the context of the creation of a European ICT security certification Framework what role the EU Agencies (such as ENISA) might have at the operational level (e.g. Identifying needs, cooperation, coordination, alerting)?**

- Yes, all of those examples
- ENISA could help ICT vendors in Europe by deepening their mapping of available ICT security standards across the EU as well as other leading certifications (and/or industry led best practices), working to identify commonalities, overlap and opportunities for harmonization. ENISA is currently not set up to play an operational role and/or to advise on the implementation of particular certification frameworks.
- Co-ordination, information sharing
- ENISA could be a registration office for all new applicable certification schemes and standards depending on a specific market segmentation. Given its neutrality and independency, the European Union could be devolved the role of managing a potential labelling scheme for cybersecurity once certification schemes have been put in place.
- guarantee the skills of the different national certification scheme
- ENISA should be involved in CERT for ICT
- Promoting the security evaluation scheme, Providing market analysis, Funding security evaluations when ICT products or services are use by the EU
- Identifying needs through technology watch, ensuring the interoperability of the framework (very important), update the procedures/methodologies, maintain the list of certified products/services

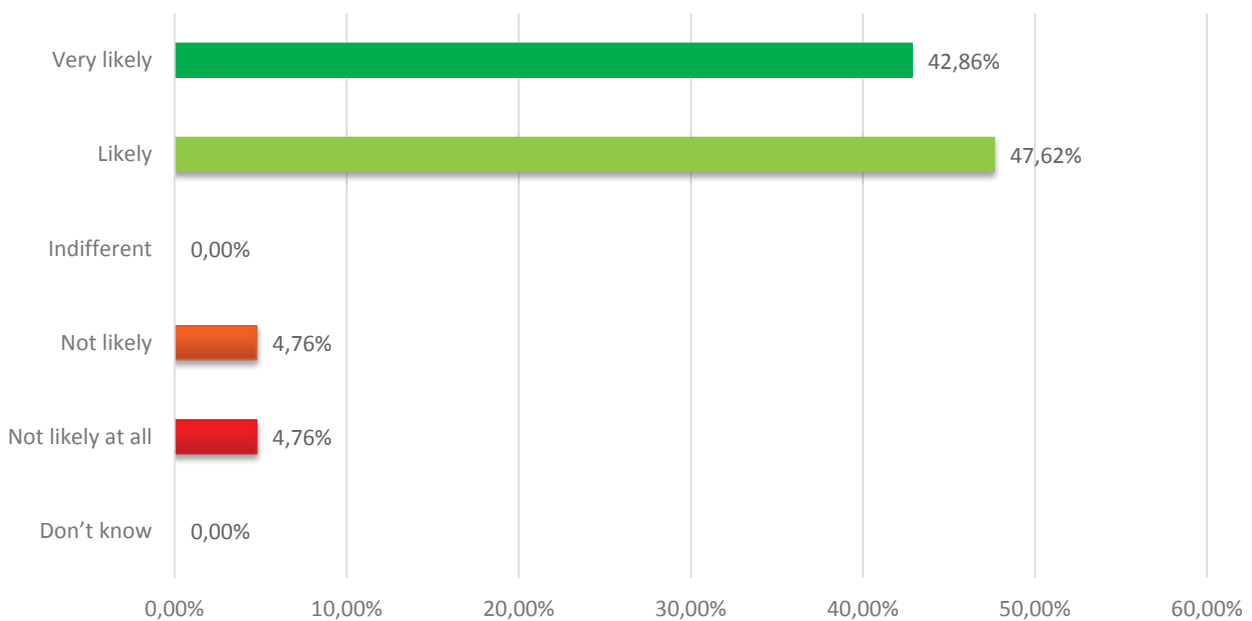
- Coordination
- Verification, audits and validation.
- Analyse the market and the situation in different MS and provide support and/or encourage them to share and reuse best practices.
- Coordinating and Guarantee of fair behavior
- identifying needs, coordination, supervision
- Merge with SOG\_IS and manage EU wide valid PPs for minimum security requirements
- Identifying needs and define and plan focus areas. Drive international cooperation

**16. How likely do you think a European ICT security certification Framework would produce the following benefits?**

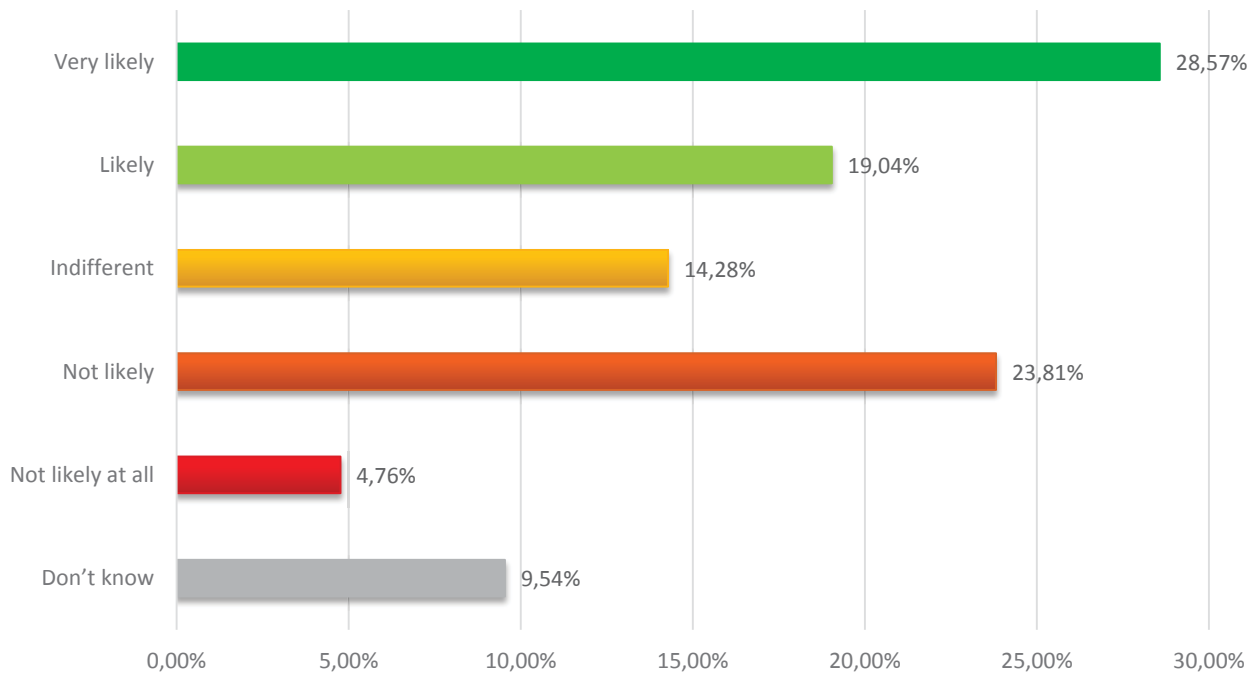
**1) higher consumer trust in the security properties of the product/service**



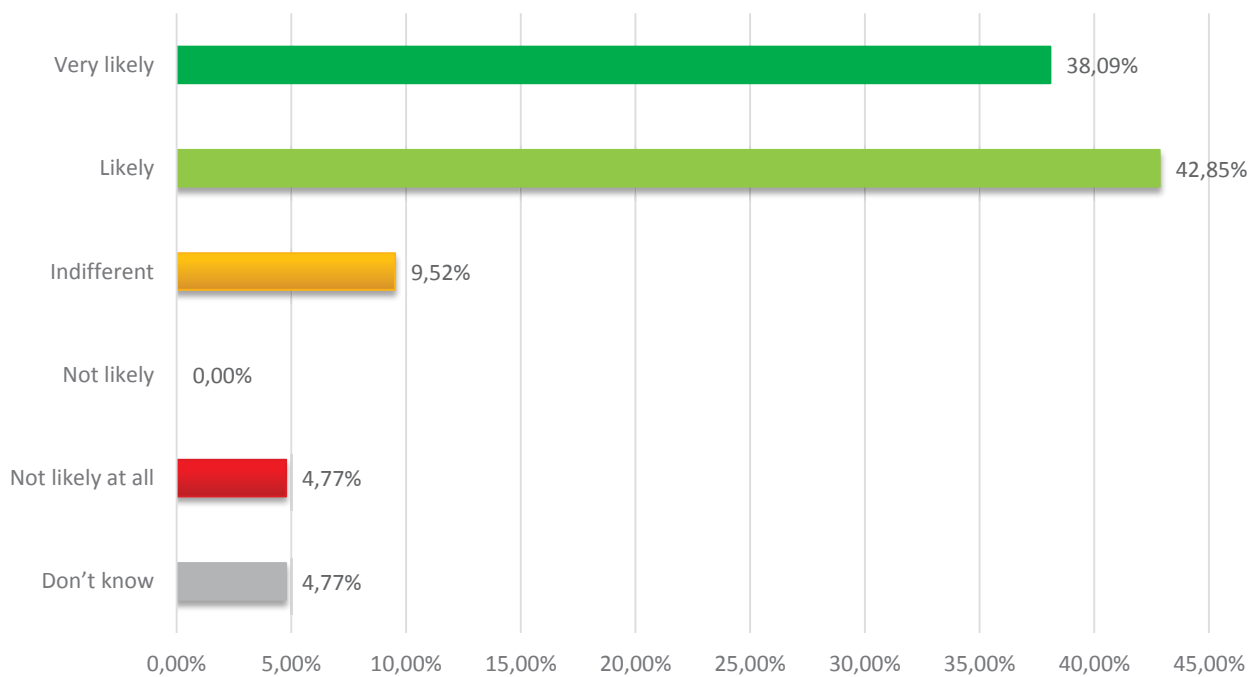
**2) higher number of certified/labelled products/services**



### 3) lower time and cost of certification/labelling



### 4) reduction/elimination of fragmentation (meant as the existence of multiple national and sectorial certification schemes not mutually recognised)





---

## Analysis

The online Questionnaire has been broadly publicised sending email to selected and impacted stakeholders, albeit within the confined certification community, and contacting representatives of impacted organisations during events and workshop. To facilitate the presentation of the results, the survey questions have been grouped across four thematic areas, namely:

- **Consumer Trust & Labelling** comprising of questions 1, 2, 3 and 4
- **Time/Costs for Certifying/Labelling** comprising of questions 5, 6, 7.1, 8.1
- **Fragmentation** comprising of questions 7, 8 9, 10, 11 and 12
- **Policy Options and envisioned features** comprising of questions 13 through to 16

### Consumer Trust & Labelling

In order to increase consumer trust and confidence in ICT products, **50%** of questionnaire participants agreed on the necessity to *adopt a certification and labelling scheme* allowing customers to compare in an informed way which products offer the highest level of security. A smaller percentage, 23,08%, of the respondents indicated the answer "Other" as the best policy/strategy option to follow, providing, for example, the following assertions:

- Hard-law approach translating IT security Requirements in Protection Profiles supporting CC evaluation/certification plus financial incentives to vendors encouraging them to certify their IT products/system and maintain the certifications through time
- A mix of policy/strategy options proposed would be the best strategy to increase consumer trust and confidence
- Industry-led best practices (with government input) on cybersecurity baselines. In addition, financial incentives and government procurement power could play helpful roles.

The majority of the questionnaire respondents think that security labelling of ICT products/services is likely to impact consumers' behaviours despite any price considerations. Indeed, **17,39%** of participants chosen the answer "*Very likely*" and **43,48%** of respondents chosen the answer "*Likely*". Moreover, according to the large majority of respondents, consumer trust is likely to increase when certifications are performed according to security requirements set by third party entities as opposed to security requirements freely chosen by vendors.

### Time/Costs for Certifying/Labelling

61,90% of questionnaire respondents indicated that the cost incurred for certifying an ICT service/product is between 10 thousand euros and 100 thousand euros. A smaller percentage, 19,05% answered that the cost incurred for certifying an ICT service/product are between 100 thousand euros and 1 million euros and only 9,52% of respondents indicated as 1 million or plus the cost incurred for certification. To better understand the answers provided, many examples can be mentioned according to the question 7.1:

- 25 thousand euros and 2 months
- 6 weeks, between 15 to 30 thousand euros
- 80 thousand euros and 4 months
- 1 million euros and 18 months
- 60 thousand euros

Looking at the answer provided by the respondents regarding time and cost of certification, it is necessary to distinguish the product/service that must be certified. In fact, time and cost depend entirely on the complexity of the product/service and the organizational structure. The same reasoning applies also to the costs of labelling. Being labelling a process not yet widely used for ICT products, the questionnaire respondents have not been able to give many examples of labelling time and costs. The only two quantitative answers are:

- 300 thousand euros
- 60 thousand euros and 3-5 months

---

## Fragmentation

The issue of fragmentation is central to the study. Respondents gave many examples of ICT products that companies have to certify in order to access the market of an EU country. For example:

- eID cards in Germany
- Smart-metering devices
- SIM cards
- QSCD products

In many cases, as widely argued within this Interim Report, additional certifications are requested in order to access to other EU countries For example:

- CSPN
- BSI German Scheme

Many example were give for cases of national procurement bids/practices restricting open competition in favour of mandatory national certifications. The respondents gave the following answers:

- CSPN in France for Military applications for Electrical Distribution
- Common Criteria EAL4+ for electronic passports
- German ePassports, ID cards, Healthcards, French SIM-cards
- Surveillance system - Italy - Public procurement - CC Certification
- Smart Metering around Europe / mainly in Germany
- eIDAS product e.g. eID documents and infrastructures. It is mandatory having the eIDAS compliance

**40%** of respondents, giving the answer "*Likely*", think that a large-sized company which has certified its product in a given EU country would restrain itself from entering the market of a second MS in consideration of additional security certifications requirements. The same percentage of respondents gave the answer "*Very Likely*" talking on the same issue for SMEs. Is therefore evident that the greatest difficulties are faced by SMEs that in the vast majority of cases are not able to cope with the costs of a certification. In the end, the majority of respondents, 35%, gave the answer "*Not Likely*" regarding the question asking the likelihood of an ICT product/service vendor to accept bearing the costs of a second certification/labelling process in order to access the market of another EU country.

## Policy Options and envisioned features

A large majority of respondents indicated with the answers "*Very Likely*" and "*Likely*", respectively **33,33%** and **42,86%** of respondents, that a foreign vendor is likely to favour accessing an EU country having in place a mutual recognition agreement with other EU countries.

In the context of a European ICT security Certification Framework, all the respondents answered that the EU Agencies (such as ENISA) would play a key role both at management an operational level.

Very high percentages are observed regarding the benefits that could be produced by a European ICT Security Certification Framework:

- Regarding an increase of consumer trust in the security properties of the product/service, the respondents answered with "*Very Likely*" in the **31,80%** of the answers and with "*Likely*" in the **45,45%** of the answers
- Regarding an increase of certified/labelled products/service, the respondents answered with "*Very Likely*" in the **42,86%** of the answers and with "*Likely*" in the **47,62%** of the answers
- Regarding the reduction/elimination of fragmentation, the respondents answered with "*Very Likely*" in the **38,09%** of the answers and with "*Likely*" in the **42,85%** of the answers
- Regarding a decrease of time and cost of certification/labelling, the respondents answered with "*Very Likely*" in the **28,57%** of the answers and with "*Likely*" in the **19,04%** of the answers

It is clear that the vast majority of respondents believe that an EU ICT Security Certification Framework would produce many benefits, reducing fragmentation and increasing competitiveness of ICT market companies.

## 7.3 Stakeholder Mapping

Working with DG CONNECT it was possible to identify and validate the list of the stakeholders who are directly or indirectly impacted by the project. During the first preliminary meeting, on the 8th of May 2017, has been highlighted by the DG CONNECT Team that surveys have been conducted by **JRC**; this means that a mapping of stakeholders has already been developed. The stakeholders **mapping** has been integrated with the identification of **new selected stakeholder** included in specific and most impacted industrial sectors, taking in consideration the JRC surveys data received and analysed by the Consortium. In particular, as requested by the Commission, the Consortium has contacted especially many representatives from National Certification Authorities, Smart-metering and Semi-conductors industries.

A detailed stakeholder map has been necessary for identifying experts and participants for the **interviews** organized. The Map was constantly updated and improved during the project running.

The Consortium selected the most impacted stakeholders which are mapped below:

Recipient	Brief Description	Classification	Domain
Amossys	Security evaluations	Conformity Assessment Body	SOG-IS, CSPN, CC
Applus Laboratories	EVALUATION LAB	Conformity Assessment Body	SOG-IS, CC
Atsec	Laboratory and consulting services for information security	Conformity Assessment Body	SOG-IS, CC
Atsec	Laboratory and consulting services for information security	Conformity Assessment Body	SOG-IS, CC
BrightSight	Security evaluation specialist	Conformity Assessment Body	SOG-IS
Leti Cea Tech	Player in research, development and innovation	Conformity Assessment Body	SOG-IS, CSPN
INTA	Public Research Agency specialized in Aerospace technological research and development	Conformity Assessment Body	SOG-IS
CGI	Provide end-to-end IT and business process services	Conformity Assessment Body	SOG-IS
COMBITECH	Independent technical consulting company	Conformity Assessment Body	SOG-IS
Consorzio RES	Security Evaluation Laboratory; Evaluation Centre; Global Consultant	Conformity Assessment Body	SOG-IS
Datenschutz		Conformity Assessment Body	SOG-IS
DFKI	German Research Center for Artificial Intelligence	Conformity Assessment Body	SOG-IS
Epoche and Espri	IT security evaluation and testing services	Conformity Assessment Body	SOG-IS
IMQ	Certification Authority and a European leader in conformity assessments and laboratory tests	Conformity Assessment Body	SOG-IS
SELTA	Leading in the design of solutions for network's automation in the field of energy and transport	Conformity Assessment Body	SOG-IS
MTG	Independent consulting and software company	Conformity Assessment Body	SOG-IS
Norconsult	Multidisciplinary consultancy firms in the Nordic re	Conformity Assessment Body	SOG-IS
NTT Security	Consulting services, managed security services and technology solutions	Conformity Assessment Body	SOG-IS
Oppida	Evaluation and consulting services	Conformity Assessment Body	SOG-IS, CSPN

Recipient	Brief Description	Classification	Domain
Riscure	Global security test lab	Conformity Assessment Body	SOG-IS
Secuvera	Security Consulting	Conformity Assessment Body	SOG-IS
Serma-Safety-Security	Security formal evaluation, Security expertize and consulting; Safety expertize and consulting.	Conformity Assessment Body	SOG-IS, CSPN
Sogeti	Technology and Engineering Services	Conformity Assessment Body	SOG-IS, CSPN
Src-Gmbh	Provide service in the areas of information technology and information security	Conformity Assessment Body	SOG-IS
Cclab	Evaluation services	Conformity Assessment Body	SOG-IS
Technisblu	IT consulting	Conformity Assessment Body	SOG-IS
Thalesgroup	Safety and Security Solutions	Conformity Assessment Body	SOG-IS, CSPN
T-Systems	Integrated solutions for the networked future of business and society	Conformity Assessment Body	SOG-IS
Tuvit	IT security	Conformity Assessment Body	SOG-IS
UL	Global leader in safeguarding security, compliance, and global interoperability	Conformity Assessment Body	SOG-IS
Roke	Evaluation LAB	Conformity Assessment Body	CPA
KPMG	Evaluation LAB	Conformity Assessment Body	CPA
Context	Evaluation LAB	Conformity Assessment Body	CPA
Dnv-GI	Evaluation LAB	Conformity Assessment Body	CPA
Info-Assure-Ltd	Evaluation LAB	Conformity Assessment Body	CPA
NCC Group	Evaluation LAB	Conformity Assessment Body	CPA
Siventure	Evaluation LAB	Conformity Assessment Body	CPA
CGI IT UK Ltd	Evaluation LAB	Conformity Assessment Body	CPA
EDSI	Evaluation LAB	Conformity Assessment Body	CSPN
Lexfo	Evaluation LAB	Conformity Assessment Body	CSPN
QuarksLab	Evaluation LAB	Conformity Assessment Body	CSPN
Serma Safety	Evaluation LAB	Conformity Assessment Body	CSPN
Synacktiv	Evaluation LAB	Conformity Assessment Body	CSPN
Trusted Labs	Evaluation LAB	Conformity Assessment Body	CSPN
Blanco	CPA-CC -CSPN fragmentation example		CPA, CC, CSPN
ANNSI	French CB	Conformity assessment and Certification Authorities	

Recipient	Brief Description	Classification	Domain
CCN	Spanish CB	Conformity assessment and Certification Authorities	
BSI	German CB	Conformity assessment and Certification Authorities	
BSI	German CB	Conformity assessment and Certification Authorities	
BSI	German CB	Conformity assessment and Certification Authorities	
NSCS	UK CB	Conformity assessment and Certification Authorities	
FICORA	Finland CB	Conformity assessment and Certification Authorities	
SERTIT	Norwegian CB	Conformity assessment and Certification Authorities	
NLNCSA	Netherlands CB	Conformity assessment and Certification Authorities	
OCSI	Italian CB	Conformity assessment and Certification Authorities	
NASK	Poland CB	Conformity assessment and Certification Authorities	
Bundeskanzleramt	Austria CB	Conformity assessment and Certification Authorities	
FMV	Sweden CB	Conformity assessment and Certification Authorities	
JHAS	Smart card JIL WG	Vendor(Product/Service)	
JEDS	HW devices JIWL WG	Vendor(Product/Service)	
Eurosmart (gemalto)	Smart card Community	Vendor(Product/Service)	
ESMIG	Smart Meters Association	European & International Organizations	Smart-meters
ESMIG	Smart Meters Association	European & International Organizations	Smart-meters
EMVco		End-users	
NXP	Semi conductors Industry	Vendor (Product/Service)	Semi-conductors
Infineon	Semi conductors Industry	Vendor (Product/Service)	Semi-conductors
BEAMA	UK association for T&D europe	Vendor (Product/Service)	Smart-meters
GIMELEC	FR association for T&D europe	Vendor (Product/Service)	Smart-meters
AFBELL	SP association for T&D europe	Vendor (Product/Service)	Smart-meters
ANIMEE	PT association for T&D europe	Vendor (Product/Service)	Smart-meters
ANIE	IT association for T&D europe	Vendor (Product/Service)	Smart-meters
SWISSMEM	CH association for T&D europe	Vendor (Product/Service)	Smart-meters
FEEI	AT association for T&D europe	Vendor (Product/Service)	Smart-meters
ZVEI	GE association for T&D europe	Vendor (Product/Service)	Smart-meters

Recipient	Brief Description	Classification	Domain
AGORIA	BE association for T&D europe	Vendor (Product/Service)	Smart-meters
FEDET	NL association for T&D europe	Vendor (Product/Service)	Smart-meters
EMSAD	TK association for T&D europe	Vendor (Product/Service)	Smart-meters
AEM		Vendor (Product/Service)	Smart-meters
Bitron		Vendor (Product/Service)	Smart-meters
CESI		End-users	Smart-meters
e-distribuzione		End-users	Smart-meters
Prodti	Academics / no profit foundation		Smart-meters
Sagemcom Broadband Sas		End-users	Smart-meters
Schneider electric		Vendor (Product/Service)	Smart-meters
TelecontroSTM		End-users	Smart-meters
Atmel		Vendor (Product/Service)	Smart-meters
Ayesa		Vendor (Product/Service)	Smart-meters
MAC		Vendor (Product/Service)	Smart-meters
landgyr	Smart meter vendor, CPA certified smart meter product	Vendor (Product/Service)	Smart-meters
EDMI Europe	Smart meter vendor, CPA certified smart meter product	Vendor (Product/Service)	Smart-meters
Siemens		Vendor(Product/Service)	Smart-meters
ST Microelectronics	Global Semiconductors company	Vendor(Product/Service)	Semi-conductors
ESIA	Voice of the Semiconductor Industry in Europe	European & International Organizations	Semi-conductors
UEAPME	Voice of SMEs in Europe	European & International Organizations	SMEs
Digital SME Alliance	European association exclusively focused on representing the interests of the SME community in the ICT sector.	European & International Organizations	SMEs
SBS	Represent and defend small SMEs interests in the standardisation process at European and international levels	European & International Organizations	SMEs
ANIE		Vendor (Product/Service)	Semi-conductors
Fraunhofer Group	Service provider for R&D in the areas of microelectronics and smart systems integration	Vendor (Product/Service)	Semi-conductors
GlobalFoundries	leading full-service semiconductor design, development, fabrication and innovation company with locations across the globe.	Vendor (Product/Service)	Semi-conductors
Imec	R&D solutions, innovation services applicable to both products and services	Vendor (Product/Service)	Semi-conductors

Recipient	Brief Description	Classification	Domain
<b>Micron</b>	global leader in the semiconductor industry	Vendor (Product/Service)	Semi-conductors
<b>TDK</b>	Semiconductor Solutions for Automotive and Industrial Electronics	Vendor (Product/Service)	Semi-conductors
<b>Nanium</b>	Advanced assembly and test services to a global customer base of semiconductor companies	Vendor (Product/Service)	Semi-conductors
<b>Rhom</b>	Semiconductor Corporate	Vendor (Product/Service)	Semi-conductors
<b>FAB</b>	The world's largest analog/mixed-signal foundry group	Vendor (Product/Service)	Semi-conductors
<b>Texas Instruments</b>	Global semiconductor company operating in 35 countries	Vendor (Product/Service)	Semi-conductors
<b>Nuki</b>	Turn smartphone into smart keys	Vendor (Product/Service)	Smart-Lock Door
<b>August</b>	Design products and services that let everyday people monitor and manage entry into their homes from wherever they are	Vendor (Product/Service)	Smart-Lock Door
<b>Igloohome</b>	Makes homes and properties smarter	Vendor (Product/Service)	Smart-Lock Door
<b>Mul-T-Lock</b>	High Security Locking and access control solution	Vendor (Product/Service)	Smart-Lock Door
<b>Friday</b>	The world's smallest smartlock	Vendor (Product/Service)	Smart-Lock Door
<b>SmartLOCK</b>	market leader in connected access solutions	Vendor (Product/Service)	Smart-Lock Door
<b>DanaLock</b>	Danish smart-lock company	Vendor (Product/Service)	Smart-Lock Door
<b>Clay</b>	Wireless, cloud-based smart lock technology company	Vendor (Product/Service)	Smart-Lock Door
<b>Smart Video &amp; Sensing Limited</b>	Value Added Reseller (VAR) of optical based survey solutions, Video Incident detection systems / Video Analytics and high end digital CCTV	Vendor (Product/Service)	Smart-CCTV
<b>Smartvue</b>	IoT video solutions	Vendor (Product/Service)	Smart-CCTV
<b>Swann</b>	Global leader in security monitoring, consumer electronics and security-centric solutions for the smart homes and businesses of today and tomorrow	Vendor (Product/Service)	Smart-CCTV
<b>Graz University, Austria</b>		Other	Semi-conductors
<b>STMicroelectronics</b>		Vendor (Product/Service)	Semi-conductors
<b>Infineon Technologies</b>		Vendor (Product/Service)	Semi-conductors
<b>Infineon Technologies</b>		Vendor (Product/Service)	Semi-conductors
<b>Infineon Technologies</b>		Vendor (Product/Service)	Semi-conductors
<b>Leonardo</b>		Vendor (Product/Service)	Semi-conductors
<b>Radboud University, The Netherlands</b>		Other	Semi-conductors
<b>ENS, France</b>		Other	Semi-conductors

Recipient	Brief Description	Classification	Domain
Eurosmart	Is an international association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications	European & International Organizations	Smart Security Industry
Eurosmart	Is an international association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications	European & International Organizations	Smart Security Industry
Eurosmart	Is an international association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications	European & International Organizations	Smart Security Industry
ST Microelectronics	Global semiconductor company	Vendor (Product/Service)	Semi-conductors
ST Microelectronics	Global semiconductor company	Vendor (Product/Service)	Semi-conductors

### Critical Infrastructures

Recipient	Brief Description	Classification	Domain
World Energy Council	Network of Energy stakeholders	Operator	Energy
ServiTecno	Software and lot for companies	Producer	Energy, Healthcare
STE S.p.a	Innovation and & Communication Technology	Operator	Energy
RSE Spa, T&D Technologies Dpt	Ricerca Sul Sistema Energetico	Operator	Energy
AIIC	Associazione Italiana esperti Infrattutture Critiche	Operator	Energy, Healthcare, Transport, Finance
Marsh	Insurance Broking, cybersecurity services for transports	Operator	Transportation
Avantune	startup, cloud services, Member of the AIIC	Producer	Finance
Digital Europe	Services for Digital transformation in the fields of finance and Healthcare	Producer	Fianance, Healthcare
Data Security Solutions	Data security solutions, including for the Healthcare system, based in Riga, Latvia	Producer	Healthcare
CER (Community of European Railway and Infrastructure Companies)	CER represent the interests of its members on the EU policy-making scene, in particular to support an improved business and regulatory environment for European railway operators and railway infrastructure companies.	Operator	Transport
Taxify.eu	ridesharing app in Europe & Africa - Estonia	Operator	Transportation
NewBanking	Based in Denmark. Services for Financial digital security and blockchains. NewBanking (www.newbanking.com) delivers verified money - KYC with payments - as a service to enterprise customers	Producer	Finance
ESI Group	The ESI Group specialise in Material Physics and are innovators in Virtual Prototyping addressing the need for products and processes which are both smart and autonomous, thus supporting industry in digital transformation	Operator	Energy
Kraft CERT	Cybersecurity for the National Energy Sector in Norway	Producer	Energy
Ansaldo Energia S.p.A.	leading international player in the power generation industry,	Producer	Energy
SOFTECO	IT Solutions for business development, Transport, Finance,	Producer	Transportation,



Recipient	Brief Description	Classification	Domain
	Energy		Finance, Energy
<b>Newron Pharmaceuticals</b>	Leader in the development of innovative therapies for Central Nervous System (CNS)	Producer	Healthcare
<b>Bayer AG</b>	Major Pharmaceutical company in Europe	Producer	Healthcare
<b>Philips</b>	A leading health technology	Producer	Healthcare
<b>Air France KLM</b>	France's major airline	Operator	Transportation
<b>Easyjet</b>	Europe's leading airline	Operator	Transportation
<b>FERROVIE DELLO STATO ITALIANE S.p.A.</b>	Italy's railway company	Operator	Transportation
<b>SNCF</b>	France's railway company	Operator	Transportation
<b>Deutsche Bahn AG</b>	Germany's railway company	Operator	Transportation
<b>F. Hoffmann-La Roche Ltd</b>	A global pioneer in pharmaceuticals and diagnostics	Producer	Healthcare
<b>Finance Norway</b>	Financial services in Norway	Operator	Finance
<b>ING Group</b>	Financial products and services	Producer	Finance
<b>AXA</b>	Pan European and global Insurance player headquartered in France. AXA strives for an integrated single market in the Insurance sector.	Operator	Finance
<b>Assicurazioni Generali S.p.A</b>	Leading insurance company in Italy	Operator	Finance
<b>Société Générale</b>	French Bank	Operator	Finance
<b>HSBC Holdings PLC</b>	HSBC is one of the world's largest banking and financial services organisations	Operator	Finance
<b>Aviva Plc</b>	UK's largest insurer with strong businesses in selected European markets	Operator	Finance
<b>Shire</b>	Leading global biotechnology company	Producer	Healthcare
<b>Sanofi</b>	Global healthcare leader	Producer	Healthcare
<b>AstraZeneca</b>	Global research-based biopharmaceutical company headquartered in the UK.	Operator	Healthcare
<b>Alitalia</b>	Italian airline	Operator	Transportation
<b>Meridiana fly S.p.A.</b>	Italian airline	Operator	Transportation
<b>Tap Portugal</b>	Portuguese Airline	Operator	Transportation
<b>GlaxoSmithKline</b>	Global healthcare company, based in UK	Operator	Healthcare
<b>Crédit Agricole S.A.</b>	Bank and Insurance	Operator	Finance
<b>BNP Paribas Personal Finance</b>	Bank and Insurance	Operator	Finance
<b>UK Finance</b>	UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK.	Operator	Finance
<b>Nederlandse Waterschapsbank</b>	Nederlandse Waterschapsbank N.V. (NWB Bank) is a leading financial services provider for the public sector.	Operator	Finance
<b>PPRO Financial Ltd</b>	PPRO Group is a cross-border e-payment specialist removing the complexity of international e-commerce payments by acquiring, collecting and processing an extensive range of alternative payments methods for PSPs under one contract, through one platform and one single integration.	Producer	Finance
<b>CLECAT - European association for forwarding, transport, logistic</b>	CLECAT was established in 1958 in Antwerp, it is now located in Brussels and it represents the interests of 24 members (consisting of national organisations of EU freight related service providers, as well as various observer and	Operator	Transportation

Recipient	Brief Description	Classification	Domain
and Customs services	associate members).		
Virtu Financial Ireland Limited	Virtu Financial Ireland Limited is a wholly owned subsidiary of Virtu Financial, Inc. and is a market-leading liquidity provider in European markets with a focus on equities, exchange traded funds and exchange traded derivatives.	Operator	Finance
Morgan Stanley	Morgan Stanley (NYSE: MS) is a leading global financial services firm providing investment banking, securities, wealth management and investment management services.	Operator	Finance
FEXCO Merchant Services Unlimited Company	Provider of Innovative Fintech, Payments & Business Solutions for merchants, acquirers and other businesses	Operator	Finance
Kreditech Holding SSL GmbH	Improving financial freedom for the underbanked by the use of technology.	Operator	Finance
Groupe GTI	Financial operations, with a focus in the field of structured finance and asset securitization.	Producer	Finance
Febelfin	Febelfin vzw/asbl (non-profit association) is the Belgian Financial Sector Federation. It tries to reconcile the interests of its members with those of the policy makers, supervisors, trade associations and pressure groups at the national and European level.	Operator	Finance
Fintech France	Promoting French Fintech Abroad	Producer	Finance
UIRR, International Union for Road-Rail Combined Transport	The International Union for Road-Rail Combined Transport (UIRR) represents European road-rail Combined Transport operators, as well as Transshipment Terminal Managers, who organise this ecologically and economically sustainable system of freight transport.	Operator	Transportation
UITP - International Association of Public Transport	UITP covers all modes of public transport - bus and other road collective transport, rail including tramway, metro, light rail, regional and suburban railways, and waterborne transport. It represents collective transport in a broader sense.	Operator	Transportation
Olivetti	Olivetti S.p.A. is an Italian manufacturer of typewriters, computers, tablets, smartphones, printers, etc. Today it is also specialized in Cloud Computing, ICT and much more	Producer	Energy
Cisco	American multinational technology conglomerate, specialised into specific tech markets	Producer	Energy
ING Group	Dutch multinational banking and financial services corporation headquartered in Amsterdam. Its primary businesses are retail banking, direct banking, commercial banking, investment banking, asset management, and insurance services.	Operator	Finance
Addison Lee	London-based private hire company	Operator	Transportation
Allianz	German financial services company headquartered in Munich, Germany. Its core businesses are insurance and asset management	Operator	Finance
Banco Santander	Spanish banking group	Operator	Finance
HSBC	British] multinational banking and financial services holding company	Operator	Finance
Orange	French multinational telecommunications corporation	Operator	Telecommunications
Vodafone	Multinational telecommunications company	Operator	Telecommunications
Telefonica	Spanish multinational broadband and telecommunications provider	Operator	Telecommunications

Recipient	Brief Description	Classification	Domain
Ryanair	Irish low-cost airline	Operator	Transportation
CIPRE	Critical Infrastructure protection & resilience europe	Expert	Energy
FCA	Financial regulatory body in the United Kingdom	Operator	Finance
Payments UK	300 firms in the UK providing credit, banking, markets and payment-related services	Operator	Finance
London Digital Security Centre (LDSC)	ActionFraud is the UK's national fraud and cyber crime reporting centre	Operator	Finance
Belgian Cybersecurity Coalition	The Cyber Security Coalition brings together the academic world, the public authorities and the private sector in Belgium to fight against cybercrime.	Operator	Telecommunications, Security
CISQ	The Consortium for IT Software Quality (CISQ) is an IT industry group comprising IT executives from the Global 2000, systems integrators, outsourced service providers, and software technology vendors committed to making improvements in the quality of IT application software	Operator	IT, Certification
Deutsche Bahn (DB)	German railway company	Operator	Transport
ATOS R&I (ARI)	Global leader in digital transformation with approximately 100000 employees in 72 countries and annual revenue of around € 12 billion.	Operator	Security
NATO ENERGY SECURITY CENTRE OF EXCELLENCE	Energy security research center of NATO	Expert	Energy
Royal Holloway University of London	University of London with an Information Security Group	Expert	Energy
University of Twente	University of Twente, with a Cyber Security and Safety Group	Expert	Energy
Universität der Bundeswehr München & Cyber Security Research Lab of Airbus	Cyber Security Laboratories	Expert	Energy
Fire Eye	Cybersecurity company that provides products and services to protect against advanced cyber threats,	Producer	Finance
RSE (ricerca sistema energetico)	Research company in the energy field	Expert	Finance, Security
Certiquality	Italian certification body	Expert	IT, Certification
University of Malaga, Spain	University of Malaga	Expert	Energy
Acris GmbH	Manufacturer of Healthcare products and technologies	Producer	Health Care
European Cyber Security Organisation (ECISO) ASBL	ECISO represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP).	Operator	IT, Security
EOS' Civil Aviation Security Working Group Chair	EOS Security Screening and Detection Technologies Working Group	Operator	Transport
EOS Urban security project	EOS' Working Groups seek the establishment of a meaningful public-private dialogue to further their domains' objectives in partnerships where user demands are met by feasible security solutions and services for the protection of Europe and its citizens'	Operator	Transport
Smiths Detection	Industry expert manufacturer of security detection devices	Producer	Transport

Recipient	Brief Description	Classification	Domain
<b>SC SAFETECH INNOVATIONS SRL</b>	Cyber security solutions, including infrastructures	Operator	Finance
<b>Easy Smart Grid GmbH</b>	Developing an innovative smart grid solution	Producer	Energy
<b>European Electronic Component Manufacturers Association</b>	Under the EECA's umbrella organization, there are 2 autonomous industry associations with members coming from the manufacturing and related industries as well as from national associations	Producer	Energy
<b>European Passive Components Industry Association</b>	Represent and promote the common interests of the Passive Components Manufacturers active in Europe to ensure an open and transparent market for Passive Components in Europe as part of the global market place	Producer	Energy
<b>Oracle Utilities</b>	Solutions for Global Utility companies, including the Energy Sector	Producer	Energy
<b>Vattenfall</b>	Swedish power company	Operator	Energy
<b>EVB Energy Solutions</b>	German Energy company	Operator	Energy
<b>Alliander</b>	Energy network company	Operator	Energy
<b>Echelon</b>	IoT Company, specialized in Smart Cities	Operator	Energy
<b>Ferranti Computer Systems</b>	Ferranti Computer Systems helps organizations improve their business through smart implementation, also in the energy field	Operator and Producer	Energy
<b>Seas-NVE</b>	Danish power company	Operator	Energy
<b>Fondazione Politecnico di Milano</b>	Developpement research Center	Expert	Energy
<b>Tuv Rheinland</b>	German businesses that provide inspection and product certification services	Expert	IT Certification
<b>Gruppo Acea</b>	Multi-Utility Company for development in the field of energy	Operator	Energy
<b>TeleTrusT</b>	Widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives	Operator	Telecommunications
<b>Rohde &amp; Schwarz Cybersecurity</b>	Award-winning IT security solutions	Producer	Telecommunications
<b>TÜVIT</b>	IT tester	Expert	IT Security
<b>Atsec information security GmbH</b>	Independent, privately-owned company that focuses on providing laboratory and consulting services for information security	Operator	IT Security
<b>CenterTools Software SE</b>	IT Secure Solutions	Producer	IT Security
<b>Detack GmbH</b>	Independent supplier of quality IT security auditing and consulting services	Expert	IT Security
<b>eco - Association of the Internet Industry e.V</b>	Largest Internet industry association in Europe	Producer	IT Security
<b>itWatch GmbH</b>	Leading provider of secure device management	Producer	IT Security
<b>NCP engineering GmbH</b>	IT Security Solutions for Fintech	Producer	Finance
<b>secunet Security Networks AG</b>	Leading German providers of high-quality IT security.	Producer	Healthcare
<b>RHEA Group</b>	Highly specialized engineering international group of	Producer	Finance, Cloud

Recipient	Brief Description	Classification	Domain
	companies providing products		
<b>World Security Report</b>	Research Center and Publications	Expert	Transport
<b>Dreger Group GmbH</b>	Consulting Company for Fintech	Expert	Finance
<b>Friedrich-Alexander-University</b>	Research Center and Publications	Expert	Finance
<b>Seconda Università di Napoli</b>	Research Center and Publications	Expert	Finance
<b>Academia General Militar</b>	Research Center and Publications	Expert	Energy
<b>AVL List GmbH</b>	Austrian-based automotive consulting firm as well as an independent research institute	Operator	Transport
<b>IMDEA Software Institute</b>	Madrid Institute for Advanced Studies in Software Development Technologies	Expert	Finance
<b>ONRIX gcv</b>	Company networked with various other consultants and professionals, each with specific core competences and capabilities	Operator	Finance
<b>BNY Mellon Investment Management</b>	Privately owned investment manager. The firm provides sub-advisory services to its client	Operator	Finance
<b>Bit4id</b>	IT Security Provider	Producer	Finance
<b>Security Affairs</b>	Major European Journal on IT Security	Expert	Finance

---

## 7.4 An overview of criticism related to Common Criteria

The Common Criteria evaluation and certification is one of the most commonly used process to improve the trust in the security of evaluated products. Nevertheless, this methodology has a lot of problems and side effects that lead to limitations of which the enduser should be aware<sup>16</sup>.

For the manufacturer, the main goal of security evaluation is to obtain a degree (such as CC certificate) which validates the security level of his product. Despite the CC certification gives many advantages to the manufacturers, on the other side CC presents various limits.

### Limit in perimeter

One very famous limit of the common criteria is that an initiator can voluntarily restrict the scope of the Target Of Evaluation (TOE) in order to exclude some part of the IT product that would be subjected to some flaws. Indeed, the initiator very often starts the security evaluation of the overall IT product and in the same time that the security evaluation is conducted, some flaws are found and he reduces the scope of the TOE. It is thus of the responsibility of the customer to verify the scope that the certificate covers. Two other limits of the common criteria are still focused on the scope of the TOE. First limit, the scope of the TOE is very static after the issuance of the certificate and each change in the scope of the product implies to evaluate again the product. To cope with this problem, a process of maintenance has been set up to follow each modification in an IT product. Second limit, even if the product is a software platform able to support several applications (like Java Card could be) and that this platform is certified, it is not allowed to make the composition of it with a new application that could have been already certified. However in the fictive example aforementioned both the platform (more precisely its scope) and the application (its scope too) have been certified. Since it is allowed to do such composition, the national body forbids evaluating an application alone independently of the platform on which it will run. We can summarize this problem as a lack of dynamicity of the scope and even if the common criteria security evaluation. It is a pity since it will be helpful to reduce the overall cost and time of the security evaluation. It would be nice to reach the time to market needs. This limit regarding the short lifecycle of the certificate is very close of the static aspect of the scope of the TOE. Indeed, the certificate is only valid at the time of its issuance. This short delay is explained by the possibility that new attacks could have been discovered just at the time of the issuance or just after.

### Integrating flaws or new attacks

Even if the product could be finally not sensitive to theses new attacks, with a fixed context, some new attacks haven't taken into account in the product conception. To limit this delay, the conception and the evaluation must be scheduled in parallel way. But with this method, flaws must be corrected in time and all depending process must be re-evaluated. Moreover during this additive delay for evaluation, the market requirements can change. A new component can appear with more capacities, more security and with a lower price. Hence the delay between the product conception and the sale must be as short as possible.

### Product distribution

When a product is certified, it is deployed on the market. However an analysis of what happens starting to the deployment time shows that any element enabling to ensure traceability and thus to maintain the chain of trust, have been set up. In the following, the problems can be raised and will be illustrated using as example the smart card products. The company considered here could be a bank, a mobile operator, in short a large company which has an important need of smart cards. In general this company will be directly provided by the chosen manufacturer and not by the retailers. Moreover this major company is very often the initiator of the evaluation (or at least the privileged target of the manufacturer for which it has funded itself the evaluation). At the time of the products reception phase, several types of problems can exist or even to coexist:

- problems due to a negligence: there is an error in the batches or in the production line and the company does not receive the good cards. Normally the procedures of delivery defined by the CC (ADO/DEL) and of audit of the production sites make it possible to be sure that such a trouble is not possible (in theory).
- problems due to an ill will of economical type: to save money the manufacturer has used more powerful (hardware/software) components during the evaluation and lost-cost and less powerful

---

<sup>16</sup> Dusart Pierre, Sauveron Damien, Tai-Hoon Kim, Some limits of Common Criteria certification, *International Journal of Security and Its Applications*

components in production. Once again the procedures of delivery and audit make it possible to counter this trouble (in theory).

- problem due to an ill will of mischievous type: for example, modification by the manufacturer of a batch of cards for specific reasons (desire to mischief, backdoor to keep the possibility to correct possible security problems later). As for the previous case, there cannot theoretically occur.
- distribution problem: according to procedures of delivery defined by the CC, the company receives from the manufacturer the good ordered cards (same model that that evaluated) and it is perfect.

At end-user level, the same problem appears. How can he be sure that the proposed product is secure? It seems important since for example, in the case of the banking world, its own money depends on the card security. He should trust his service supplier whereas this one is perhaps not able itself to have a full trust in its product. Clearly the limits of trust in CC certification are related to the absence of proof attached to the product.

### **Conformity of penetration tests.**

To verify the security of the product, some tests are achieved in the Vulnerability analysis part. Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: the completeness of the security functions, the dependencies between all security requirements and whether any of the security requirements can be undermined through unexpected behavior of the system. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the system. The number and the complexity of these tests depend on the assurance level indicated in the main document (Security Target document). One must verify that the security functions are efficient through these tests. Some attack paths use different kind of attack and knowledge. But the execution of these tests is made in different ways by the ITSEF Centers. There is no homologated set of attack but what the evaluator wants to do or what he can do. The effective level of the vulnerability tests depend on the center quality and knowledge. Hence a same product can be evaluated as good by one center and as bad by another center. However these differences are limited by the certification authority which asks for complementary tests if doubts on security level appear. This choice of management facilitates the mind of initiative to create / to invent new tests. If the list of attacks was fixed as for tests of validity, it would not correspond to the reality of the real world.

### **Problems of interpretation**

The problems of interpretation are split in two sorts:

- difficulties in the intrinsic comprehension of the criteria: it is exactly the same thing that the laws (a paper can understand differently according to the situation, the use, the past abuses, etc.): it is necessary to legislate. An international committee exists to limit this kind of difficulty (<http://www.commoncriteriaportal.org/interpretations.html>)
- difficulties in terms of translation in the language of the country. The used terms do not necessarily exist and can be understood or felt in a different way. (Ex: the term "freedom" will not be understood / felt in the same way into different countries)

Moreover, as shown in the study "Analyzing Common Criteria Shortcomings to Improve its Efficacy", in the view of industry-related security researchers and various stakeholders identifies some main problems of CC. The most common problems identified within the study are:

- The whole process of the evaluation is costly to fulfil the CC requirements in a sense of expenditure, time and production.
- The EALs (i.e. 5, 6, and 7) are known as the higher assurance level for US and European member's countries who signed the MRA agreement, which is a challenge for new member's countries.
- Outsized IT systems evaluation is very complex because evaluation zoom-in to the system components and evaluate each unit. After the evaluation zoom-out and viewing the system as a whole, the task is very much complex and sometime impossible to recombine<sup>17</sup>.

<sup>17</sup> Hunstad, A.; Hallberg, J.; Andersson, R., "Measuring IT security - a method based on common criteria's security functional requirements," Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, pp. 226-233, 10-11 June 2004, URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1437821&isnumber=30958>

- 
- The attempt and time required placing evaluation confirmation and certification is very hard job that by the time the work is finished, the artefact in evaluation is usually outdated.
  - From industry point of view there is some input but have slight impact on the CC assessment.
  - From the evaluation point of view CC is just paperwork the actual product is not properly evaluated. However, this point is for the lower level of EALs not for the higher level.
  - CC discriminates against Free and Open Source Software because these are not dependent on any type of criteria for evaluation.
  - Quick raise in extent, strength, rigor for TOE at high EALs, but not for PP, produce a generalization hole that is costly to overpass.

Another study entitled "*Common Criteria: Its Limitations and Advice on Improvement*"<sup>18</sup> confirms the shortcomings and limitations of CC shown above. In fact, some issues are related to evaluation process. Especially, CC is criticized as being costly and time consuming. Meanwhile, there are issues in general evaluation methodology. Particularly, its limitation on vulnerability analysis is eminent: CC is not good at addressing security flaws in product implementation. The methodology of vulnerability assessment in CC is too generic, not rigorous to identify vulnerability in implementation, and does not take into account vulnerabilities specific to individual technology area.

As exposed within the article "*Symantec: Common Criteria is bad for you*", vendors have to pay hundreds of thousands of dollars to get their products evaluated, and the evaluations ' which are conducted by third-party testing firms ' can take up to a year.

As a result, agencies may have to install older, already-obsolete versions of software in order to comply with NSTISSP. With security products in particular, this is a dangerous practice, as updates are frequently added to these products in order to address recent vulnerabilities,

As a result, by the time most companies can assemble adequate information for a Security Target, they are already halfway through the development cycle.

After many years of development, there are still many limitations in Common Criteria. It shall have to continuously improve to be relevant to current development of security assurance. Adoption of security practices into the development life cycle (e.g., threat and risk analysis, misuse and abuse case generation, analysis of implementation representation to detect any implementation defects, risk-based security testing, vulnerability analysis, and penetration testing, etc.) can not only improve the security assurance but also facilitate the evaluation process. All in all, the goal of improving the security assurance cannot be achieved only through the third-party evaluation and certification; it needs the developer to reasonably retrofit and introduce good security practices into its product development life cycle.

---

18

[http://www.difesa.it/SMD\\_/Staff/Reparti/II/CeVa/Pubblicazioni/Estere/Documents/CommonCriteria\\_ISSA%20Journal\\_0411.pdf](http://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pubblicazioni/Estere/Documents/CommonCriteria_ISSA%20Journal_0411.pdf)

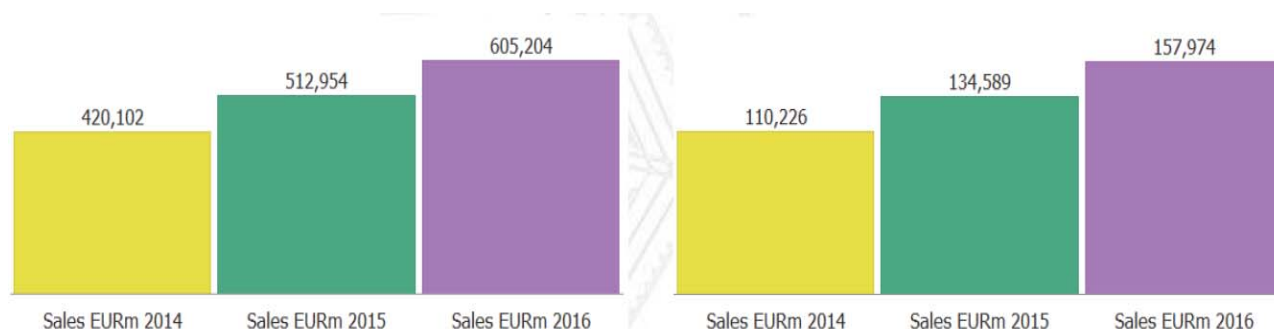


## 7.5 Cyber Security market Insights

The European Commission has mandated PwC and LSEC for a Cyber Security Market Study that should be completed within 2017. On the 6<sup>th</sup> June 2017 in Brussels, European Cyber Security Organisation (ECSO) with PwC and LSEC have organised a “Fact Finding Workshop” in order to share the first preliminary results of the study “Cyber Security Industry Market Analysis (CIMA)”<sup>19</sup>.

The purpose of the study is to assess how cybersecurity challenges can become an EU competitive advantage and propose a European industrial cybersecurity roadmap. In addition, it should also investigate how the cybersecurity industrial tissue in Europe needs to be developed to support the European organisations, governments, infrastructures, enterprises, services and manufacturing industries.

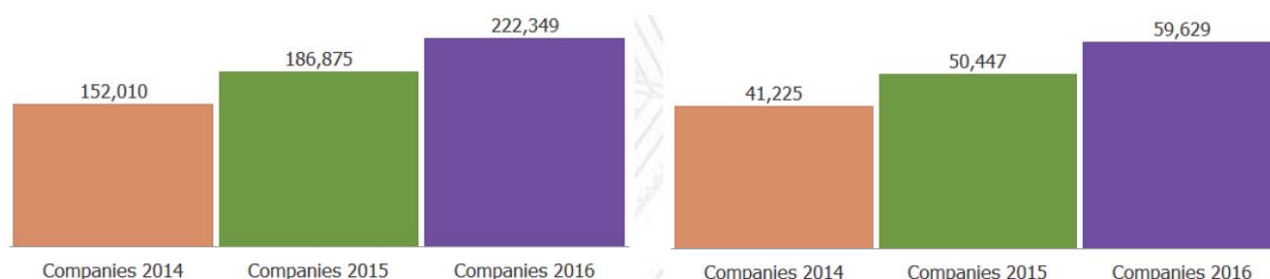
The value of Global Cyber Market has reached **640 billion euros** in 2016 increasing compared to 2015 (512 billion euros). The Value of EU Cyber Market increased by 17.4% compared to 2015 reaching **157 billion euros** of Sales. EU Cyber Market accounts for 26,3% of global market.



**Figure - Global vs EU Cyber Market 2014 through 2016**

Sales by EU country shows consistently strong growth for the past two years: growth to 2016 ranges between 14-20%. Moreover, the largest economy does not always equate to the largest growth.

Together with sales, the number of companies on the cyber market is growing: in 2016 the number of cyber companies in the world reached **222 thousands** increasing by 19% from 2015. In Europe, nearly **60 thousands companies** operated in 2016 increasing by 18,2% from 2015.



**Figure - Global vs European number of Cyber security related companies**

The number of Global Cyber employment is increasing according to the growth of the global cyber market: in 2016 the Global Cyber Employment reached 3,7 million increasing by 18% from 2015. In Europe, it is possible to note the same growth: 17,5% increase from 2015 reaching the number of 910 thousands employees.

To have a better overview on the global cyber security market, the demand for cybersecurity solutions from the sectors identified in the NIS Directive is analysed with a high-level segmentation to provide quantitative analysis of the market size and forecasts:

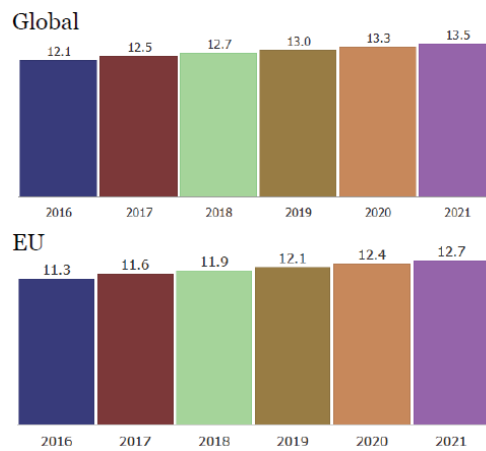
<sup>19</sup> The study is still ongoing and the preliminary results presented within the Interim Report are updated to June 6, 2017.

- "Government" – including any department, organisation or agency that is Security-specific and funded by government. For the UK, that would include Home Office, UKTI, Police and public security organisations.
- "Other Public" – including any public funded not listed above i.e. local government and those responsible for the security of public places (amongst other responsibilities).
- "Private Sector" – including a wide range of industries like Utilities, Manufacturing, Energy etc.

The range for each segment vary globally:

- Government = 18% to 26%,
- Other Public Agencies = 13% to 23% and
- Commercial = 51% to 70%

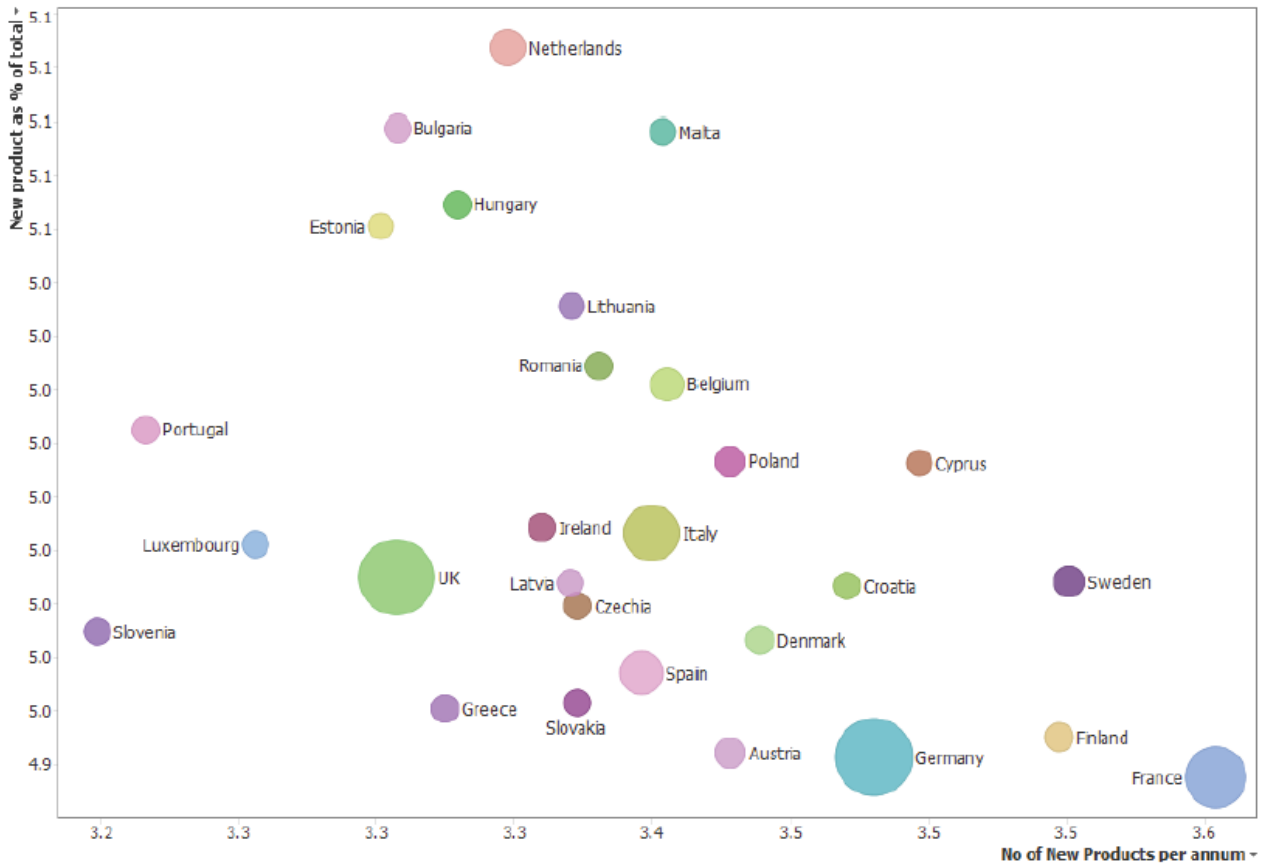
Growth forecasts for Europe are between 11% and 13% to 2021. This percentage is slightly less than global forecast growth. Both for Europe and globally, the forecast is lower than actual growth in last two years and is likely to be underestimating future short-term growth.



**Figure - Analysts Growth Forecast**

To measure the degree of innovation, the study has adopted market (demand for) innovation as an appropriate and quantifiable measure of performance. This is applied by country and by product / service. Standard metrics, taken from industry practice and collected from a wide variety of industry sources, include:

- Number new products/services per annum (pull)
- Value of new products/services per annum (pull)
- New product as % of total sales (pull)
- Average investment in R&D per annum (push)



**Figure - Country Cyber Innovations - Whole Sector**

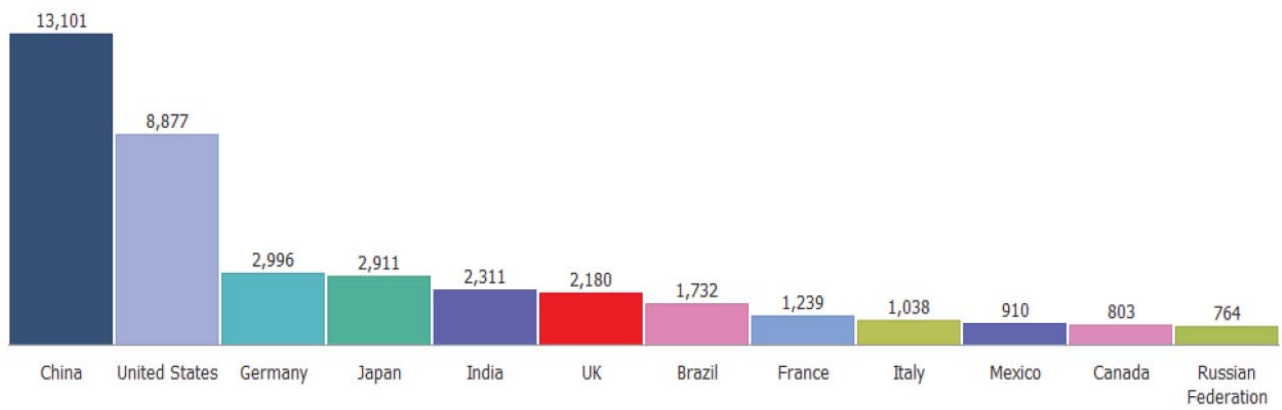
**Graphic shows:**

- Horizontal axis = new product as % of sales
- Vertical axis = new product per annum
- Bubble = value of new product sales

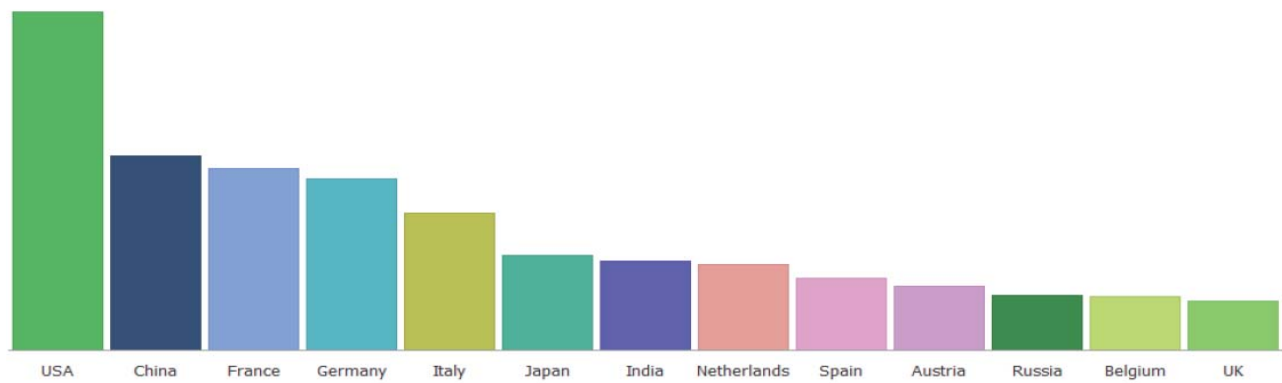
Axis ranges are narrow at this aggregated level but extend (and are more meaningful) at the sub sector level.

The cybersecurity market has also been analysed by looking at the import and export flows of cybersecurity products.

In 2016, the first country that exported the largest quantity of cybersecurity products is China. The analysis shows that four EU countries fall within the top 12 exporters of Cybersecurity products.



**Figure - Top 12 Exporters (EURm)**



**Figure - Export Destinations**

In the end, looking at the market import side, the highest value importers are Germany, France and Italy.

Country	Total EUR	Total EU EUR	Total Non EU EUR
Austria	570.8	190.9	379.9
Belgium	485.8	161.0	324.8
Bulgaria	216.5	38.6	177.9
Croatia	25.8	5.1	20.7
Cyprus	8.1	1.6	6.5
Czech Republic	389.1	62.7	326.4
Denmark	439.3	68.5	370.8
Estonia	99.8	22.8	77.0
Finland	362.8	79.3	283.6
France	1,011.4	539.1	472.2
Germany	1,608.3	508.4	1,099.8
Greece	416.5	82.7	333.8
Hungary	433.5	79.0	354.4
Ireland	66.0	13.6	52.4
Italy	964.1	406.7	557.4
Latvia	129.5	26.7	102.8
Lithuania	86.1	23.1	63.0
Luxembourg	14.4	3.0	11.4
Malta	3.7	0.7	3.0
Netherlands	709.8	255.4	454.4
Poland	461.3	84.0	377.3
Portugal	379.1	102.8	276.3
Romania	360.2	80.8	279.5
Slovakia	41.2	8.2	33.0
Slovenia	20.5	4.2	16.3
Spain	553.7	213.1	340.6
Sweden	363.7	81.3	282.4
UK	870.7	150.0	720.7

**Figura 1 - EU Cyber Imports**

## 7.6 Case Study – “The impact of an EU wide Certification Scheme on Smart-Meter Industry”

**A smart-meter company, which wants to sell its products in two Member States e.g. France and UK.**

	Now	Future
<b>Requirements</b>	<ul style="list-style-type: none"> <li>• <i>In order to sell in UK and France manufacturers have to certify against different schemes:</i> <ul style="list-style-type: none"> <li>○ <i>CPA (Commercial Product Assurance) in UK,</i></li> <li>○ <i>CSPN (Certification de Sécurité de Premier Niveau) in France</i></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>○ Manufacturers will need to undergo a single certification process, as envisaged in the future European certification scheme for smart meters. The resulting certificate will be accepted by all public authorities in Member States.</li> </ul>
<b>Cost</b>	<ul style="list-style-type: none"> <li>• The overall cost is at least 300 thousand euros for the two markets (about 150 thousand euro in UK and about 150 thousand euros in France).</li> </ul>	<ul style="list-style-type: none"> <li>• The estimation of costs saving ranges up to <b>80% of current costs</b></li> </ul>
<b>Time</b>	<ul style="list-style-type: none"> <li>• <b>6 to 18 months.</b> This estimate takes into account: <ul style="list-style-type: none"> <li>○ Completion of multiple certifications processes and supporting documentation</li> <li>○ Identification of various requirements that a vendors needs to comply with.</li> <li>○ limited number of conformity assessment bodies able to certify against the requirements of different schemes.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Faster process</b> that takes into account: <ul style="list-style-type: none"> <li>○ Role of ENISA that provides information needed for compliance with the European scheme (e.g. specialised conformity assessment; documentation)</li> </ul> <p>Completion of single process : no multiple certifications are needed and capacities of existing CABs can be used more efficiently</p> </li> </ul>
<b>Other</b>	<b>Different methodologies</b> for risk assessment and definition of security requirements	<b>Standard methodologies</b> for risk assessment and definition of security requirements

---

## Full Description:

**Methodology:** The research methodology of this case study is based on literature retrieved from desk research and on the analysis of multiple interviews with cybersecurity experts and professionals working in the Smart-Meter Industry.

**Background:** By May 2014, Member States committed to rolling out close to 200 million smart meters for electricity and 45 million for gas by 2020 at a total potential investment of €45 billion. By 2020, it is expected that almost 72% of European consumers will have a smart meter for electricity while 40% will have one for gas. Up to date, 80 million smart meters have been installed in the EU28 and Norway, which constitutes 30% of the overall European electricity metering points<sup>20</sup>. With potentially millions of networked end-points, there are significant cyber threats organizations and consumers will be exposed to.

**Fragmentation of the Smart Meter Industry:** Various and not fully coordinated certification initiatives across Europe are increasing fragmentation in the domain of ICT certification and therefore also for Smart-Meter Industry, resulting in duplication of efforts and waste of resources. The non-exhaustive list of certification schemes applicable to Smart Meters across Europe includes, among others:

- CPA (Commercial Product Assurance) is the certification scheme recognised in UK,
- CSPN (Certification de Sécurité de Premier Niveau) is the certification scheme recognised in France,
- A protection profile based on Common Criteria is the certification scheme recognised by BSI in Germany.

These three European Countries **do not recognise** each other their certification scheme.

The processes of certification are based on national requirements. In the UK, they are called security objectives. Based on these requirements and objectives, each MS has defined a security certification approach at a national level. There are also national communications infrastructure for devices connected to smart-meters including interfaces with the different stakeholders involved such as the German Smart Meter "**Gateway**" and in the UK the so-called "**Communication Hub**". Other national initiatives are emerging as the **Dutch Smart Meter Requirements** (DSMR) developed by the Dutch national organization of DSO's "Netbeheer Nederland". If Member States across Europe continue not to accept each other Certification schemes, each Member States will continue to improve its own Certification scheme and this could create a strong legacy making harmonisation more difficult. Another problem regards a European accordance on minimum requirements, on documentations and tests results for the same functionality and in the same language, ready and accepted by the different authorities of different countries. Furthermore, such fragmentation is also happening on the evaluation side; the three different Certification Schemes mentioned above require three different methodology of evaluation and it's not always sure that they give the same results. There are only limited number of Conformity Assessment Body (CAB) that are able to certify against the requirements of different schemes and the evaluation period for Smart meters products, as above mentioned, usually can last from **6 months to 18 months**. In this way, additional market entry barrier are created.

**Cost for Certification:** The proliferation of national certification scheme increases costs for businesses operating cross-border and is likely to create obstacles for the internal market, as it raises the costs for companies/vendors operating across borders. This barrier is more significant for small and medium sized enterprises, which have usually less resources to dedicate to certification programmes.

To provide concrete example, considering that the cost of certification depends on products, evaluation assurance level needed or components to be evaluated, the cost of certification can reach more than 1 million euros and the SMEs are out of this gain. For BSI "**Smart Meter Gateway**" certificate the cost is much more than **one million euros**. The cost for smart meters certification in UK is almost **150 thousand euro**. In France, the cost it is similar to the UK, about **150 thousand euros or more**. In Netherlands, the average costs of a certification under Baseline Security Product Assessment (BSPA) scheme are approximately **40 thousand euros**. The significant difference of costs for certification between Germany and other Member States have various reasons. France is for instance more focused on testing in a fixed time: given a fixed time

---

<sup>20</sup> USmartConsumer Project, European Smart Metering Landscape Report, "Utilities and consumers", 2016

---

the device has to pass all the security tests during that time. At the end of the fixed time, a finale report is sent on whether it is working fine or not. The German approach has a higher level of tests and assurance. On the other hand in UK and in France a security assessment is performed on one product, while in Germany the whole infrastructure need to be tested and certified. Considering that these National Certification schemes are not mutually recognised, smart meters companies should sustain additional costs in order to enter another Member State's market. In fact, the total cost for certification usually ranges **from 150 thousand euros to 1 million euros and more**. Only one of the biggest smart-metering companies is starting a certification to enter other markets and all the other companies are present only in the German market. In this context, one of the most important barrier to trade for the smart metering industry are the costs for certification. In the absence of an EU wide certification framework a Smart Meters company that wants to access the French market must certificate its products under the CSPN scheme and once again under the CPA scheme to enter the UK market, therefore it would pay **300 thousand euros**. With an EU wide framework, being the product certification of France deemed as equivalent to the one in the UK, the smart-meter company will have to certificate only once but will access the French and English market paying a cost of around 150 thousand euros and a **direct saving of 150 thousand euros**. More in general, it is estimated that the introduction of an EU wide certification framework could lead to smart meters companies **saving up to 80% on costs**.

**Benefits for the Smart Meter Industry of an EU wide Certification Framework:** For the Smart-Meters industry a European scheme would be a valuable policy option. It would make certification schemes mutually recognised across Europe, standardise a methodology on how risks are assessed and how security requirements are defined. Moreover, it would be very important to have flexibility in certification scheme, determine also on the risk connected to the product evaluated and the risk connected to the location of the product. The introduction of an EU wide Certification scheme will produce many benefits for the Smart Meters industry including:

- the reduction of fragmentation,
- the reduction of market barriers,
- the reduction of the costs for certification.

**Conclusion:** There is no common baseline set of security requirements that can be recognized by all participating EU Member States. At least three Member States have defined their own protection profiles. These requirements are different per country, based on different standards and adopted by technical committees. There is no scheme that includes all aspects and enables a pan European approach<sup>21</sup>. In order to improve the current situation and to reduce the market fragmentation and the costs for certification, the introduction of an EU wide Certification scheme could have a positive impact for the Smart Meter Industry. A European framework would reduce also the information asymmetry on security requirements of ICT products and make the European Market less fragmented.

---

<sup>21</sup> ENISA, Smart grid security certification in Europe, December 2014

## 7.7 Case Study – “The impact of an EU wide Certification Scheme on Alarm Systems Industry”

	Now	Future
<b>Requirements</b>	<ul style="list-style-type: none"> <li>A manufacturer of a security alarm systems seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates requested in different Member States</li> </ul>	<ul style="list-style-type: none"> <li>Manufacturer need to undergo a single certification process as envisaged in the future European certification scheme for alarm system. The resulting certificate will be accepted by all public authorities in Member States</li> </ul>
<b>Cost</b>	<ul style="list-style-type: none"> <li>The costs of certifications of an alarm system are on average (with a large spread depending on the nature of the product) at the level of <b>200-300 thousand euros</b> for full access to Europe including all tests</li> </ul>	<ul style="list-style-type: none"> <li>The estimated cost for obtaining a single European certificate would amount to <b>40-60 thousand euros</b></li> <li>A potential impact in terms of cost savings for intruder alarm systems amounts to a range of <b>4.7 million euros to 9.9 million euros per year</b></li> </ul>
<b>Time</b>	<ul style="list-style-type: none"> <li><b>Long “time to market”</b> due to the multiple processes/test to obtain several certifications for a single product</li> </ul>	<ul style="list-style-type: none"> <li><b>Reduction</b> of the "time to market" thanks to a single certification process. ENISA would accelerate this process by providing all information and documentation needed for compliance with the European scheme</li> </ul>
<b>Other</b>	<ul style="list-style-type: none"> <li>High costs and long duration of certifications are barriers to market for alarm systems. These will deteriorate the competitiveness of the EU industry on the global market.</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced competitiveness of European industry through: <ul style="list-style-type: none"> <li>Reduction of costs and time associated to multiple certification requirements</li> <li>Improved transparency of EU-wide security requirements needed for this product</li> <li>Enhanced competition among EU suppliers</li> </ul> </li> </ul>



---

## Full Description:

**Methodology:** The research methodology of this case study is based on literature retrieved from desk research and on the analysis of the European landscape of Alarm-Systems and Security Industry.

**Background:** The security industry in the EU generates a turnover of close to € 200 billion, and creates employment for 4.7 million persons<sup>22</sup>. European companies are still among the world leaders in the majority of the segments of the security sector. One of these segments is represented by Alarm Systems Industry. According to a new research report by Berg Insight, the number of monitored alarm systems in Europe is forecasted **to grow from 8.7 million in 2016** at a compound annual growth rate (CAGR) of 4.0 percent **to reach 10.6 million in 2021**<sup>23</sup>. The growing international competition and recent market evolutions do however indicate that the global market shares of European companies could drop significantly over the next years if no action is launched to enhance the competitiveness of the EU security and alarm systems industry. The Security market has three distinctive features<sup>24</sup>:

- (1) It is a highly fragmented market divided along national or even regional boundaries. Security, being one of the most sensitive policy fields, is one of the areas where Member States are hesitant to give up their national prerogatives.
- (2) It is an institutional market. In large parts the security market is still an institutional market, i.e. the buyers are public authorities. Even in areas where it is a commercial market, the security requirements are still largely framed through legislation.
- (3) It has a strong societal dimension. Whilst security is one of the most essential human needs, it is also a highly sensitive area. Security measures and technologies can have an impact on fundamental rights and often provoke fear of a possible undermining of privacy

**Fragmentation of the Security Industry:** Various and not fully coordinated certification initiatives across Europe are increasing fragmentation in the domain of ICT certification and therefore also for Security and Alarm Systems Industry which are becoming more and more dependent on the internet, resulting in duplication of efforts and waste of resources. A producer of a security alarm system seeking to supply their product throughout the EU will typically need to apply for 10-15 certificates from different Member States<sup>25</sup>. The non-exhaustive list of certification schemes applicable to Alarm Systems and Security products across Europe, includes, among others:

- **CertAlarm:** The CertAlarm Certification Schemes provide a proof of conformity the European (EU) product, system, installation and service standards. The scheme is based on the principle of independent third-party assessment and certification of security products. The CertAlarm Certification includes some standards on IP interoperability implementation based on Web services for each kind of alarm<sup>26</sup>.
- **Alarm System Certificate**<sup>27</sup>: The alarm system Certificate is the UL Mark for programs designed to meet the needs of alarm service providers, their customers, and interested stakeholders. It is the alarm company's declaration that the system will be installed, maintained, tested and monitored in accordance with applicable codes and standards. The Alarm System Certificate includes a cybersecurity standard (UL 2900)<sup>28</sup>
- **ONVIF and PSIA:** the Open Network Video Interface Forum (ONVIF) and the Physical Security Interoperability Alliance (PSIA) are two recently created organisations with the aim of developing interoperability standards for Internet Protocol (IP) based security systems. Both these bodies are promoting conformity schemes based on manufacturers undertaking their own conformance testing. ONVIF's Profile Q offers the advanced security required in today's technological world, giving integrators and end users the necessary protections from today's cyber security threats, in addition to providing out-of-the-box interoperability<sup>29</sup>.

---

<sup>22</sup> [https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/industry-for-security_en)

<sup>23</sup> <http://www.berginsight.com/news.aspx>

<sup>24</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0417&from=EN>

<sup>25</sup> ECORYS. (2011). Security Regulation, Conformity Assessment & Certification. Brussels: Report delivered by ECORYS for the European Commission.

<sup>26</sup> [http://www.certalarm.org/ca/sites/default/files/Scheme%20Rules-2-Iss\\_5.pdf](http://www.certalarm.org/ca/sites/default/files/Scheme%20Rules-2-Iss_5.pdf)

<sup>27</sup> <http://industries.ul.com/blog/alarm-system-certificate>

<sup>28</sup> ([http://industries.ul.com/wp-content/uploads/sites/2/2016/04/UL\\_CAP-Overview-Info.pdf](http://industries.ul.com/wp-content/uploads/sites/2/2016/04/UL_CAP-Overview-Info.pdf))

<sup>29</sup> <https://www.ifsecglobal.com/onvif-introduces-profile-q-to-tackle-cyber-security-challenges/>

- **EuroPriSe:** EuroPriSe is a European scheme providing privacy and data protection certification for IT products and IT-based services. The procedure consists of an evaluation of the product or service by admitted legal and IT experts and a validation of the evaluation report by an independent certification authority<sup>30</sup>.

**Cost for Certification:** The costs of certification of an alarm system are on average (with a large spread depending on the nature of the product) at the level of **200-300 thousand euros** for full access to Europe including all tests. Stakeholders indicate that the estimated cost for obtaining a mutually recognised certificate for the same alarm system would amount to **40-60 thousand euros**<sup>31</sup>. Under an EU-wide system of conformity assessment and certification that provides for mutual recognition of certification throughout the EU, security products will have to be certified only once, instead of multiple times. This implies a reduction of costs associated to multiple conformity assessment (i.e. testing) and certification for those products, and in those markets, that are currently required to undergo national conformity assessment and certification. A global estimate of the potential impact in terms of cost savings for intruder alarm systems **amounts to a range of EUR 4.7 million to 9.9 million per year**. For other product categories for which national authorities require some form of approval, the evaluation of product performance is more often organised on an *ad hoc* basis involving a mixture of testing and operational trials.

**Benefits for the Alarm-System Industry of an EU wide Certification Framework:** Without (effective) action at the EU-level (baseline), the lack of an internal market for alarm systems products/components will deteriorate the position of the EU industry on the global market. The development of EU-wide harmonised standards and a common conformity assessment procedure is expected to significantly reduce the certification costs for suppliers of intruder alarm systems where they serve multiple national markets in the EU. Moreover, it should reduce costs incurred in developing variants of products that are adapted to comply with differing standards and conformity assessment procedures at national level, which industry stakeholders consider often have limited actual impact on product performance for final customers. Removing the need for multiple certifications would enable suppliers of alarm systems to more rapidly access different parts of the EU market which, in turn, could benefit the organisation and scale of production activities. Further, by reducing delays in 'time to market' caused through multiple certification requirements, an EU-wide scheme should reduce the risk of new product innovations being replicated by competitors. Thus, an EU wide scheme should increase the potential return and reduce the level of risk associated to investments in research and technology development<sup>32</sup>.

The expected positive consequences of harmonised EU wide certification procedures are:

- reduction of costs associated to multiple testing;
- facilitated access to markets;
- reduction of the "time to market";
- improved transparency of performance requirements and standards;
- enhanced competition among EU suppliers;
- reduction of costs for conformity assessment and certification (CAC) services and the development of security technologies;
- lower prices for security technologies

**Conclusion:** In order to ensure the market leading position of EU companies over the years to come, the first priority will be to overcome the fragmentation of the EU security markets through the harmonisation of standards and certification procedures for security technologies. The societal acceptance of security technologies will be promoted through the introduction of the "privacy by design" and "privacy by default" concepts throughout the development of new security technologies. Although a handful of major players dominate both the EU (and US) market, there remain many niche markets that are very attractive for SMEs, either directly or through the supply of specialized products and components to major manufacturers and integrators, and to the installation service market. Conformity assessment and certification costs represent a proportionately higher share of total costs for SMEs and consequently a greater market access barrier. Accordingly, they are expected to benefit in particular from the cost savings resulting from EU-wide

<sup>30</sup> <https://www.european-privacy-seal.eu/EPS-en/Product-and-Service-Privacy-Certification>

<sup>31</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN>

<sup>32</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN>

---

harmonised standards and certification procedures. In addition, an EU certification scheme should serve as a recognised mark of product performance and quality that can reduce the importance of 'reputation effects' of larger players and local companies, thus facilitating SMEs to trade across borders within the EU and even in global markets. Overall, an EU-wide scheme is expected to increase market efficiency in the EU by raising the level of competition – both between EU companies and from outside the EU – and stimulate improvements in industry performance levels (e.g. productivity). It is not expected, however, that the reduction in costs resulting from an EU-wide approach would have a significant impact on the price competitiveness of EU alarm products in international markets. Nonetheless, a less fragmented EU market should encourage investment in research, technology development and innovation, which would have an impact on 'dynamic' competitiveness. Further, to the extent that it obtains higher market recognition than existing national schemes, an EU-wide certification scheme (providing for a corresponding EU security 'performance mark' or 'quality label') should contribute to strengthening broader international market awareness and acceptance of EU products<sup>33</sup>.

---

<sup>33</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0233&from=EN>

## 7.8 Case Study – “The impact of an EU wide Certification Scheme on Cloud Computing Industry”

	Now	Future
<b>Requirements</b>	<ul style="list-style-type: none"> <li>In order to sell Cloud Computing Products / Services in France and Germany providers have to certify against: <i>SecNumCloud</i> and <i>Compliance Controls Catalogue (C5)</i></li> </ul>	<ul style="list-style-type: none"> <li>Providers need to undergo a single certification process, as envisaged in the future European certification scheme for cloud computing. The resulting certificate will be accepted by all public authorities in Member States</li> </ul>
<b>Cost</b>	<ul style="list-style-type: none"> <li>Costs associated to compliance with different technical rules and multiple testing is estimated around 1.2 billion euro, that accounts for <b>2% to 10%</b> of companies' annual expenditures.</li> </ul>	<ul style="list-style-type: none"> <li>An increased level of competition, introducing an EU wide Certification Scheme, would result in a <b>yearly saving of € 1.1 billion in the EU public sector alone</b></li> </ul>
<b>Time</b>	<ul style="list-style-type: none"> <li><b>Around 7-9 months</b> due to the multiple audit and testing processes to obtain several certifications</li> </ul>	<ul style="list-style-type: none"> <li><b>Reduced time:</b> duration of a single process is estimated to take around 4 to 6 months. ENISA would accelerate the process by providing the information needed for compliance with the European scheme</li> </ul>
<b>Other</b>	<ul style="list-style-type: none"> <li>Faced with co-existence of multiple schemes and standards<sup>34</sup>, end-users (esp. in the banking sector) are not able to compare and judge which scheme or standard would best satisfy their particular security requirements. This deteriorates the trust in cloud computing services.</li> </ul>	<ul style="list-style-type: none"> <li>The existence of a security certification scheme for cloud computing agreed at EU level, increases the trust in this service</li> <li>Competitive gain for cloud providers due to cost and time reduction</li> </ul>

<sup>34</sup> ECSO has published a State-of-the-Art Syllabus listing 8 different schemes and standards to certify the security of cloud computing services. See here: [www.upm.es/observatorio/vi/gestor\\_general/recuperar\\_archivo.jsp?idf=642&tipo=2](http://www.upm.es/observatorio/vi/gestor_general/recuperar_archivo.jsp?idf=642&tipo=2)

---

## Full Description:

**Methodology:** This case study is based on information obtained from secondary sources (literature review), from the analysis of the European landscape of Cloud Computing Industry conducted on the basis of an online search and from interviews conducted with different impacted Stakeholders.

**Background:** The ongoing digital transformation is strategically affecting both private and public sector organisations also in terms of cybersecurity<sup>35</sup>. Cloud computing has the potential to reduce IT expenditure and boost organisational flexibility while at the same time improving the scope for delivering flexible high-quality new services. Some of the general benefits are reducing costs, increasing the storage capabilities and the chance to adapt in a flexible way to the changing business conditions<sup>36</sup>. These benefits can be applied in a lot of different domains and fields.

The increase in the use of Cloud globally is also visible from the Market, over the last two years<sup>37</sup>. In 2017, spending on public cloud Infrastructure as a Service hardware and software is forecast to reach **61 billion U.S. dollars worldwide**<sup>38</sup>. According to Gartner, Inc., the highest growth will come from cloud system infrastructure services (IaaS), which is projected to grow **36.8 percent in 2017 to reach \$34.6 billion**. Cloud application services (SaaS) is expected to grow 20.1 percent to reach \$46.3 billion<sup>39</sup>. Despite its growing influence, concerns regarding cloud computing still remain. There are in fact challenges that it still has to face, such as: **Data Protection, Data Recovery and Availability, Management Capabilities and Regulatory and Compliance Restrictions**<sup>40</sup>.

Incidents related to Cloud Computing services worry the companies especially for sectors such as Finance where a data breach can cause huge economic and reputable damages. According to representatives from European Banks, they are not very sure if the data are stored in a secure way, especially according to the various jurisdictions of different Countries.

Cloud Computing is going to be fundamental for the future. For this reason, it is necessary that it as secure as possible.

**Fragmentation of the Cloud Computing Industry:** Cloud service providers offer their services internationally in several markets. Therefore, national approaches for certification and assurance are of limited use to them. National cyber security authorities can usually only set national standards, even if other countries use them too<sup>41</sup>. ANSSI (Agence national de la sécurité des systèmes d'information) and the BSI have been very intensively involved with the security of Cloud Computing in recent years. Both authorities arrived at a very similar understanding of the Cloud security standards that need to be met, and both initiated new ways of verifying secure Cloud Computing, since the existing certifications failed to adequately meet the needs in this area. However, both authorities pursued different paths<sup>42</sup>.

- **Compliance Controls Catalogue (C5)** - The BSI developed the Cloud Computing Compliance Controls Catalogue (C5). This catalogue, which is closely oriented to tried and tested standards, defines the requirements for the secure provision of services critical to businesses, which the Cloud provider must meet. Additionally, the provider must make their offer transparent, such as the location of data processing and the subcontractor. The auditing process is conducted in line with the international recognised standard, the ISAE 3000. The audit report is based on standards such as the ISAE 3402 and SOC 2. Auditors and Cloud experts conduct this audit and issue an audit opinion, for which the auditor bears liability. The C5 also contains standards for greater protection needs and can be individually extended – for example for a specific industrial sector. The BSI sets the standards and specifies criteria for the audit, but has no further supervisory role with regard to specific procedures.
- **SecNumCloud** - The ANSSI takes a very different approach. The Référentiel SecNumCloud, which is strongly oriented to the ISO/IEC 27001 standard and which supplements it with several specifications of its own, defines the standards required for secure Cloud Computing. In the Référentiel, there are two levels: *sécuré* and *sécuré plus*, whereby the latter sets higher security standards and limits to France the service provided. Taking this as a basis, the ANSSI has developed a completely new certification of its

---

<sup>35</sup> <https://www.enisa.europa.eu/publications/exploring-cloud-incidents>

<sup>36</sup> [http://picse.eu/sites/default/files/ProcuringCloudServicesToday\\_March2016\\_web.pdf](http://picse.eu/sites/default/files/ProcuringCloudServicesToday_March2016_web.pdf)

<sup>37</sup> <https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#51dfa21b2187>

<sup>38</sup> <https://www.statista.com/statistics/507952/worldwide-public-cloud-infrastructure-hardware-and-software-spending-by-segment/>

<sup>39</sup> <http://www.gartner.com/newsroom/id/3616417>

<sup>40</sup> <http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf>

<sup>41</sup> [https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel\\_node.html](https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel_node.html)

<sup>42</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin\\_2016-02.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4)

own, which it has established in France. Cloud providers receive a certificate which is issued by the ANSSI and on which an audit report produced by ANSSI certified auditors is based. For example, providers who want to be certified with SecNumCloud can be audited by AFNOR Certification<sup>43</sup>.

While the security levels which the BSI and ANSSI would like to see in place are very similar, **the two very different approaches towards certification and attestation appear to contradict each other.**

Moreover, the list of applicable Standards and Certification Schemes for Cloud Computing across Europe includes, among others: ISO 27001/2, ISO 20000 (ITIL), CSA Open Certification Framework (OCF), Eurocloud, Star Audit, SOC 1-2-3, PCI – DSS, Europrise, FISMA, Cloud Industry Forum Code of Practice, ISACA COBIT, Security Rating (Leet security), TUV certified.

Motivated by the German-French business consultations<sup>44</sup> and based on a high level of mutual trust, the idea therefore emerged of generating a **new Cloud Label**. It stands for the joint Cloud security standards and is suitable evidence that they have been met. The underlying principle on which the label is based is a joint short catalogue with security targets (“core rules”). Naturally, the attestation in accordance with the BSI’s C5 and the ANSSI certification are sufficient to meet these standards. **A provider who already has one of the two certifications can receive this label and as such advertise the security level of their product very easily on both markets.** The Cloud Label is regarded by the ANSSI and BSI as being an explicitly European initiative, which can also incorporate the certifications of other countries. In this way, the expertise and independent nature of the BSI and ANSSI, as well as their cooperation based on trust, are of benefit to the whole of Europe.

Another European initiative towards a unique approach for ICT Security Certification Schemes comes from **Horizon 2020 Programme**: the project EU-SEC<sup>45</sup>. The EU-SEC, started at the beginning of 2017, will last until 2019 and aims to create a framework under which existing, certification and assurance approaches can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the Cloud.

**Cost Analysis:** An economic paper by economists of DG ECFIN estimated that the cost associated to differences in technical rules and multiple testing/certification are between **2% to 10% of companies annual turn-over**<sup>46</sup>. According to this paper inadequate standards and insufficient mutual recognition, including in the ICT sector, is among the main barriers to the single market. For example, the costs of an ISAE 3000 implementation project, in order to be certified under the Cloud Computing Compliance Controls Catalogue (C5) Scheme, can vary from **ten thousand USD up to a million USD or even more**<sup>47</sup>. The costs for enterprises of product conformity assessment can be substantial and where there is lack of mutual recognition this implies the multiplication of such costs: for companies offering several product types on a national market of a receiving Member State the costs amount to approximately 2% of their entire annual turnover on that market, whereas they can reach up to 10% for companies specialized in one specific product type because they do not benefit from economies of scale<sup>48</sup>. Even applying the lower bound of 2% only to 60% of the cyber security market to be conservative (i.e. assuming 40% of the market concerns products for which certification is not required) **the costs of lack of mutual recognition reach a figure in the range of 1.2 billion euro.**

Moreover, many organizations are ‘locked’ into their ICT systems because detailed knowledge about how the system works is available only to the provider, so that when they need to buy new components or licenses only that provider can deliver. **This lack of competition leads to higher prices and some € 1.1 billion per year is lost unnecessarily in the public sector alone**<sup>49</sup>.

<sup>43</sup> <http://www.afnor.org/en/news/cybersecurity-vigilance-required/>

<sup>44</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin\\_2016-02.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4)

<sup>45</sup> [http://cordis.europa.eu/project/rcn/207439\\_en.html](http://cordis.europa.eu/project/rcn/207439_en.html)

<sup>46</sup> Ilzkovitz, F. Dierx, A. Kovacs, V. & Sousa (2007) Steps towards a deeper economic integration: the internal market in the 21st century<sup>46</sup>, European Economy, Economic Papers, No. 271. European Commission.

<sup>47</sup> <https://www.isae3000.com/controlreports>

<sup>48</sup> Ibid. p. 61

<sup>49</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0455&from=EN>

As mentioned in the SWD "A Single Market Strategy for Europe - Analysis and Evidence"<sup>50</sup> a large body of economic studies that show the impact that standards have on economic growth and GDP<sup>51</sup>. **For France the impact on growth is estimated at 0.8 %, for United Kingdom at 0.3 % and for Germany at 0.9 % of GDP.** To put this in monetary terms, DIN (the German Institute for Standardization) estimates that in Germany alone, standards generate up to EUR 17 billion a year. A more recent study from the UK 'The Economic Contribution of Standards to the UK Economy' also confirms that the use of standards benefits the national economy: standards contributed to around EUR 11 billion of the EUR 40 billion GDP growth in 2013 (2014 prices) and to around EUR 8.5 billion to UK exports<sup>52</sup>. The same study shows that standards help to enhance quality, with 70 % of respondents stating that standards had contributed improving the quality of supplier products and services. In the econometric models supporting such estimates standards are considered, together with R&D expenditure and patents, as fuelling the knowledge input in the classical production functions. One key hypothesis is that standards can, to some extent, counterbalance some well-known market failures and the possibility that investments in knowledge by private players are sub-optimal and not sufficient to produce social surplus (externalities).

**Benefits for the Cloud Computing Industry of an EU wide Certification Framework:** In a world that is increasingly interconnected, it does not make much sense for a State to tackle digital security issues on its own. The new French digital security strategy states France's will to engage a dialogue both within multilateral organizations and with long-term trustworthy partners following two objectives: contributing to the global stability of cyberspace as well as reinforcing the States' own cybersecurity.

The longstanding and close bilateral cooperation between ANSSI and BSI is based on trust and has been greatly facilitated by a shared vision on many strategic and political issues, a common positioning at the national level fulfilling only defensive missions and a comparable high level of technical expertise.

ANSSI and BSI have been working together in many fields, such as cloud-computing with the creation of a common label for secure cloud service providers, security certification through a very strong support of the international recognition schemes (CCRA and SOG-IS) and industrial synergies. An EU wide Certification Framework could guide these initiatives in order to avoid the fragmentation of Standards and Certification Schemes across Europe and the further development of National Approaches. The benefits of standardization through an EU wide Certification Scheme include, among others:

- **Competitive Advantage.** Companies are motivated to participate in standardization because they gain an edge over non-participating companies in terms of insider knowledge. Early access to information is valuable;
- **Cost Reduction.** Standardization leads to lower transaction costs in the economy as a whole, as well as to savings for individual businesses. Transaction costs drop considerably as a result of standards, since they make information available and they are accessible to all interested parties;
- **Supplier/Client Relationship.** Standards can help businesses avoid dependence on a single supplier because the availability of standards opens up the market. The result is a broader choice for businesses and increased competition among suppliers;
- **Standards and R&D.** Businesses not only reduce the economic risk of their R&D activities by participating in standardization, but can also lower their R&D costs. When a company can influence the content of standards to its advantage, the economic risk is lower. The expense of R&D is potentially reduced when the participants in standards work make their results generally available, and research need not be duplicated

<sup>50</sup> Brussels, 8.10.2015 SWD (2015) 202 final, accompanying the document Upgrading the Single Market: more opportunities for people and business (COM (2015) 550 final) {SWD(2015) 203 final}.

<sup>51</sup> Among peer-reviewed journal articles see: Acemoglu, D., G. Gancia and F. Zilibotti (2012), 'Competing Engines of Growth: Innovation and Standardization,' *Journal of Economic Theory*, 147, 570–601; Blind, K. and A. Jungmittag (2008), 'The Impact of Patents and Standards on Macroeconomic Growth: A Panel Approach Covering Four Countries and 12 Sectors,' *Journal of Productivity Analysis*, 29, 51–60; Jungmittag, A., K. Blind and H. Grupp (1999), 'Innovation, Standardisation and the Long-term Production Function,' *Zeitschrift für Wirtschafts- und Sozialwissenschaften*, 119, 205–222; Wakke, P., Blind, K.; Ramel, F. (2016): The impact of participation within formal standardization on firm performance, *Journal of Productivity Analysis* 45 (Issue 3), 317–330; Wijen, F.H. (2014). Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. *Academy of Management Review*, 39 (3), 302-323. Swann, P. (2010), *International Standards and Trade: A Review of the Empirical Literature*. Report for the UK Department of Business, Innovation and Skills (BIS). OECD Trade Policy Working Papers. Among reports commissioned by standardization bodies see: SCC (2007). Economic Value of standardisation; AFNOR (2009). The Economic Impact of standardisation; DIN (2011). The Economic Benefits of standardisation; Standards Australia (2012). The Economic Benefits of standardisation; Cebr (2015). The Economic Contribution of standards to the UK Economy; Cebr (2016). Economic Contribution of Standards in Ireland – A report for the National Standards Authority of Ireland.

<sup>52</sup> British Standards Institution (BSI), 'The Economic Contribution of Standards to the UK Economy', 2015

- 
- **Raising Trust.** An annual report featured on eWeek<sup>53</sup> shows that 73% of survey respondents are worried about cloud computing security. An EU wide Certification Scheme could raise the trust level of companies in the Cloud Computing services, reducing insecurity due to the various jurisdictions of different Countries.

**Conclusion:** Even if States are primarily responsible for their national digital security, it is France and Germany's shared vision that many challenges can best be addressed **through a common and coordinated effort at European level.** This could be guaranteed introducing an EU wide Certification Framework, which avoids multiplication of National Approaches, duplication of efforts and waste of resources. Beyond the development of EU Member States' capacities and cooperation, the EU must as well recognize that European digital security is challenged on other fronts, requiring a collective ambition to guarantee Europe's digital sovereignty. Three challenges in particular are ahead of us<sup>54</sup>:

- the EU and the Member States' ability to protect and defend the EU institutions, the administrations, the critical infrastructures, the companies and the general public in cyberspace must be ensured;
- the EU must actively support the development of sustainable European industries in the field of digital security and guarantee Member States' ability to evaluate and approve the security of digital products and services;
- the EU must preserve its capacity to choose autonomously how data and related services should be protected in Europe.

Along with like-minded Member States, France and Germany will closely work together to promote the European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of European values.

---

<sup>53</sup> <http://www.eweek.com/cloud/companies-worry-about-security-implications-of-cloud-services>

<sup>54</sup> Federal Office of Information Security, BSI, Security in focus, Europe and International Cooperation, BSI Magazine 2016/02



---

## 7.9 IoT Trust Label - Proposed Requirements as a Basis for Endpoint Trust Labels (from Stakeholder Support)

The IoT Trust Label requirements consist of a set of endpoint guiding principles that enable for an IoT solution to have an intelligent, automated and secure way to manage the device through its lifecycle. End users, including consumers, enterprises, and service providers, purchasing labeled equipment and services can have confidence as to the level of trustworthiness that vendors are building into their products. The basis of these requirements is that the system and its components should provide protection across the end to end solution – before, during, and after an attack.

In the context of the IoT, a “Thing” is an endpoint that has network connectivity and a well-designed purpose with constrained functionality as compared to general purpose IT devices. **A trust labeled Thing has additional capabilities that provide owners and operators the confidence that it is designed to be secure and simple to manage.** For the purpose of this trust label document, “Endpoint” and “Thing” are the same.

The IoT Trust Label requirements are intended to improve overall cyber resilience of IoT solutions by addressing common weaknesses with products and ecosystems that provide easy attack vectors. A second and equally important outcome is that the end user can have confidence in these products because manufacturers are accountable for what is “built in” to the product.

Labeling is a mechanism of informing interested parties of the capabilities or components of the labeled equipment. The following information should be delivered as part of the label definition:

- The actual assertions being made,
- Identification as to whether assertion is made by vendor or 3rd party testing/certification organization.

Additional information that could be considered for either part of the label definition or part of the assertions include:

- Is this assertion time limited?
- Is this assertion dependent on external services or facts that might change?

Where the assertions being made are direct facts, it is sometimes advantageous to simply list them. For example, the “grams of sugar” within a food serving is a factual statement. A conversion of this direct fact, using an external standard, can be used to help consumers make informed choices. For example, 25g of sugar is “50% daily value” and performing this lookup when printing the label is intended to help consumers understand the relevancy of their decision; it saves them a step of doing the lookup or memorizing the recommendations. While advantageous for communicating with homogenous user base with general agreement concerning the “daily value” metrics, this form of label is less helpful at communicating core information (# of grams) to consumers with custom use cases (for example a vet at zoo attempting to determine if the grams of sugar in a snack are appropriate for an orangutan with a different calorie diet, a different daily value for sugar).

Similarly, security labeling provides simple information to the end user for making purchasing decisions. The situation is complicated by the variety of use cases and associated disagreement about the “daily value” metrics. One use case might prioritize lots of confidentiality (sugar) and another might prioritize lots of availability (think “protein” in our nutrition metaphor).

The labeling method therefore must impart either:

- The use case labeling indicates the offer is appropriate for
- Or, discrete facts that allow the end user to judge appropriateness for arbitrary use cases

There is commonality among use cases in that, at least with respect to cyber security resilience, it may be useful to combine and generalize facts in a way that imparts high level information without also enforcing a specific use case. This hybrid approach may be more tractable.

---

Endpoint capabilities will vary greatly depending upon intended application(s), deployment environment, and cost considerations (memory size, computing power, battery life, etc.). As such, the requirements have been aligned to three Trust Label categories that aim to provide purchasing guidance based on the expected usage of the device and the environment where it operates.

- **Bronze:** The bronze level of IoT device provides the lowest level of assurance and cyber resilience to the end user and does not require any technical changes to the product itself. Vendors provide one-time information describing the device and expected behavior to achieve this level of compliance. Bronze devices rely on their implicit identities to provide the underlying network infrastructure to provide essential “Before” capabilities in the security, data protection, and privacy areas.

Devices in the Bronze tier are targeted at buyers that are price sensitive and NOT concerned about the overall security or resilience of the individual device due to the level of management that can be provided through existing network and security capabilities that exist within the organization to provide before, during, and after protections. If the device is compromised by an attacker, the buyer accepts the fact that the device would have to be replaced with a new unit.

- **Silver:** In addition to meeting the Bronze level requirements, the Silver level IoT device implements more trustworthy identity and authentication mechanisms, standalone cyber security functionality, and assists the network in enhancing the device’s cyber resilience in the “Before” and “During” attack continuum stages by providing some visibility into the devices security state. The cybersecurity functionality of the device compliance tested by vendor and the results MAY be shared with customers. Vendors must also provide or contract for any ongoing cloud services that are required to maintain the cyber resilience of the device.

Devices in the Silver tier are targeted at buyers that are concerned about the overall cyber security and resilience of the individual devices being deployed, but do not have the need or capability to provide ongoing network and security management for their devices. Unlike the Bronze device, if this class of device is vulnerable to exploit or compromised by an attacker, the vendor provides software updates to mitigate security vulnerabilities for a period of time that is made known to the buyer via the trust label.

- **Gold:** In addition to meeting the Silver level requirements, the Gold level IoT device and its vendor provide visibility into the security, data, and privacy assertions that are made as well as coverage across the Before, During, and After stages of to the attack continuum. Secure development lifecycle compliance, independent security testing results, information on data usage and protection controls, and the ability to control the personal or customer data usage MUST be readily available for customers.

Devices in the Gold tier are targeted at buyers that are extremely sensitive to risks associated with security, data, and privacy. As a result of the increased visibility into the device’s security state, Gold devices are best suited for tight network integration and enable maximum cyber resilience across the attack continuum.

**Bronze Devices** Appropriate use cases for Bronze devices include areas where the things are deployed within a managed environment that provides appropriate security and safety controls to compensate for the lack of resilience of the actual Thing.

An example of a bronze device would be connected lights deployed within a traditional enterprise network environment where an IT organization is able to layer in appropriate controls based on the Thing manufacturer’s device usage information in order to compensate for the device’s lack of cyber resilience capabilities.

### **Silver Devices**

Silver devices are well suited for deployment within consumer use cases where an IT organization is not present and/or the consumer is not able to provide sufficient management and control of the devices to protect them against a cyber-attack.

An example of a silver device would be a connected baby monitor that allows the consumer to trust that the device is operating securely and protecting the privacy of the owners.

---

## Gold Devices

Gold devices are best suited for deployments that require a higher level of assurance that the device is operating in a known to be good state of security due to either the criticality of the use case or sensitivity of the data being processed.

An example of a gold device would be an autonomous vehicle being used by a taxi service where the passengers of the vehicle would ideally be able to be aware of the security state of the vehicle prior to departure.

## Endpoint Capabilities

Each requirement is specified with an associated compliance level. Where applicable, a normative reference and/or open source reference implementation is provided. For areas where a standard does not exist, or the requirement may be more difficult to measure, we have provided non-normative references.

### Secure Manufacturer-based Identity and Certificate Storage (Silver)

Endpoints that communicate via IEEE 802 networking MUST contain a certificate (IDevID) along with the MUD-URL, and associated private key for the certificate. [IEEE802.1AR]

### *Secure Local Identity (Silver)*

Endpoints that implement IEEE 802 networking MUST support installation of at least one local certificate (LDevIDs) and associated private keying material.

### *Certificate Management (Silver)*

An Endpoint that communicates via IEEE 802 networking MUST support [RFC7030], Section 3 on TLS Layer, for certificate management of secure transport.

### *Key and Certificate Storage Requirements (Silver)*

The Endpoint MUST contain the certificate chain used to validate BRSKI vouchers, as well as any trust chains necessary to validate signatures on firmware or software updates.

### *Secure Storage (Gold)*

Endpoints MUST store private keying material and certificates in tamperproof storage.

### *Random Number Generation (Silver)*

Quality random number generation is required by several of the security protocols implemented by an Endpoint.

An Endpoint MUST provide random number generation either through hardware or as compliant with FIPS 140-2 Sections 4.7.1 and 4.9.2 or equivalent standards.

### *Cryptographic Protocol Support*

#### Hash Algorithms (Silver)

An Endpoint MUST minimally support the SHA-256 hash algorithm. Endpoints MAY support stronger suites and algorithms.

### *Asymmetric Cryptography: LDevIDs (Silver)*

An Endpoint MUST provide support for Elliptic Curve Cryptography described in [RFC6090] and [IEEE802.1AR] for use as LDevIDs.

### *Asymmetric Cryptography (IDevIDs) (Silver)*

An Endpoint MUST support either 2048-bit RSA certificates or ECC certificates as described in [RFC6090] and [IEEE802.1AR] for IDevIDs .

### *(D)TLS Cipher Suite Support (Silver)*

Endpoints MUST minimally support the TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CCM\_8 cipher suite which is detailed within [RFC 7251] for EAP-TLS. This cipher suite will be used for the authentication operations used for both network layer and application layer authentication processes.

### *Endpoint Hardening (Silver)*

---

Endpoints MUST only run services that are described in the MUD profile. Extraneous code MUST be removed prior to Endpoint production.

#### *Authentication*

The focus of this section is Endpoint-2-Network authentication. This includes during initial establishment of secure network connectivity (aka onboarding) and subsequent management activities.

#### *EAP-TLS (Gold)*

Endpoints using IEEE 802.3 (wired Ethernet) MUST support [IEEE 802.1x] using the EAP-TLS [RFC5216] EAP method. Endpoints that have IEEE 802.11 transceivers MUST make use of [IEEE802.11] security in conjunction with [IEEE802.1X] (WPA Enterprise) to exchange [IEEE802.1AR] certificates.

#### *IEEE 802.1x (Silver)*

Prior to completing onboarding (e.g. obtaining a local trust anchor and LDevID) Endpoints communicating on IEEE 802 networks MUST authenticate using their IDevID and MUST accept the local 802.1X network credentials without validation purely for the purposes of onboarding.

[[NOTE: the change-of-authorization for the 802.1X session after onboarding is complete is not clearly defined]].

After LDevID enrollment via onboarding subsequent 802.1X sessions are authenticated using the LDevID. The Endpoint MAY make full use of the connection for management and thing-to-thing and thing-to-vendor communications.

The reference implementation for IEEE 802.1X can be found here and is available in most Linux distributions.

#### *Onboarding (Silver)*

Endpoints MUST initiate BRSKI onboarding, including support for the BRSKI-optional integrated EST enrollment for an LDevID. Network infrastructure MUST only allow BRSKI onboarding for Endpoints that authenticate using their IDevID credential. See [BRSKI] for details.

The Endpoint MUST fail gracefully, if attempted connections are rejected.

#### *Ongoing Key Management (Silver)*

EST supports key renewal. IoT Trust Label Endpoints that use IEEE 802 networking to communicate MUST renew their LDevIDs via EST no later than 30 days prior to expiration of the current key, and must log any renewal failures with increasing urgency.

#### *Transmission and processing of MUD-URLs (Silver)*

A MUD-URL is transmitted as part of a certificate. If the endpoint cannot find a local registrar for 802.1X or BRSKI, it MUST transmit the MUD-URL found in the certificate or otherwise configured via LLDP or DHCP.

A reference implementation for a DHCP client that supports MUD is dhcpcd, which is distributed with most major distributions. A second reference implementation is dhclient, which is distributed by ISC.

A MUD File generator is available at <https://www.ofcourseimright.com/mudmaker/>.

#### *Secure Firmware/Software Update (Silver)*

Endpoints MUST have the ability to securely receive and apply a software and/or firmware update. All Updates MUST be signed by the manufacturer and Endpoints MUST validate signatures. The endpoint MUST be configured to check for an HMAC signature whose key strength is determined by deployment environment. Careful key management processes SHOULD be implemented during code development and release.

#### *System Event Logging (Silver)*

Endpoints MUST implement SYSLOG to report all anomalous behavior and any supervisory access to provide the necessary visibility for incident monitoring and defense.

Examples of supervisory access include:

- Reading the Endpoint state.

- 
- Configuration change to the Endpoint.
  - Updating Endpoint software or firmware.

Anomalous behavior includes excessive unauthorized access attempts or excessive or inappropriate use of the Endpoint. An example would be door lock that is repeatedly activated in a very brief period of time.

A normative reference for logging can be found at:  
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf>.

#### *Secure Event Logging (Silver)*

Event logging MUST be made using syslog over DTLS [RFC6012]. The certificate used to authenticate to the syslog server SHOULD be the same one established during onboarding operations.

A reference implementation for syslog over DTLS can be found at  
[http://www.rsyslog.com/doc/tls\\_cert\\_client.html](http://www.rsyslog.com/doc/tls_cert_client.html)

#### *Time Distribution (Silver\*)*

During onboarding, the BRSKI protocol is designed to support devices that do not have a real-time clock. The full details are described in the BRSKI document but are summarized as: The network administrator decides if BRSKI vouchers are permanent (timeless) or if they are required to have a cryptographic nonce ensuring freshness for the particular bootstrapping attempt. Certificate validity periods are ignored until BRSKI completes. At this point the device enters a mode in which the certificate authority root certificate validity period is used to assume a current time window until Network Time Protocol (NTP) time updates narrow the window further.

A trusted time source is necessary for the process of certificate validation and reliable system event logging and correlation. Endpoints MUST use either Simple NTP version 4 [RFC4330] or time provided by a trusted and authenticated server as described in Section 5.5.

Endpoints MUST periodically write the current time to non-volatile storage, and use that as a base prior to being configured with accurate time. The purpose of doing so is simply to prevent attackers from using expired certificate to gain unauthorized access to an Endpoint.

#### *Privacy*

Endpoints may collect, store, or transmit a variety of information based on the intended usage of the device and the market vertical. Endpoint manufacturers MUST use [PRENG] or [PbD] principles during the product development cycle.

#### *Limited Collection (Bronze\*)*

Endpoints MUST only collect the information that is necessary for the stated purpose of the device and that has been communicated to the end user via a standard Privacy Policy that is available from the manufacturer's website.

A normative reference for this requirement is the EU General Data Protection Regulation (GDPR) Article 5(1c).

#### *Controlled User Access to Personally Identifiable Information (Gold\*)*

Endpoints MUST protect personally identifiable information from disclosure and modification. The actual implementation will depend on the nature of the Endpoint and associated service, but an example would be to encrypt information on the device such that only authorized users may access it.

A normative reference for this requirement is GDPR Article 5(1f).

#### *End User Data Removal (Bronze)*

During the lifecycle of an endpoint, it may be necessary to ensure complete erasure of all end user (personal or customer) data from the device. This could through a factory reset option or data removal option. One use-case for data removal would be the event of an endpoint passing from one owner to another legally or illegally.

---

Endpoints MUST provide a means to remove/erase all end personal and/or customer data. This includes any data that may be stored on the cloud server.

A set of normative references for this requirement are GDPR Article 20 - Portability and Article 17 – Erasure.

#### *Service Requirements*

These requirements relate to those necessary procedures and mechanisms that manufacturers must support in order for devices to properly function on an ongoing basis.

#### *MASA Server (Silver)*

An IoT Trust Label Manufacturer MUST provide a Manufacturer Authorized Signing Authority (MASA) service in accordance with [BRSKI]. In addition, this service MUST be secure, fault tolerant and available at all times, in order for a new device and operational network to establish trust in one another.

BRSKI supports the issuance of nonce-less vouchers that enable onboarding or recovery operations when the MASA service is not available. This does not impact the requirement that a MASA service be available when the local network administrator wishes to obtain either nonce-less or nonced onboarding vouchers.

A third-party MAY initially offer as a trusted service a MASA Server. However, the manufacturer is under no obligation to use that site.

#### *MASA Server Logging (Silver)*

The MASA server MUST maintain logging of all transactions (success and failure) for analytical purposes, such as enabling for the legitimate transfer of ownership with minimal requirements upon the device vendors. The log is made available as defined in BRSKI.

#### *MUD Server (Bronze)*

An IoT Trust Label Manufacturer MUST provide a file server that distributes Manufacturer Usage Description (MUD) files in accordance with [MUD]. This service MUST be fault tolerant and available at all times, as it is required to establish appropriate network access controls for IoT Trust Label devices.

A third-party MAY initially offer as a trusted service a site that an Endpoint manufacturer may use to distribute MUD files. However, the manufacturer is under no obligation to use that site. The service provider will validate signatures of MUD files and vet them for risks prior to them being used in local deployments.

#### *Cloud-Based Management Functionality (Gold)*

IoT Trust Label Endpoints will often establish cloud-based communications in order to satisfy various operational requirements (e.g., firmware upgrade). Such services may not be reachable by other devices in an IoT Labelled Network unless all specifically allowed by local network administrator or automatically authorized based on identity and posture of the devices. Manufacturers meeting IOT Trust Label “Silver” requirements MUST clearly label and advertise, in a MUD file or other well-known place, whether Internet access is required for a given device.

All communications to the cloud service MUST make use of TLS 1.2 or higher with the TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CCM\_8 cryptographic suite.

Furthermore, any information provided to the manufacturer (logging or customer related) must be explained clearly to customers prior to collections and transport. See Privacy requirement about Limited Collection of Data in 0.

#### *Identification by Heuristics (Bronze)*

Manufacturers MUST provide a description of device behavior that may be used by the network to infer identities and apply policies. This includes MAC address ranges used, services, and any cloud-based addresses. Note: devices that provide certificates as described in Section 3.1 are exempt from this requirement.

#### *Process Requirements*

##### *Product Vulnerabilities, Incident Reporting and Remediation (Silver)*

Product vulnerabilities will arise from time to time, either through some flaw in coding practices or through a vulnerable third party library or entity. Endpoint manufacturers MUST have an active product incident

---

response team (PSIRT), with documented processes and service level agreements that customers and others can easily locate and call to report product vulnerabilities.

The European Union Agency for Network and Information Security has published a Good Practice Guide on Vulnerability Disclosure.

#### *Secure Development Lifecycle (Gold)*

IoT Trust Label Endpoints are intended to be “trusted” by our customers and our partners. This includes the confidence and assurance that secure (and good) development lifecycle practices are followed in the development and maintenance of the product. IoT Ready vendors MUST have SDLC Process in place that includes the following elements at a minimum:

- Training for software developers which includes secure coding techniques and requirements standard C libraries.
- Threat modeling that includes a summary report of findings and a diagram.
- Software security testing thru either dynamic or static analysis tools and a report that demonstrates testing was completed and output of testing.

A way to document and track third party and open source components used in product.

A summary of the vendor’s specific SDLC process MUST be available on their public facing webserver.

While this requirement is listed as Gold, it is highly recommended for all IoT Label certification levels.

Normative Reference: NIST Security Considerations in the System Development Lifecycle

#### *Data Privacy – Right to Erasure (Bronze)*

The manufacturer MUST support the capability for the erasure of end user data at either a point in time when the data no longer provides value for the purpose for which it was collected or the end user withdraws consent for the processing of the data.

A set of normative references for this requirement are GDPR and Article 17 – Erasure.

#### *Data Privacy – Pseudonymization (Gold)*

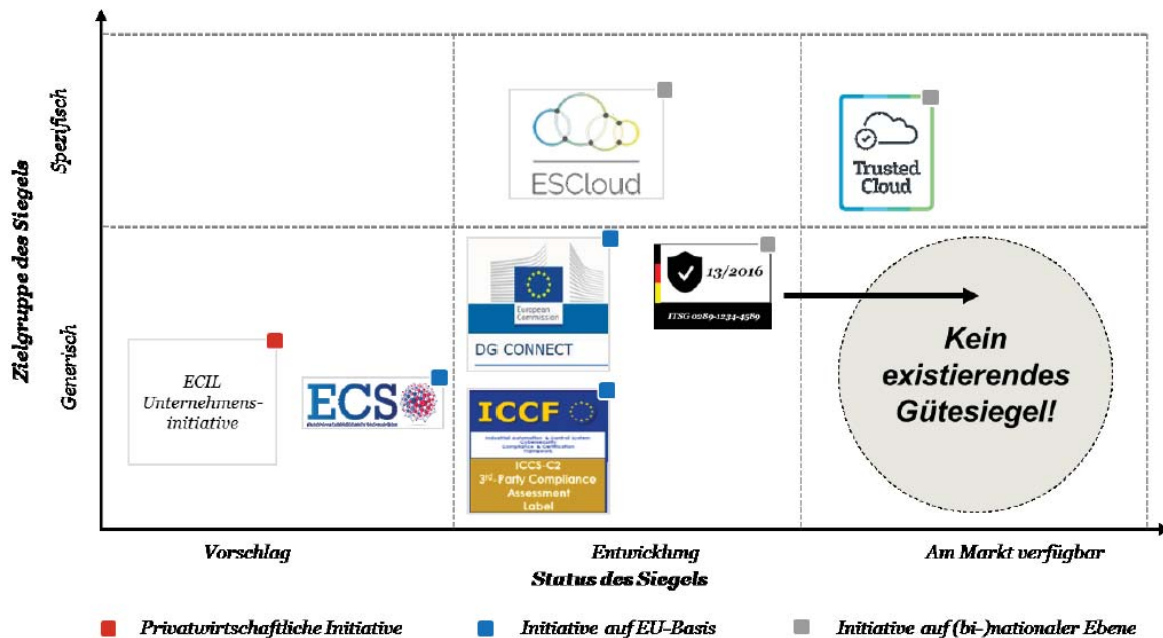
The manufacturer MUST support the use of pseudonymization as a process for protecting end user data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

A set of normative references for this requirement are GDPR and Article 6 – Lawfulness of Processing.

## 7.10 German Ministry of Interior – Study on “Introduction of a label of quality for IT security features of Internet-enabled products”

Right after the cyber-attacks of on hundreds of thousands Router of a German telecommunication group and the "Mirai"-Botnet Attack, IT security has become more and more important for the citizens. In order to face these threats, the Cyber security strategy of the Federal Government included the introduction of a quality label for IT Security in 2016. To do so, the Federal Ministry of the Interior asked PwC Strategy& to do a research on this topic. In their study, PwC Strategy& organized a representative survey specifically designed for consumer side and set direct interviews with IT manufacturers, in order to understand their interest and potential necessity for an IT Security Certification.

The necessity of this Certification also comes from the fact that the EU suggested the Member States to increase Cyber Security levels and at the moment the only label initiatives at European level are still at a launch stage (see Trusted Cloud label “and “label ESCloud). Therefore, the IT Security label could function as a pioneer for a European solution.



### Customer’s Survey

PwC Strategy& collected information from the consumer’s side through a survey to which 1.022 interviewees answered in the period from the 2nd to the 8th February, 2017. Their age ranged from the age of 18 to 69 years old.

Through the survey PwC Strategy& discovered that:

- On security information: 90% of the interviewees would like to receive more information about the security of their IT devices
- On the buying decision:
  - 91% of the interviewees considered the Security of the Device important at the moment of purchase
  - 70% of the customers is influenced positively by the presence of a security label.



- More than 65% of the customers would be in favor of paying a higher price for security labelled product

As a consequence of these results, PwC Strategy& found out that an IT security label would be a demarcation characteristic feature from the "less protected" products.

According to consumer's priority, the products that should be labelled for their Security are computer and laptop (> 83%), followed by Smartphones and Tablets (82%), while smart Home and electrical appliances and wearables are less relevant.

#### Im Auftrag des Bundesministeriums des Innern

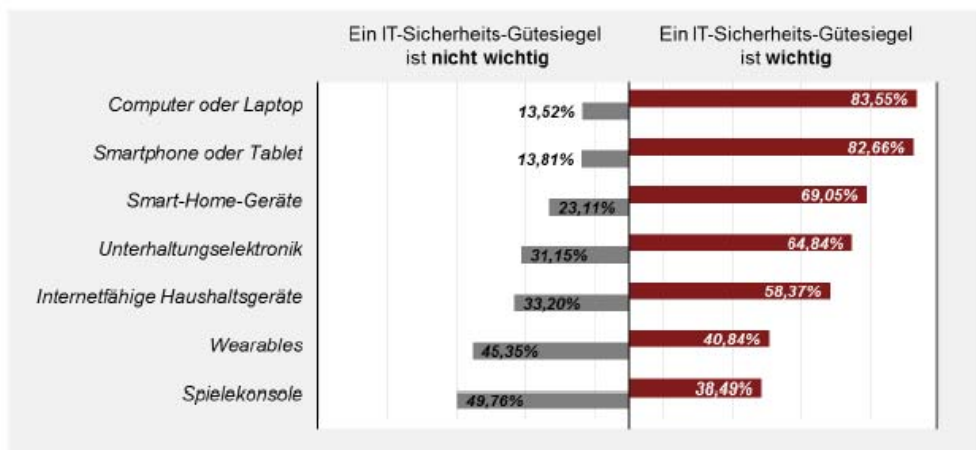


Abbildung 4: Interesse an einem IT-Sicherheits-Gütesiegel nach Produktgruppen

According to the responsibility of who should assure the security of the products, it was discovered that:

- Nearly 90% of the interviewees believe that the responsibility for IT security depends on the manufacturers.
- Only 61% see the government (state) as the responsible authority with the obligation for IT security.
- More than 82% of the interviewees think that the IT Security Label should come from State promoted institute
- Only 44% believes that the label should be a responsibility of a private test institute
- A majority of the interviewees considers that the assignment of the security label should not depend from private-economic institutions (57%).

#### Manufacturer's interviews

PwC Strategy& asked the opinion of 18 relevant manufacturer's enterprises and five groups of the IKT branch on the IT security label, in the period from the 1st February to the 7th April, 2017.

What they found was:

On the importance of IT Security label for the company

- IT security is a central factor in the product development
- Manufacturer with higher prices don't want to endanger their brand by a possible security gap in their IT devices
- Only very much few enterprises know or use existing security labels in the area of IT security with end user's focus
- If the IT security label would guarantee a uniformed standard at European levels, manufacturer interest would increase remarkably

- Enterprises have a bigger interest in an IT Security label in the middle price segment of the market

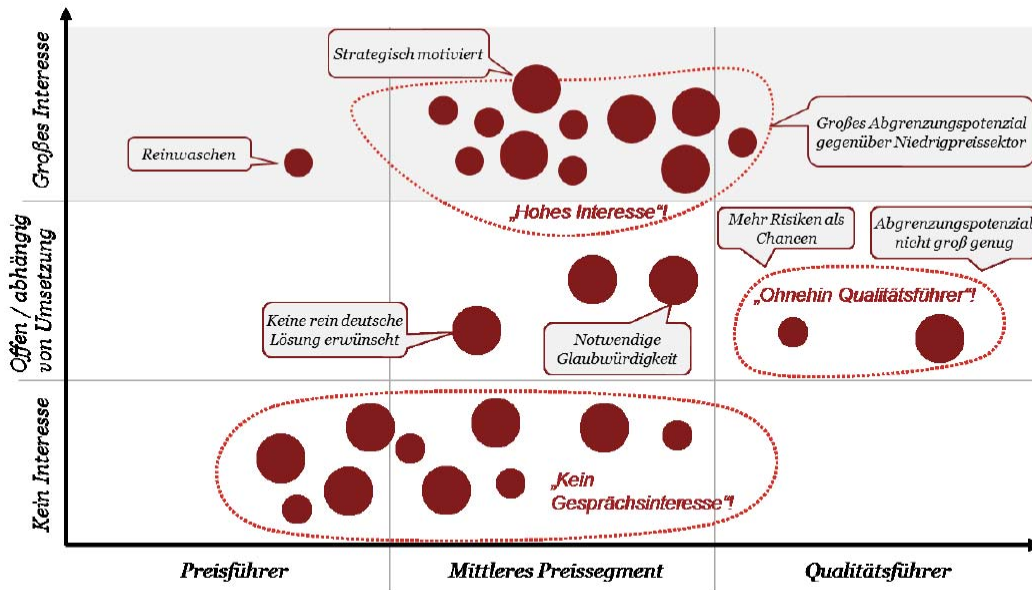


Abbildung 5: Einordnung der Hersteller hinsichtlich Interesse und Preissegment

### Challenges for the certification:

- The certification would guaranty IT security only for a limited period of time, since there always newer security threats.
- The security label would be only an indication, not a proof. In some cases, the
- Enterprises can guarantee no IT security for a certain period in this frame, but minimize only risks or conclude (close) recognized security gaps. The consumer has in fact partial responsibility on the security of the IT device.
- IT devices have multiple components such as hardware, software and apps. It is important to clarify where the security label applies.

### Patronage of the certification

Since the BSI would be the responsible for the definition of the criteria, they will have to cooperate with the manufacturers and the consumers' protectors. The responsible ministries can also cooperate. Even though the BSI is the distributor of the label, the security tests can be done in other external structures.

## 7.11 Cyber Risks and Cyber Resilience of Critical Infrastructures

European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State. This includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors<sup>55</sup>.

In the last years, the dependence of critical infrastructures from cyber space has become increasingly important. Europe and the entire world is experiencing a massive growth in connected cyber-physical infrastructures – ranging from IoT-based smart environments to critical infrastructures such as power grids, energy, water and manufacturing systems.

The number of connected devices is expected to grow to tens of billions by the year 2020. Very large cyber-physical infrastructures are envisioned which will integrate multiple applications run by a variety of stakeholders within a shared fabric. Examples include future industrial environments, infrastructure monitoring technologies and intelligent transportation systems. In such contexts, thousands of nodes will be deployed and used by a large number of stakeholders to provide a multitude of services. Such shared fabrics will remain in operation for a long time (potentially decades) and the physical composition, the services provided and the stakeholders involved will change with time.

In a survey of critical infrastructure organisations in the United States (US), the United Kingdom (UK), France, and Germany, 48% of respondents expressed that it would be likely for a cyber-attack to take down critical infrastructure with the potential loss of life<sup>56</sup>. The scale of future cyber-physical infrastructures and their dynamic nature in terms of stakeholders, services and physical properties over long time periods poses unique security and resilience challenges<sup>57</sup>.

In the following paragraphs, four critical infrastructures sectors will be analysed to underline problems, risks and resilience due to the dependence from cyber space.

### *Energy Sector*

New energy technologies such as renewable generation, electricity storage and electric vehicles will have far-reaching social and economic benefits. These transformations, however, depend upon the employment of 'smart' technology, which underpins other digitalisation strategies to deliver the benefits associated with smart cities, health, transport and logistics.

The smart energy system is therefore created through the significantly greater use of ICT in the digitalisation of energy production and distribution. The resulting energy transformation will see increasing decentralization of the energy system and greater inclusion of the consumer across the energy value chain.<sup>58</sup> It is essential to maintain equilibrium in critical infrastructure such as energy, which supports and sustains other critical infrastructure. A power outage often has serious consequences due to the cascade effect, inevitably affecting other sectors and their infrastructure<sup>59</sup>. The Ukraine power grid attack<sup>60</sup> in 2015 demonstrated the potential impact of cyber-attacks to the electricity subsector. This well-planned hack on 3 power-distribution companies caused outages to 80,000 energy customers.

The focus of cyber security in the energy sector is to support the reliability and resilience even in the event of a cyber-attack. Unlike IT systems, a control system in the energy sector that is under attack cannot be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts.<sup>61</sup> The scale of the threat to energy cyber security is massively increasing as energy systems develop ubiquitous intelligence and communications capabilities throughout their operations. In addition, development of a cost effective low carbon energy system across the EU will require a more distributed energy system, whilst also employing increased inter-connection and cooperation across national boundaries.<sup>62</sup> At the same time, demand for energy is always on the rise. As the German government put it,

<sup>55</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN>

<sup>56</sup> The Aspen Institute and Intel Security, 2015: Critical Infrastructure Readiness Report: Holding the Line Against Cyber threats

<sup>57</sup> Awais Rashid, Wouter Joosen, Simon Foley, *Security and Resilience of Cyber-Physical Infrastructures*, Lancaster University Technical Report No: SCC-2016-01

<sup>58</sup> [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL\\_STU\(2016\)587333\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf)

<sup>59</sup> <http://www.osce.org/secretariat/103500?download=true>

<sup>60</sup> Analysis of the Cyber Attack on the Ukrainian Power Grid, Defense Use Case, March 18, 2016, SANS ICS and E-ISAC.

<sup>61</sup> [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

<sup>62</sup> [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL\\_STU\(2016\)587333\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf)

“New solutions must be found that support the transition to liberalized markets, decentralized and volatile power generation structures, and electro mobility – while also ensuring the maximum possible level of cost-effectiveness, security of supply, and environmental compatibility.” In this context, the security of critical infrastructure is a core issue in national, international, and corporate security dialogue and policies.<sup>63</sup> Energy reliability at the European level relies on trans-European connectivity. A failure in one energy system can have a potential cascading effect across regions as shown in a major European blackout in 2006 caused by a planned disconnection of a transmission line.

Despite cyber security being a recent subject, a number of initiatives have already been conducted by Member States in order to enhance the country’s ability to face any attack. Member States need to learn about best practice from other sectors or other world regions that deal with highly sensitive information or are subject to cyberattacks on a regular basis. For example<sup>64</sup>:

- In **Denmark**, there is a close exchange of data between the transmission system operator (TSO), DSOs, generators and retailers via a data hub. Energinet.dk (TSO) is responsible for data security in relation to information exchange in the electricity market, but it has outsourced the security service to a third party;
- In **Norway**, companies are obliged to report major incidents (including cyber security incidents) to the national authority NVE. Apart from that, in 2014 Norway has set up “KraftCERT” (see <https://www.kraftcert.no/english/index.html>);
- In **Austria**, there is a public-private cooperation in order to set up (voluntary) national security and safety standards for the power industry, carry out a risk assessment and develop an action plan to tackle these risks;
- In **France**, companies are about to be obliged to report large cyber security incidents to the national cyber authority, ANSSI. There is also a CSPN certification for black box testing of product security level. However, there is a lack of mutual recognition with other Member States: no market for suppliers, therefore no incentive for certification. That is why it has been mainly used only by Small and Medium Enterprises (SMEs) so far;
- In **Sweden**, there is a long tradition of cooperation between the energy sector and the responsible authorities regarding all security matters. A common security website for the energy sector ([www.energisakerhetsportalen.se](http://www.energisakerhetsportalen.se)) has been developed where all relevant information is gathered;
- In **Portugal**, the National Cyber security Center (CNCS), part of the National Security Authority, ensures effective crisis management, coordinates the operational response to cyberattacks, develops national synergies and enhance international cooperation in this field. It has been developing a number of initiatives closely related to the energy sector;
- In **Germany**, the national IT-Security Act came into force in June 2015. Since May 2016, operators of critical infrastructures in the energy sector are obliged to report network and information security incidents that may have a disruptive effect on the provision of their service. In addition to that, all DSOs and TSOs need to fulfill a catalogue of IT-security measures and implement an Information Security Management System (ISMS) compliant with ISO/IEC 27001. Electricity generation plants that have been identified as critical infrastructures will need to fulfill a different catalogue of IT-security measures that is currently being drafted by the national regulatory authority.”

Ensuring resilience of the energy supply systems against cyber risks and threats are becoming increasingly important as widespread use of ICT and data communication is becoming the foundation for the functioning of infrastructures underlying the energy systems. The increased efficiency in supply services comes with a price: increased exposure to cyber incidents and attacks. In a cross-sector manner, these threats apply to all generation, transmission, distribution and process technologies, and to energy market services.

The digitalization of the energy sector also raises the question of how to face the risks and threats of cyber incidents and attacks affecting personal data and strategic energy infrastructure data, which are sometimes crucial for the security of the energy supply.<sup>65</sup>

<sup>63</sup> <http://www.osce.org/secretariat/103500?download=true>

<sup>64</sup> [http://www.eemg-mediators.eu/downloads/Report\\_on\\_smart\\_grid\\_cyber\\_security\\_20.12.2017.pdf](http://www.eemg-mediators.eu/downloads/Report_on_smart_grid_cyber_security_20.12.2017.pdf)

<sup>65</sup> [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

---

## Transportation Sector

The integration of several ICT systems for water transport, railways, airports and intelligent public transport, where cyber-physical devices, communication networks and central servers optimise the transport service up to a certain degree of automation, it also has the effect of introducing cyber security risks into transport networks that have not historically been susceptible to such risks. A total of 81% of large businesses and 60% of small businesses suffered a cyber security breach in the past year. €700,000 – € 1,30 million is the averaged cost to a large organisation<sup>66</sup>.

Some examples of cyber risks for the transportation sectors are related to: Physical asset damage and associated loss of use, unavailability of IT systems and networks, loss or deletion of data, data breach leading to the compromise of third-party confidential information including personal data, cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information<sup>67</sup>. Risks for railway comes for example when informational systems are attacked leading to unavailability of services for the passenger, like being unable to buy a ticket or digitally check a ticket into the system<sup>68</sup>.

For Smart airports, the introduction of new components and functionalities to facilitate the infrastructure-to-passenger interaction and vice-versa paves the way for new attack vectors or pathways and exposes airport assets to a larger attack surface. These risks include vulnerabilities in ICT and electronic systems as well as the information and data held and processed by such systems. Vulnerabilities can be exploited by malicious actions, but also human errors, system or third party failures and natural phenomena.

Therefore, it is imperative to put in place a collaborative model to set goals and define an appropriate cyber security approach to strengthen the aviation system's resilience against attacks. To this aim, significant effort is being invested across the aviation community at different levels, including standardization, security working groups, research and education. Identification of challenges posed by cyber threats, risk assessment approaches and guidelines to enhance cyber security, either in terms of high-level governance strategies or in terms of specific technological supports, are priorities currently tackled.<sup>69</sup>

## Finance Sector

For the Finance Sector, a complex set of interconnected networks allows real-time data exchange thus increasing the efficiency of communications, but, on the other side, it increases the risk of accessibility to confidential information and to critical systems able to control physical assets.<sup>70</sup>

Financial IT systems are exposed to a number of hazards which require consistent efforts to operate securely. In recent years, NIS risks have become more complex and their impact can range from low to very high, including domino effects. Such impacts will not be confined to the "virtual" world; a major attack outreach would most certainly impact the assets in safekeeping or in transit.<sup>71</sup>

Online financial services and lending companies are increasingly being targeted by fraudsters and costing consumers millions of euros around the world, according to research. Cyber-attacks against online lending companies and alternative payment systems increased 122% in 2016, according to ThreatMetrix, a security company that monitors more than 20 billion online transactions a year. The fraud is estimated to have cost consumers as much as 9 billion euros in 2016, the company said<sup>72</sup>.

ICT operators, intended as operators who directly manage Internet connections (such as Internet Service Providers and telecom operators), are directly involved in the cybersecurity issues and considered the most liable actors. Due to the fact that they manage ICT infrastructures and connected services, in the case of a successful cyber-attack, they would suffer the most direct consequences, but wide damages would also affect the rest of society.<sup>73</sup> A survey of 1,000 companies who have been victims of a ransomware attack, when cyber criminals lock all the files in a system and demand payment, revealed such breaches on average knock

---

<sup>66</sup> 2014 Information Security Breaches Survey: <http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf>.

<sup>67</sup> <http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf>

<sup>68</sup> <https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/>

<sup>69</sup> <https://www.enisa.europa.eu/publications/securing-smart-airports>

<sup>70</sup> Fabio Bisogni, Simona Cavallini, Sara Di Trocchio, Cybersecurity at European level: The Role of Information Availability, Fondazione FORMIT, 2011

<sup>71</sup> <https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector>

<sup>72</sup> <http://www.telegraph.co.uk/technology/2017/02/27/cyber-attacks-against-financial-services-cost-consumers-8bn/>

<sup>73</sup> Fabio Bisogni, Simona Cavallini, Sara Di Trocchio, Cybersecurity at European level: The Role of Information Availability, Fondazione FORMIT, 2011

systems down for a full week, costing up to €2,300 a day in lost revenue. Of the affected businesses, more than 250 paid over €5,700 for the safe return of their data. One third could not access their information for a month after the attack, while 15% said it was never recoverable<sup>74</sup>.

Moreover, Criminals have moved away from cracking metal safes and bank vaults. The money is now in their digital equivalents and these are proving vulnerable to the hackers and crackers of the codes of the digital world. The cryptographic codes of the digital world are extremely hard to break, but however hard these may be, they can be vulnerable to being bypassed. In the case of Bitcoin, the 'wallets' that hold the currency have proved vulnerable to theft — but the ledger itself has remained resilient, though in principle it would be vulnerable if over 50% of the computer processing power for the Bitcoin ledger fell into the hands of a single malevolent individual or organisation. Indeed, a great strength of distributed ledgers is that they should be highly resilient to attack.<sup>75</sup>

Against this background and according to the "SANS Financial Services Security" Survey<sup>76</sup>, most organizations operating in the finance sector need to be compliant with multiple mandates, which could also explain why so much of their budgets are being spent on compliance. Maintaining these compliance requirements requires automated tools to help identify overlaps in compliance reporting requirements as they monitor against multiple frameworks. Payment Card Industry Data Security Standard (PCI DSS), a requirement for processing credit cards, was cited by 50% of respondents as a mandate they adhered to. Other key mandates included Sarbanes-Oxley Act of 2002 (SOX, P.L. 107-204), a requirement for publicly traded companies (49%), and Gramm-Leach-Bliley Act, the Financial Services Modernization Act of 1999 (GLBA, P.L. 106-102; 47%), a requirement for financial institutions. In addition, approximately 37% adhere to the Bank Secrecy Act and 35% to Federal Financial Institutions Examination Council (FFIEC). Almost 45% of the respondents answered that their organization must be compliant also with State/Regional laws or rules governing financial services systems. Survey respondents also use a range of security frameworks and standards. The top two (49% each) were the ISO 27000 Series and PCI DSS for securing card payments. Credit card processors require card issuers and merchant banks to be compliant with PCI DSS as well as to use only service providers that also demonstrate compliance. In November 2013, the PCI Security Standards Council released PCI DSS version 3.0. Another common security framework is COBIT. Published by the Information Systems Audit and Control Association (ISACA), it is a business framework for the governance and management of enterprise IT.

Growing numbers of regulations are attempting to control the potential losses in the financial services industry. The amount organizations spend on meeting regulatory requirements is huge and is getting bigger. But, for every euro spent on completing a regulatory form, there is one less euro available for actually making systems more secure. There is room for legislative reform to move mature organizations away from being compliance driven to focusing on reducing attack surfaces, minimizing vulnerabilities and defending against threats.

## *Healthcare Sector*

Devices, system components and networks are becoming autonomous, ubiquitous and interconnected. When this technological advancement applies to the healthcare sectors, one of the most traditional critical sectors, the results are remarkable. Connected medical devices transform the way the healthcare industry works, both within hospitals and between different actors of the healthcare industry.<sup>77</sup>

In most countries an eHealth strategy exists, following the recommendation of the first EU eHealth Action Plan requesting the Member States to setup such policy documents to describe eHealth specificities, bodies involved and their responsibilities at a national level. Overall, eHealth infrastructures protection falls under the generic umbrella of CIIP.

Currently, there is no specific regulatory framework on critical eHealth infrastructure protection.<sup>78</sup> Not all MS consider eHealth as a critical sector; in some cases eHealth services formulate a different category of emergency services and are not classified as critical, in other cases healthcare ICT services are not considered critical as the environment is considered so isolated that any incident would have small impact. Instead, the complexity of eHealth systems is very high, which renders information quality (completeness, integrity),

<sup>74</sup> <http://www.telegraph.co.uk/technology/2017/02/27/cyber-attacks-against-financial-services-cost-consumers-8bn/>

<sup>75</sup> <http://www.ameda.org/files/gs-16-1-distributed-ledger-technology.pdf>

<sup>76</sup> <https://www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690>

<sup>77</sup> <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals>

<sup>78</sup> <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services>

---

accessibility and availability a very challenging task. Emerging healthcare data sharing schemes like EHR (Electronic Health Records) or PHR (Patient Health Records) as well as cross-border scenarios further complicate the technological challenges and respective protection requirements.<sup>79</sup>

Another major issue affecting cyber security in the case of healthcare is the lifespan of medical devices and equipment. Medical devices like CAT scanners, MRI machines etc. can stay as part of a hospital for more than a decade. This means that new vulnerabilities arise as attackers become more sophisticated. Moreover, this shows that intensive focus should be given in the patching and updating management of these devices. The very thin line between usability and security is becoming now more transparent as patching comes second (or even lower) in priority especially as the machines might need to be available at any given moment.<sup>80</sup>

To provide some quantitative data, according to "Health care and Cyber Security: Increasing Threats Require Increased Capabilities"<sup>81</sup> report, the greatest vulnerabilities for the health sector come from: 65% External Attackers, 48% Sharing Data with Third-Parties, 35% Employee Breaches/Theft, 35% Wireless Computing, 27% Inadequate firewalls. Mature incident and vulnerability management processes are lacking in most organizations, and thus, daily threats are not even reported or managed effectively by many organizations. In fact, there were more than 700,000 hacking attacks in any given minute against healthcare organizations in the fourth quarter of 2016, according to a study of 450 providers around the world by the threat intelligence arm of cybersecurity vendor Fortinet<sup>82</sup>.

There is no getting around the huge financial results of a data breach<sup>83</sup>. According to Ponemon Institute's 2016 Cost of Data Breach Study, the average total cost of losing sensitive corporate or personal information is approximately 3,51 billion euros. Per stolen record, businesses and associations can spend anywhere between €130 and \$140, with health card information costing the most to lose, at \$311 per record.

The majority of data breach costs are associated with resolving the matter, as organizations must pay compliance fines and court fees, invest in forensic and investigation processes, and spend revenue on identity theft prevention services for customers or employees. Additionally, Ponemon's report noted that turnover of consumers directly impacts business costs, and from then on out, these organizations must spend more on customer acquisition as the reputational losses of a data breach last a long time.

Healthcare actors including hospitals need to anticipate, prepare for, and respond and adapt not only to incremental change but also to sudden disruption. In smart hospitals, achieving this is more challenging than in traditional hospitals because the number of components that could lead to and be affected by service unavailability is much higher. Moreover, with the constant increase in the use of ICT components/products applied to the healthcare sector, to make sure that security-related requirements from users as well as regulators are met, it is important to involve them into test design and execution at an early stage. In the healthcare context, hospitals should play a key role in the testing activities. For instance, cross-testing could be performed in a larger number of hospitals before products are released. Moreover, regular penetration testing and mock by through security companies are advisable to assess security levels. Mock attacks could also be useful for hospitals as they allow determining response times.<sup>84</sup>

---

<sup>79</sup> <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services>

<sup>80</sup> <https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/>

<sup>81</sup> <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf>

<sup>82</sup> <http://www.healthcareitnews.com/news/how-many-hacks-happen-every-minute-against-healthcare-more-700000-fortinet-says>

<sup>83</sup> <https://www.cloudmask.com/blog/the-cost-of-data-security-are-cybersecurity-investments-worth-it>

<sup>84</sup> <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals>

---

## 7.12 The Lack of Appropriate Standards and the Need for a Common International Approach

Standards and other standardisation publications are **voluntary** guidelines providing **technical specifications** for products, services and processes. Standards are developed by private standardisation organisations usually on the initiative of stakeholders who see a need to apply a standard. Although standards as such are voluntary, using them proves that your products and services reach a certain level of quality, safety and reliability. In some cases, standards are referenced in legislation as a **preferred way** or even as a **mandatory requirement** to comply with specific laws (i.e. safety legislation or interoperability requirements).

Nations are using standards to meet a variety of objectives, in some cases imposing standards that are competing and contradictory, or excessively restrictive and not interoperable. Standardizing processes and procedures is an essential part of achieving successful cooperation in a cross-border or cross-community environment. In the absence of standardization, both processes and communication can be rendered ineffective.

Standards play a key role in ensuring that security products can be put together into systems capable of detecting and responding to real events. In particular, standard interfaces and protocols make systems integration much simpler and allow products to interoperate in heterogeneous environments. Standardization of testing methods also makes it possible to compare security products in a meaningful manner ('benchmarking') and provides a means for the end user to assess new products or services.<sup>85</sup>

The rapid evolution of the IoT market has caused an explosion in the number and variety of IoT solutions. Additionally, large amounts of funding are being deployed at IoT startups. Consequently, the focus of the industry has been on manufacturing and producing the right types of hardware to enable those solutions. In the current model, most IoT solution providers have been building all components of the stack, from the hardware devices to the relevant cloud services or as they would like to name it as "IoT solutions", as a result, there is a **lack of consistency and standards** across the cloud services used by the different IoT solutions.

The increasing dependence on ICT goods and services in today's society emphasizes the need to ensure their security. ICT is responsible for economic growth in Europe and is at the core of daily life. With these positive developments also come with an increasing risk of ICT dependencies, disruption and failure as well. The question arises on who is responsible for ensuring cyber security and cyber resilience. This is not an easy question to answer as government, consumers, ICT providers, companies all have an equal stake in this field.

Within the study "Challenges of security certification in emerging ICT environments"<sup>86</sup>, five sectors have been selected to investigate in more detail and to consider a broad spectrum of different requirements and cases that could lead to certification drivers concerning these devices. The five sectors are Energy, ICT, Health Care, Rail Transport and Water Transport. The key finding is that every sector has its own functional and security challenges which makes the target of a common certification framework a challenge. The energy sector, for example, largely depends on real-time interfaces on process automation level to provide a stable and reliable electrical power supply. The need for more real-time data exchange is increasing due to the decentralization of the power grid, increasing penetration of renewables and further integration of markets. On the other hand, the health care sector largely depends on informational systems and interfaces, like centralized patient databases that are used by companies that provide healthcare. Automation takes place on small scale, for example at hospitals to provide health monitoring. Transportation is mostly about logistics and safety. Finally, trains on a track need to be able to communicate with the generic infrastructure, while for the water transportation a vessel contains automation systems from office automation to process automation concerning electric power supply and vessel control. At the same time, ICT becomes the common processing platform which supports all these different functional and security requirements. **This underlines the (increasing) need for a common approach on standards and frameworks for certification.**

When the EU launched the strategy for the Digital Single Market, which included cyber security, it also produced Directives on General Data Protection Regulation (GDPR) and Network and Information Security (NIS), to strengthen the protection of consumers. However, the general legal framework in the EU that applies to the sale of goods and services from ICT providers to consumers was not covered properly.

---

<sup>85</sup> <https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security>

<sup>86</sup> <https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/>



Fragmentation is still a major issue. **A single market following international standardization is necessary to ensure a consistent approach to the IoT and cybersecurity.** The development of national efforts that would lead to further fragmentation should be avoided, as it could hinder IoT technologies to unfold its economic and social positive impact<sup>87</sup>.

### *Energy sector*

In the progression to smart energy networks the IT and OT environments within energy utilities have become more interconnected and reliant upon one another. In addition, communication technologies and system heterogeneity are increasing the technological complexity of the energy networks. The security challenges of sub-systems, combined with an increasingly distributed and multi-functional environment, therefore only increases the energy system vulnerability and potential level of cyber threats. Smart grids are a relatively new concept and therefore experience or relevant information regarding security threats or incidents is minimal. As a result, many application-level protocols have been designed without adequate levels of intrinsic security mechanisms which fully address the impacts of a fully integrated smart energy network. A few examples<sup>88</sup> of resulting issues that have been identified include:

1. In 2014, a team of university researchers from Portugal, found a flaw in an encryption standard developed by the Open Smart Grid Protocol (OSGP) Alliance, intended to secure smart grid networks in the EU and adopted by the European Telecommunications Standards Institute (ETSI).
2. The UK' Government Communications Headquarters (GCHQ) in 2014, intervened in the UK's smart meter roll-out plans due to the proposed use of a single decryption key for all communications between smart meters and energy service providers. This approach created the potential for chaos across the network, as a single hacker could conceivably disable the entire population's electricity meters.
3. Similar concerns were raised from a study conducted by security researchers in Spain in 2014, where millions of network-connected electricity smart meters were deemed susceptible to cyber-attack due to lack of proper security controls.

Typically, protection concepts are prepared at the time of procurement of a system which may take under consideration the risks and threats known at this point in time. Threat and risks are evolving and those legacy systems and devices used in the network do not necessarily comply with up-to-date operational and/or security standards. This reflects one key challenge in energy systems today. Additionally, cyber security in a multi-vendor environment requires interoperability where components should rely on the same set of security standards and requirements used, but these requirements of course vary depending on the operational context.<sup>89</sup>

**The harmonization of security implementation across the European Union is not sufficiently addressed** as mainly the common base to rely on international standards and specifications is requested. Consequently, the **level of implementation is expected to be unequal** across European Union.<sup>90</sup>

As instance, the architecture of the smart metering infrastructure varies from country to country with the use of different applications (i.e. DLMS, Meters and More or OSGP), different communication technologies and different regulatory requirements<sup>91</sup>.

Protection of the energy grid is a collective responsibility of the respective operators and the Member States. However, the criticality and the interdependency of the grid require a harmonization of the protection of respective systems across the European Union. An appropriate tool to define and develop the protection level of an energy grid is the usage of a cyber security maturity framework, which should be defined at EU level and best based on international standards (e.g. ISO/IEC 27000 series). This would allow a flat assessment scheme against to which Member States and the EU can evaluate the maturity of security within the Member State and the EU and on which the overall resilience of the energy grid within the EU can be measured and assessed while avoiding a scattered view of the EU landscape. Examples of a maturity framework for the energy grid exist for example by the ES-C2M241 framework for electricity subsector or the ONG-C2M2

<sup>87</sup> [https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016\\_tcm56-102235.pdf](https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf)

<sup>88</sup> [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL\\_STU\(2016\)587333\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf)

<sup>89</sup> [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

<sup>90</sup> [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

<sup>91</sup> <https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/>

framework for the oil and gas subsector from the United States Department of Energy (DoE). An additional advantage of a maturity framework would be to enable and foster use of cyber insurance as one mechanism to cover potential damages by cyber-attacks and by the achievement of a higher maturity level that may result in a lower insurance cost.<sup>92</sup>

The current lack of standards for smart energy communication system design and integration increases the vulnerability of communications networks to cyber-attacks. Such standards and guidelines should in turn provide a basis for the development of a European certification scheme. These communication standards should include:

- a common reference architecture,
- technical and operational requirements for smart energy / grid applications and systems,
- remote updates and reconfiguration – providing for smart energy / grid communications systems that utilise updatable devices to dynamically and remotely update security applications,
- a reference risk assessment framework and methodology<sup>93</sup>

Another concrete example of lack of standards and common approach for the Energy sector regards the Virtual Power Plants. A Virtual Power Plant consists of a central IT control system and distributed energy resources (often renewable energy resources like solar, wind, hydropower, and biomass units) as well as flexible power consumers. By networking all participating units through a remote control unit, it establishes a data transfer between the central control system and the participating units. The central control system is then able to monitor, forecast, and dispatch the networked units.

Currently for the security of Virtual Power Plants, the VHPready standard is not mature and finalized yet, therefore there is currently no compliance scheme available. It is currently focusing on security rules and best practices imposed by other standards like IEC 62351<sup>94</sup>.

Looking at the nuclear energy sector, As no regulation for cyber security currently exist at EU level, **Member States often simply follow in their national approaches** on computer security principles and methods developed by the IAEA, which offers a set of cyber security standards supplemented by the voluntary possibility of an advisory service (IPPAS66) of IAEA on State's request. However, not all EU Member States have already an effective legislation and regulation developed or implemented, as can, for example, be seen from the detailed evaluation of the Nuclear Threat Initiative (NTI) on security conditions.<sup>95</sup>

### *Transportation Sector*

There is currently no common EU approach specific to either intelligent or standard public transport, or related framework that specifically address IPT cyber security needs. Potentially the proposed NIS Directive might have an impact on addressing elements of this gap, above all in relation to cyber threat reporting, but may need to be expanded to encompass requirements for IPT cyber security within both urban transport networks and national/international rail networks.

There is a lack of specific security standards for IPT that can address the specific context and security threats faced by IPT assets. Generic standards, such as the ISO27000 series, are not sufficiently useful for the complex reality of IPT and are poorly related to the security environment within which transport organisations interact and operate today. It is important that standards are able to accommodate new IPT functionalities and concepts as they become relevant, while being able to remain dynamic, extensible and flexible.

The lack of a dedicated cyber security standard for IPT is an obstacle to the adoption of good security principles by IPT operators, manufacturers and solution vendors. With the support of the EC and MS, the industry (private and public sector) should ensure the development and adoption of harmonised standards adapted to the particularities. One or several completing standards could be developed to cover cyber security from various points of views as it has been proposed in other domains (e.g. Smart Grids)<sup>96</sup>.

<sup>92</sup> [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

<sup>93</sup> [http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL\\_STU\(2016\)587333\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf)

<sup>94</sup> <https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments/>

<sup>95</sup> [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

<sup>96</sup> <https://www.enisa.europa.eu/publications/good-practices-recommendations>

---

Many of the component technologies that can deliver intelligent and resource-efficient mobility and energy production and use have already been developed. Now industry players from different sectors need to jointly develop and apply solutions that meet, for example, the demand for energy efficiency, alternative fuels and ICT in urban energy efficient applications. At the same time, risks related to the scale-up and integration of these solutions remain. They originate from and are related to regulatory uncertainties, risk averseness of public procurement concerning innovative solutions, the current absence of standards and the immature market for truly integrated energy, transport and ICT solutions, among other things<sup>97</sup>.

A concrete example where the lack of standards affect the Water Transport sector are the IMO mandatory requirements. IMO mandatory requirements for the electronic exchange of information on cargo, crew and passengers have been adopted by the International Maritime Organization (IMO) on 11/04/2016. These include standardized forms for the maximum information required for the general declaration, cargo declaration, crew list and passenger list; and agreed essential minimum information requirements for the ship's stores declaration and crew's effects declaration. Although standards and recommended practices relating to stowaways are updated to include references to relevant sections of the International Ship and Port Facilities' Security (ISPS) Code, the ISPS audits **do not currently address the cyber security aspect** of the electronic passenger lists<sup>98</sup>.

Given the highly interconnected and complex nature of transportation networks, there is the need for more sophisticated analysis tools that can capture asset interdependence and cascade-effects among all the involved assets and different stakeholders. These tools will help capture how interdependencies operate and will heighten impacts in order to develop procedures and policies to improve recovery.

Risk assessment methodologies that can deal with multiple networked stakeholders working in collaboration need to be developed. This requires a different mind-set for existing risk management approaches, which often begin by scoping a system (*i.e.* defining its borders) prior to a risk assessment based on the individual elements. However, in interconnected systems this clear border does not exist. To address this gap we need to redesign risk management systems/approaches so that they operate from a *stakeholder* perspective rather than *border* perspective<sup>99</sup>.

---

<sup>97</sup> <https://ec.europa.eu/digital-single-market/en/news/smart-cities-and-communities-european-innovation-partnership-communication-commission-c2012>

<sup>98</sup> ENISA, *Challenges of security certification in emerging ICT environments*, December 2016

<sup>99</sup> <https://www.enisa.europa.eu/publications/good-practices-recommendations>

---

## Financial Sector

The financial industry is more regulated and has more oversight than any other industry on the planet. However, fintech's do not face the same level of regulation, because they may not fall under FDIC, SEC, or any other number of federal and state agencies. Therein lies one of the major hurdles to regulation. The sheer volume of oversight agencies creates more complexity in trying to build a singular regulatory policy or framework for the industry. Financial institutions are more regulated, because of the calamitous disruption and financial instability that will ensue when not properly regulated. Fintech's create the same types of disruption and instability with data breaches and exposing customer data, because they are creating a larger attack vector for the organization utilizing their service offering.<sup>100</sup>

Sensor data analytics and, in general, big data technologies, are changing the provision of insurance and other financial services as new sources of data, alternative data, can be taken into account for risk scoring, pricing and for the provision of tailor-made products.

**The lack of security standardization in the Internet of Things (IoT) and sensor data analytics** is an example of a real challenge we are seeing nowadays and on which the EC and other regulators are beginning to be concerned. IoT manufacturers should increase security measures to protect data. There is also a lack of consensus on the security standards to be used among manufacturers or among countries like China, USA and Europe.<sup>101</sup>

Organizations in the industry also use fewer processes to analyse compromised systems, eliminate the causes of security incidents, and restore affected systems. The lack of security maturity, limited funds, and the low priority placed on security may be major factors for this trend.<sup>102</sup>

## Healthcare Sector

Mobile medical applications or wearable devices allow patient data to be collected. Health events can be captured or monitored and data connected to a private or public cloud. However, as more healthcare devices become network-aware, it becomes challenging for IoT companies to agree on common interoperability protocols and standards for sharing and protecting data, and for the hardware sensors that collect that data.

Many implantable medical devices have already wireless capabilities. Patients and care providers are becoming more and more security aware. Lack of standardization have triggered concerns and raised questions whether products fulfill safety and security standards like the ISO80001. The once seemingly futuristic exploit of implanted medical devices has been made present with the demonstration of successful attacks against devices such as the insulin pump and pacemakers. Research from the Archimedes, Ann Arbor Research Center for Medical Device Security at the University of Michigan has demonstrated the potential compromise to implanted devices. The lack of device embedded security controls is of greater concern than the incidents they result in. Research has demonstrated that issues such as web interfaces to infusion pumps, default hard coded administration passwords, access to the Internet through devices connected to internal networks, are just a few of the common vulnerabilities found in devices used in the hospital environment. Embedded web services, with unauthenticated and unencrypted communication are one of the biggest vulnerabilities, as an attacker can potentially affect these devices remotely from anywhere in the world.<sup>103</sup>

Security experts compare **the lack of standards to the wild days of the web of the '90s**. Today competing standards, vendor lock-in, proprietary devices and private networks make it hard for devices to share a common security protocol.

To that end, healthcare is a microcosm of the larger security challenges that face IoT. A lack of loyalty to one IoT common standard for connected devices in other business environments is one of a number of barriers that is holding back mass adoption broad IoT security protection, say security experts.

Gartner argues it's the sheer number of IoT use cases that contribute to a wildly divergent number of approaches to solve IoT problems, which creates interoperability challenges and, ultimately, security gaps<sup>104</sup>.

Recognition of the increasing vulnerability of medical networks, as well as medical devices connected to these networks, is reflected in the revisions to the international standard International Organization for Standardization (ISO)/IEC 27000-series "Information security management systems" and ISO/IEC 80001

---

<sup>100</sup> <https://tokenex.com/fintech-solving-problems-finance-introducing-risk-part-2-3/>

<sup>101</sup> [http://www.ebf.eu/wp-content/uploads/2017/06/EBF\\_026943-Fintech-consultation\\_EBF-response\\_15.06.2017.pdf](http://www.ebf.eu/wp-content/uploads/2017/06/EBF_026943-Fintech-consultation_EBF-response_15.06.2017.pdf)

<sup>102</sup> <http://www.cisco.com/c/dam/assets/docs/transportation-security.pdf>

<sup>103</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/>

<sup>104</sup> <https://www.nsslabs.com/company/news/media-resources/iot-insecurity-pinpointing-the-problems/>

---

“Application of risk management for IT networks incorporating medical devices”. However, consideration of the threat to the devices themselves and subsequently the resulting patient safety concerns are of greater concern when the connections are to wireless networks.

What complicates the security risks with medical devices is that these devices expose both data/information and potentially the control of the device itself. In addition, the cybersecurity discipline tends to take a risk approach to any problem. Traditionally security has been viewed as a technological solution space, and subsequently the change in the operating environment driven by technology such as wireless, has been focused on controlling the risk with technology. This perspective has gradually altered over time with acknowledgment that those practical security solutions in health care need to take a socio-technical approach. Further, for practical security solutions to be effective, research shows that they must, at the very least, consider clinical workflow, if not seamless integration with this workflow.

While there are a number of international standards that are pre-requisites for the certification of medical devices, these are limited to the development and design risk assessment process. **These standards do not focus on the specificity required for cybersecurity within the complex deployment setting.** However, since many security flaws and subsequent vulnerabilities are a consequence of poor software design, which may include medical device software.<sup>105</sup>

Considering the very sensitive nature of health data and the vulnerability and easy dissemination of information on electronic format, special attention should be paid to the security of data from EHRs. The Study<sup>106</sup> shows, however, that half of the countries covered have not set specific rules for institutions hosting and managing EHRs, relying instead on the general rules setting security requirements for all types of data controllers. In addition, almost all the countries covered have not gone beyond Directive 95/46/EC in what relates to authorisation requirements. The authorization procedure to host and process EHRs is, in the vast majority of countries, the same as to host and process other data. Also, only a minority of the countries has set specific auditing requirements for institutions hosting and managing EHRs.

A binding European legal framework on basic user and access management that should also include operational rules on other security aspects such as end-to-end encryption (currently not possible because of the lack of a common encryption standard) and audit trails (who will be in charge of recovering data events in case of an incident) should be adopted. Agreement is also recommended on a model service level agreement for cloud services with regard to EHRs. The eHealth Network should closely follow up the progress made in this context and stimulate the development of European model provisions for cloud SLAs dedicated for eHealth services and EHRs in particular.

Belgium has developed and uses a standard for the exchange of minimal medical transaction information, called SumEHR. The SumEHR standard was introduced in 2005 and an EHR software package used by a physician should be capable of exporting a SumEHR message for any given patient. Currently more than 80% of all GPs across Belgium use certified EHR systems with this capability. In Slovakia, health care providers are required to use certified information systems which comply with connectivity and security standards, as well as with rules on identification and authentication of health professionals. In Italy, the draft implementing decree and an annex thereto lay down specific provisions on interoperability.

---

<sup>105</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/>

<sup>106</sup> [http://ec.europa.eu/health/sites/health/files/ehealth/docs/laws\\_report\\_recommendations\\_en.pdf](http://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf)

## 7.13 Economics of Standards

Lack of mutual recognition in cybersecurity certification can be equated to an absence of common technical standards; by the same token having common certification criteria for cybersecurity in EU28 would amount to introducing new technical standards. The economics of standardisation in general<sup>107</sup>, and of ICT standards in particular<sup>108</sup>, show that technical standards have positive impacts on R&D and on economic growth. ICT standards embed knowledge that becomes accessible to all and firms can invest the resources released from having to go through multiple certification to R&D. ICT standardisation reduce costs (transaction costs and cost reduction), improve competition (using standards to organize markets) or communication and coordination (organizing the development of technology around agreed technical specifications) and in the long run creates selection efficiencies by pruning the tree of available technical solutions for any given problem and channelling R&D efforts in the most efficient directions. Not surprisingly, as mentioned in the SWD “A Single Market Strategy for Europe - Analysis and Evidence”<sup>109</sup> a large body of economic studies that show the impact that standards have on economic growth and GDP. For France the impact on growth is estimated at 0.8 %, for United Kingdom at 0.3 % and for Germany at 0.9 % of GDP. Furthermore, an economic paper by economists of DG ECFIN estimated that the cost associated to differences in technical rules and multiple testing/certification are between 2% to 10% of companies’ annual turnover<sup>110</sup>. According to this paper inadequate standards and insufficient mutual recognition, including in the ICT sector, is among the main barriers to the single market. The costs for enterprises of product conformity assessment can be substantial and where there is lack of mutual recognition this implies the multiplication of such costs: for companies offering several product types on a national market of a receiving Member State the costs amount to approximately 2% of their entire annual turnover on that market, whereas they can reach up to 10% for companies specialised in one specific product type because they do not benefit from economies of scale<sup>111</sup>. Even applying the lower bound of 2% only to 60% of the cyber security market to be conservative (i.e. assuming 40% of the market concerns products for which certification is not required) the costs of lack of mutual recognition reach a figure in the range of 1.2 billion euro.

<sup>107</sup> Among peer-reviewed journal articles see: Acemoglu, D., G. Gancia and F. Zilibotti (2012), ‘Competing Engines of Growth: Innovation and Standardization,’ *Journal of Economic Theory*, 147, 570–601; Blind, K. and A. Jungmittag (2008), ‘The Impact of Patents and Standards on Macroeconomic Growth: A Panel Approach Covering Four Countries and 12 Sectors,’ *Journal of Productivity Analysis*, 29, 51–60; Jungmittag, A., K. Blind and H. Grupp (1999), ‘Innovation, Standardisation and the Long-term Production Function,’ *Zeitschrift für Wirtschafts- und Sozialwissenschaften*, 119, 205–222; Wakke, P., Blind, K.; Ramel, F. (2016): The impact of participation within formal standardization on firm performance, *Journal of Productivity Analysis* 45 (Issue 3), 317–330; Wijen, F.H. (2014). Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. *Academy of Management Review*, 39 (3), 302-323. Swann, P. (2010), *International Standards and Trade: A Review of the Empirical Literature*. Report for the UK Department of Business, Innovation and Skills (BIS). OECD Trade Policy Working Papers. Among reports commissioned by standardization bodies see: SCC (2007). *Economic Value of standardisation*; AFNOR (2009). *The Economic Impact of standardisation*; DIN (2011). *The Economic Benefits of standardisation*; Standards Australia (2012). *The Economic Benefits of standardisation*; Cebr (2015). *The Economic Contribution of standards to the UK Economy*; Cebr (2016). *Economic Contribution of Standards in Ireland – A report for the National Standards Authority of Ireland*.

<sup>108</sup> Blind, K., Gauch, S. and Hawkins, R. (2010), ‘How stakeholders view the impacts of international ICT standards’, *Telecommunications Policy*, Elsevier, vol. 34(3)

<sup>109</sup> Brussels, 8.10.2015 SWD (2015) 202 final, accompanying the document *Upgrading the Single Market: more opportunities for people and business* (COM (2015) 550 final) {SWD(2015) 203 final}.

<sup>110</sup> Ilzkovitz, F. Dierx, A. Kovacs, V. & Sousa (2007) *Steps towards a deeper economic integration: the internal market in the 21st century*, *European Economy, Economic Papers*, No. 271. European Commission.

<sup>111</sup> *Ibid.* p. 61

## 7.14 References

- Baldini, G., Giannopoulos, G., & Lazari, A. (2017). Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.
- Akerlof, G. (1970). The Market for Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3), 488-500.
- ANSSI. (2015). Introduction A La Certification De La Sécurité Des Technologies De L'information Paris: Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI).
- ANSSI, & BSI. (2017). Towards a European certification scheme: Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) & German Federal Office for Information Security (BSI).
- BITAG. (2016). Internet of Things (IoT) Security and Privacy Recommendations. A Uniform Agreement Report: BROADBAND INTERNET TECHNICAL ADVISORY GROUP (BITAG).
- Business Insider. (2017). The Internet of Things 2017 Report.
- Codagnone, C., Bogliacino, F., & Veltri, G. (2013). Testing CO2/Car labelling options and consumer information. Final Report. Brussels: European Commission (available at: [http://ec.europa.eu/clima/policies/transport/vehicles/labelling/docs/report\\_car\\_labelling\\_en.pdf](http://ec.europa.eu/clima/policies/transport/vehicles/labelling/docs/report_car_labelling_en.pdf)).
- Codagnone, C., Veltri, G. A., Bogliacino, F., Lupiáñez-Villanueva, F., et al. (2016). Labels as nudges? An experimental study of car eco-labels. *Economia Politica*, 33, 403-432.
- CSIS. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Washington, D.C.: Center for Strategic and International Study (CSIS).
- Dusart Pierre, Sauveron Damien, Tai-Hoon Kim, Some limits of Common Criteria certification, *International Journal of Security and Its Applications*
- DIGITALEUROPE. (2017). DIGITALEUROPE'S views on Cybersecurity Certification and Labelling Schemes. Brussels: DIGITALEUROPE.
- ECORYS. (2011). Security Regulation, Conformity Assessment & Certification. Brussels: Report delivered by ECORYS for the European Commission.
- Enisa. (2014). Smart grid security certification in Europe. Challenges and recommendations: European Union Agency for Network and Information Security (ENISA).
- Enisa. (2016a). Results of ENISA workshop on a common European ICT product security certification framework (February 2016): European Union Agency for Network and Information Security (ENISA).
- Enisa. (2016b). A European ICT Security Certification Framework - Workshop Summary (17 October 2016): European Union Agency for Network and Information Security (ENISA).
- ERNICIP. (2014). Proposals from the ERNICIP Thematic Group, "Case Studies for the Cyber-security of Industrial Automation and Control Systems", for a European IACS Components Cyber-security Compliance and Certification Scheme.
- European Commission. (2006). Labelling: competitiveness, consumer information and better regulation for the EU. Brussels: DG Sanco, European Commission.
- European Commission. (2009). Impact Assessment Guidelines. SEC(2009) 92, Brussels: European Commission, available at: [http://ec.europa.eu/governance/impact/commission\\_guidelines/docs/iag\\_2009\\_en.pdf](http://ec.europa.eu/governance/impact/commission_guidelines/docs/iag_2009_en.pdf).
- European Commission. (2012a). Security Industrial Policy. COM(2012) 417 final, Brussels: European Commission.
- European Commission. (2012b). Commission Staff Working Document Accompanying the Communication on Security Industrial Policy. SWD(2012) 233 final, Brussels: European Commission.
- European Commission. (2015a). Commission Staff Working Document, Better Regulation Guidelines. Brussels, COM(2015) 215 final, SWD (2015) 110 final.
- European Commission. (2015b). A Digital Single Market Strategy for Europe. COM(2015) 192 final, Brussels: European Commission.
- European Commission. (2016a). Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2016) 410 final, Brussels: European Commission.
- European Commission. (2016b). Staff Working Document. Contractual Public Private Partnership on Cybersecurity & Accompanying Measures. SWD(2016) 216 final, Brussels: European Commission.
- European Commission. (2016c). Staff Working Document. Report on the public consultation and other consultation activities of the European Commission for the preparation of the EU Cybersecurity contractual Public-Private Partnership and Accompanying Measures. SWD(2016) 215 final, Brussels: European Commission.

- European Commission. (2016d). Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation. C(2016) 4400 final, Brussels: European Commission.
- European Commission, SWD(2016) 216 final, Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry
- European Commission. (2017). Building a European Data Economy. COM(2017) 9 final, Brussels: European Commission.
- Friedman, C. (2015). Cybersecurity workforce shortage: Millions of experts needed, <http://www.ksat.com/news/cybersecurity-workforce-shortage-millions-of-experts-needed>.
- Hunstad, A.; Hallberg, J.; Andersson, R., "Measuring IT security - a method based on common criteria's security functional requirements," Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC, pp. 226-233, 10-11 June 2004, URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1437821&isnumber=30958>
- IDC. (2009). The European Network and Information Security Market Brussels: Report delivered by IDC for the European Commission.
- Iizkovitz, F., Dierx, A., Kovacs, V., & Sousa, N. (2007). Steps towards a deeper economic integration: the internal market in the 21st century. Brussels: . European Commission, European Economy, Economic Papers, No. 271.
- ISACA. (2015). 2015 Global Cybersecurity Status Report: ISACA.
- Lunn, P. (2015). Are Consumer Decision-Making Phenomena a Fourth Market Failure? *Journal of Consumer Policy*, 38(3), 315-331. doi: 10.1007/s10603-014-9281-1
- OECD. (2013). Exploring Data-Driven Innovation as a New Source of Growth. Paris: OECD.
- OECD. (2015). OECD Digital Economy Outlook 2015. Paris: OECD.
- NIST. (2010). Guide for Applying the Risk Management Framework to Federal Information Systems. Washington DC: National Institute of Standards and Technology (NIST), US Department of Commerce
- Norton. (2016). Cyber Security Insights Report: Symantec.
- Optimity Advisors. (2015). Study on Synergies between the civilian and the defence cybersecurity markets Brussels: Report delivered by Optimity Advisors for the European Commission.
- PwC. (2015). Cyber Security M&A Decoding deals in the global Cyber Security Industry: <https://www.pwc.com/gx/en/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf>.
- Schierholz, R., & McGrath, K. (2010). *Security Certification – A critical review*. ABB by DHS.
- Symantec. (2017). Internet Security Threat Report: Volume 22, Symantec.
- Thales, P. (2016). Introduction to the European IACS components Cybersecurity Certification Framework (ICCF). JRC Science for Policy Report. Luxembourg: Publications Office of the European Union.
- Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118-136. doi: 10.1080/1369118X.2016.1186713
- ZVEI. (2017). Benefits and limitations of certifications and labels in the context of cyber security: German Electrical and Electronic Manufacturers' Association (ZVEI).





Brussels, 13.9.2017  
SWD(2017) 500 final

PART 6/6

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT**

*Accompanying the document*

**PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF  
THE COUNCIL**

**on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013,  
and on Information and Communication Technology cybersecurity certification  
("Cybersecurity Act")**

{COM(2017) 477 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

**Annex 8:**

**JRC Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe**



JRC SCIENCE FOR POLICY REPORT

# **Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe**

Gianmarco Baldini, Georgios  
Giannopoulos, Alessandro Lazari

2017

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

**Contact information**

Name: Gianmarco Baldini  
Address: Via Enrico Fermi 2749  
Email: gianmarco.baldini@jrc.ec.europa.eu  
Tel. : +39 0332 786618

**JRC Science Hub**

<https://ec.europa.eu/jrc>

JRC 105757

Luxembourg: Publications Office of the European Union, 2017  
© European Union, 2017

The reuse of the document is authorised, provided the source is acknowledged and the original meaning or message of the texts are not distorted. The European Commission shall not be held liable for any consequences stemming from the reuse.

How to cite this report: Gianmarco Baldini et al., Analysis and recommendations for a European certification and labelling framework for cybersecurity in Europe, JRC 105757, 2017

All images © European Union 2017

## Table of contents

Executive Summary .....	3
1 Introduction .....	5
2 Definitions .....	9
3 Existing certification schemes .....	11
3.1 International certification schemes.....	11
3.1.1 Common Criteria .....	11
3.1.2 The ISASecure Certification Programme.....	13
3.1.3 Information Technology Security Evaluation Criteria (ITSEC) .....	14
3.1.4 Federal Information Processing Standards FIPS-140 .....	15
3.2 National Certification schemes.....	16
3.2.1 French security certification scheme .....	16
3.2.2 German security certification scheme .....	16
3.2.3 UK certification scheme .....	17
3.3 Other initiatives .....	18
3.3.1 Industrial Automation and Control Systems (IACS).....	18
3.3.2 Common Criteria Recognition Arrangement (CCRA) .....	21
3.3.3 SOG-IS .....	21
3.3.4 UL 2900 certification. ....	22
3.3.5 Secure Change.....	22
3.3.6 EN50128. ....	22
3.3.7 IEC61508.....	23
3.3.8 ISO 27001/27002.....	23
4 Analysis of the existing certification schemes .....	24
4.1 Issues and challenges .....	24
4.2 Domains applicability .....	27
4.2.1 Specific aspects of the energy sector .....	27
4.2.2 Specific aspects of the automotive sector .....	28
5 A way forward for a European certification scheme .....	31
5.1 Drivers for a new European certification scheme .....	31
5.2 Key elements of the new European security certification scheme.....	32
5.3 Labelling .....	35
5.4 Security and Privacy certification .....	36
5.5 Accreditation and testing laboratories.....	38
5.6 Main roles .....	39
5.7 Functional Architecture .....	40
5.8 Trusted applications.....	40

5.9	Market surveillance and monitoring.....	41
5.10	Model based testing (MBT).....	42
5.11	Inherent risks and uncertainties .....	44
5.11.1	Obstacles to implementation .....	44
5.11.2	Potential negative effects.....	44
5.12	Recommendations .....	45
5.13	Policy Options .....	46
6	Conclusions.....	47
	References.....	48
	List of abbreviations .....	54
	List of figures .....	56
	List of tables .....	57
	Annex: Report on the meeting of the experts on the 6 <sup>th</sup> of December 2016 .....	58
A.1.	Background.....	58
A.2.	Participants .....	58
A.3.	Agenda of the meeting.....	59
A.4.	Presentations and discussions .....	60
	Sergio Lomban: The view from the European Cyber Security Organisation of cPPP 60	
	Arthur van der Wees (Arthur Legal) .....	62
	Kai Rannenbergh (Goethe University Frankfurt).....	62
	Paul Theron (Thales) .....	64
	Philippe Cousin (Egloalmark), Bruno Legeard (Université de Franche-Comté): ARMOUR project for security certification in IoT and Model Based Testing .....	65
	Eireann Leverett of IOActive .....	66
A.5.	Discussion.....	68
A.6.	Conclusions of the meeting.....	71

## Document History

Version	Date	Comments	Modified Pages
0.1	04/07/16	First draft	Initial version
0.2	27/09/16	Second version	Updated sections 4,5,6.4 and 6.10 after phoneCall on 28/09/2016.
0.3	01/10/16	Third version	Updated section on privacy
0.4	15/10/16	Fourth version	Minor Comments
0.5	21/10/16	Fifth Version	Added considerations for the automotive sector.
0.6	22/01/2017	Sixth version	Added report of the meeting on the 6 <sup>th</sup> of December 2016
0.7	23/01/17	Seventh version	Added section on market monitoring.
0.8	31/01/17	Final version for internal review	Proof-read and other small checks
1.0	13/02/17	Final version	Changes after internal review.

## **Foreword**

This report has been prepared in the context of the Administrative Arrangement Id 34294 between the JRC and DG CNECT to investigate and propose recommendations for the establishment of a European ICT security certification framework and to assess the feasibility of a European cybersecurity labelling framework. The report has been prepared on the basis of inputs received from security experts, Senior Officials Group Information System Security (SOG-IS) and DG CNECT H.1 - Cybersecurity and Digital Privacy.



## **Acknowledgements**

We acknowledge the valuable input of DG CNECT H.1 colleagues Pierre Chastanet , Aristotelis Tzafalias and Domenico Ferrara, the colleagues of DG JRC E.3 Jean Pierre Nordvik, Igor Nai Fovino, Laurent Beslay and Ignacio Sanchez, the representatives of SOG-IS, ESCO-cPPP and AIOTI.

## Executive Summary

Security certifications such as ITSEC and Common Criteria are often used to certify products in several domains such as in the case of Intelligent Transport Systems or SCADA. An example of the potential process can be found in the Cooperative-ITS domain where the certification and labelling process for C-ITS communication systems and ITS platforms is a key element to support the safety of the users. Similarly, information security management certifications such as ISO 27001 are often used to certify business processes and are also widely deployed in the industry.

Although these certification schemes are deemed as appropriate in certain areas, they are often perceived as too complex and resources consuming by the industry specially when applied to SMEs, which do not have the needed resources to implement such schemes.

In the context of the Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (COM (2016) 410), this report analyses the current state of art on the security certification processes at international and national level, and provides recommendations and policy options to support the establishment of an European security certification and labelling framework. The report identifies the key issues of the security certification processes to be addressed and proposes and European wide framework for security certification and compliance that can be effective in the delivery of trust, whilst at the same time reduces the burden typically introduced by other certification schemes. The key elements of this European framework are identified and described. Finally, the report provides recommendations for the design and deployment of a European security certification framework.

The recommendations provided in this report include the following:

1. A European security certification scheme should be set-up to overcome the national differences.
2. The basis for the new European security certification scheme shall be based on the Common Criteria.
3. A process to define harmonized protection profiles for specific domains should be put in place with the collaboration of existing organizations like SOG-IS or agreements like CCRA.
4. The definition of harmonized protection profiles is the basis for the definition of a labelling scheme to support the comparability and visibility of the security certification for end-users.
5. Security and privacy requirements should be validated in the same certification process and with the same harmonized protection profiles.
6. A process to create accredited security testing centres should be defined. The experience from the Horizon 2020 Future Internet Research & Experimentation (FIRE) could be useful at least for the IoT related products.
7. A post certification framework to support the lifecycle of products and to mitigate gaps in the security certification process and execution should be investigated and deployed.
8. The application of testing models and automated testing suites should be investigated in security certification to improve the efficiency of the security certification process and to address the issue of re-certification after product changes.

This study has been done taking in considerations other existing initiatives at European and national level in security certification and the current wider European regulatory

framework for conformity and compliance of products. Various meetings have been organized with SOG-IS and security experts in 2016, which are reported in DG JRC progress report JRC105854. A specific meeting was organized on the 6<sup>th</sup> of December 2016 with security experts to discuss together the main elements of the security certification framework and receive feedback on the priorities or feasibility of the proposed elements. A report of the meeting is provided in the Appendix.

Beyond security, the report does also take in consideration the certification of product against privacy requirements, especially in the prospect of the new Data Protection Regulation. We consider security and privacy closely related because security mechanisms can and should also be used for privacy protection (e.g., data confidentiality).

As preliminary set of policy options are described at the end of this report in section **Error! Reference source not found.** and they are briefly summarized here:

- a) Encouraging and supporting the certification scheme. This option envisages the Commission using various soft measures to stimulate and encourage the adoption of security certification in Europe.
- b) Definition of harmonized standards and protection profiles at European level. This option envisages the setting up of organizations and entities or the empowering of existing entities like SOG-IS and ETSI/CEN/CENELEC to define sets of harmonized protection profiles, without enforcing on the manufacturers binding measures.
- c) Full regulation. This option envisages a full regulatory approach to secure certification for specific domains or applications.

# 1 Introduction

Certification has been defined in various ways in literature. In this document, we define certification as “A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system”. This definition is extracted from NIST SP 800-37 (NIST 2010).

Security certification is needed to ensure that a product satisfies the required security requirements, which can be both proprietary requirements (i.e., defined by a company for their specific products) and market requirements (i.e., defined in procurement specifications or market standards). In the latter case, these requirements are also defined to support security interoperability. For example, to ensure that two products are able to mutually authenticate or to exchange secure messages.

Security certification is needed to ensure that products are secure against specific security attacks or that they have specific security properties.

Note that in the rest of this report, the term security certification does also include certification of a product or a system against privacy requirements. We believe that the privacy certification should be part of security certification and it can be addressed with the same certification process by including additional test suites and certification steps. Further details on this aspect are described in

The process for certification of a product is generally summed up in four phases:

1. Application. A company applies a product for evaluation to obtain a certification.
2. An evaluation is performed to obtain certification. The evaluation can be mostly done in three ways: a) the evaluation can be done internally to support self-certification. b) The evaluation can be performed by a testing company, which is legally belonging to the product company. c) It can be third party certification where the company asks a third party company to perform the evaluation of its product.
3. In case of an internal company or a third party company evaluation, the evaluation company provides a decision on the evaluation.
4. Surveillance. It is a periodic check on the product to ensure that the certification is still valid or it requires a new certification.

As described in (Anderson 2009), the initial efforts to define a security testing and certification framework for products originated in the Defence domain. An obvious reason was that the military systems are designed to operate in a hostile environment and must be protected against security threats, which are more likely to appear than with those systems that belong to a commercial domain (even if we show in the subsequent sections of this report that the commercial environment has seen an increase of security threats for a number of reasons). In addition, there was the need to design a system able to support different access levels for classified and non-classified information and support interoperability. Through various phases, described in detail in (Lipner 2015), which will not be repeated here, these initial needs produced the Orange book, which provided criteria for classifying system security into a series of levels of products evaluation – C1, C2, B1, B2, B3 and A1 – depending on how carefully engineered were the mechanisms for assuring the confidentiality of classified information.

The different levels are provided in Figure 1.

D: Minimal Protection  
C1: Discretionary Security Protection  
C2: Controlled Access Protection  
B1: Labeled Security Protection  
B2: Structured Protection  
B3: Security Domains  
A1: Verified Design  
A2: Verified Implementation

*Figure 1 Levels of products evaluation in the Orange book*

Note that some of the levels (D,C1) could also be based on commercial product. At that time, mature commercial operating systems with reference to Unix were mentioned.

The Orange book was published in August 1983 and it became a requirement for ICT systems processing classified information at more than one level. As described in (Anderson 2009), while this was a valuable and needed process to support trust in government systems dealing with secure and sensitive information, the certification process was lengthy and costly. In fact, it could last 2-3 years. While, this was acceptable for the defence domain where a project or a product (e.g., a secure ICT system) could last for years and cost millions of dollars, this could be an issue for market distribution of a commercial product. The certification process also introduced a delay and certified products lagged behind the commercial state of art. In addition, the evaluation had to be performed by the National Computer Security Centre, a division of the NSA, a government agency.

A similar system was set up in Europe, which was called the Information Technology Security Evaluation Criteria (ITSEC), which eventually evolved to the Common Criteria, which is also known as ISO 15408. The Common Criteria is described in detail in section 3.1.1; here we want to identify some key elements and difference with the original Orange book.

In comparison to the Orange book, which was focused on protecting classified information, the Common Criteria is wider and permits systems and devices to be evaluate against a specific protection profile. In a similar way to the Orange book, Common Criteria also defines different levels of evaluation called Evaluation Assurance Levels (EAL) from 1 to 7.

A significant difference from the Orange book is related to the certification laboratories. As written before, the Orange book process involved a government agency for certification, while in the Common Criteria process, products can be evaluated by competent and independent licensed laboratories to determine the fulfilment of particular security properties (e.g., protection profiles) or a certain assurance level. This approach applies only to the lower assurance levels and the highest levels of certification are still performed directly by government labs.

The protection profile is based on Security Targets, which are the documents, which identify the security properties of the target of evaluation. For more details on the definition of the protection profiles, EAL and other elements of the Common Criteria see (CC 2016) and section 3.

As in the case of the Orange book, the process of evaluation using Common Criteria can be quite expensive and there is an ongoing discussion if some other process could be more suited to the commercial market.

An analysis of the issues and challenges for the certification scheme is presented in section 4.

In recent time, a certification scheme for Privacy seals has also been put in place by EuroPrise (<https://www.european-privacy-seal.eu/EPs-en/Home>). The workflow and standards for privacy certification have similarities to the security certification workflow.

A proposed joint certification process is proposed in the subsequent sections of the report.

This report provides a state of art on certification and labelling in different domains analyses and proposes more lightweight initiatives in the field of cybersecurity certification and compliance that can be effective in the delivery of trust whilst at the same time reduce the burden typically introduced by other certification schemes. In this context, lightweight does not mean that the security objectives should be addressed with minor attention but that some specific aspects of the security certification should be made more efficient.

To support the goal of a European certification and labelling scheme, two other aspects will be taken in consideration in this report:

- 1) the creation of a European networks of accredited certification centres, to support the certification scheme proposed in the report.
- 2) Exploitation of the existing conformity assessment processes for European products in general, where a regulatory framework has already been defined or it is being defined (EU 2008), the new Radio Equipment Directive (EU 2014) and the "Blue Guide" on the implementation of on the implementation of EU product rules 2016 (EU 2016)



## 2 Definitions

Accreditation	Accreditation shall mean an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity. (EU 2008)
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (NIST 2010)
CE marking	'CE marking' shall mean a marking by which the manufacturer indicates that the product is in conformity with the applicable requirements set out in Community harmonisation legislation providing for its affixing (EU 2008)
Compliance Assessment	Compliance assessment is an activity that helps to directly or indirectly identify the extent, to which a device or its constituent parts comply with the set of technical requirements, which must be validated to make the device operational. From an operational point of view, compliance assessment is an equipment authorization issued by a compliance assessment body based on representations and test data submitted by the applicant.
Conformance assessment	Conformance assessment means checking that products, materials, services, systems or people measure up to the specifications of a relevant standard.
Conformity assessment	Conformity assessment is the process carried out by the manufacturer of demonstrating whether specified requirements relating to a product have been fulfilled. (EU 2016)
Conformity / Compliance Testing	Conformance testing is the process used to determine whether a product or system complies with the requirements and/or functional specifications.
Declaration of Conformity	Declaration of Conformity is the conclusive step of a procedure where a responsible party makes measurements or takes other necessary steps to ensure that the equipment complies with the appropriate technical standards.
Manufacturer	Manufacturer shall mean any natural or legal person who manufactures a product or has a product designed or manufactured, and markets that product under his name or trademark. (EU 2008)
Protection Profile	A Protection Profile (PP) is a document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC)



Verification	Verification is a procedure where the manufacturer makes measurements or takes the necessary steps to ensure that the equipment complies with the appropriate technical standards.
--------------	--

## 3 Existing certification schemes

The aim of this section is to provide an overview of the existing certification schemes. In this section, we will also identify the key standards for risk analysis, certification and labelling.

### 3.1 International certification schemes

Here we describe the existing international certification schemes like Common Criteria.

#### 3.1.1 Common Criteria

The Common Criteria is also known as ISO 15408.

Common Criteria Certification provides independent, objective validation of the reliability, quality and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality and availability for systems and data, accountability at the individual level, and assurance that all goals are met.

The Common Criteria is a descendant of the US Department of Defence Trusted Security Evaluation Criteria (TCSEC) originally in the 1970s. TCSEC was informally known as the 'Orange Book'. Several years later Germany issued its own version, the Green Book, as did the British and the Canadians. A consolidated European standard for security evaluations, known as ITSEC, soon followed. The United States joined the Europeans to develop the first version of the international Common Criteria in 1994.

The first major CC release came in May 1998 with the release of CC 2.0 followed by version 2.1 in August 1999. CC parts 1-3 became an International Organization for Standardization (ISO) standard in 1999 (ISO/IEC 15408) followed by the CEM which became an ISO standard (ISO/IEC 18045) in 2005.

In 2007 the next significant version of the CC standard, version 3.1 was released. The current version is CC v3.1 release 4. Statistics provided by the CC international portal as of September 2014 list a grand total of 2,436 products have been certified using the Common Criteria standard (CC 2014).

The following key concepts are described here. They are extracted from (CC 2012) and (CC2014):

- A Target of Evaluation (TOE) is defined as a set of software, firmware and/or hardware possibly accompanied by guidance. While there are cases where a TOE consists of an IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these.
- A Protection Profile (PP) expresses an implementation-independent set of security objectives for a type or category of ICT product. It also specifies the security requirements and assurance measures which fulfil those objectives.
- A Security Target (ST) expresses security objectives of a specific ICT product and defines the functional requirements and assurance measures to fulfil those stated objectives. It also defines an implementation of the security requirements. The ST forms the basis for an evaluation and may claim conformance to one or more PPs.
- Evaluation Assurance Levels (EALs) are formed from a taxonomy of assurance classes, families, and components defined in CC standard Part 3. There are seven hierarchically ordered EALs increasing in assurance that serve to provide general-purpose assurance packages.

The EALs are defined in Figure 2.

EAL level	Description
1	Functionally Tested. Provides analysis of the security functions, using a functional and interface specification of the TOE, to understand the security behaviour. The analysis is supported by independent testing of the security functions.
2	Structurally Tested. Analysis of the security functions using a functional and interface specification and the high level design of the subsystems of the TOE. Independent testing of the security functions, evidence of developer "black box" testing, and evidence of a development search for obvious vulnerabilities.
3	Methodically Tested and Checked. The analysis is supported by "grey box" testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required
4	Methodically Designed, Tested and Reviewed. Analysis is supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.
5	Semi-formally Designed and Tested. Analysis includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure relative resistance to penetration attack. Covert channel analysis and modular design are also required.
6	Semi-formally Verified Design and Tested. Analysis is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure high resistance to penetration attack. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.
7	Formally Verified Design and Tested. The formal model is supplemented by a formal presentation of the functional specification and high level design showing correspondence. Evidence of developer "white box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimised.

*Figure 2 Definition of EALs from Common Criteria extracted from (ECORYS 2011).*

The international community has embraced the Common Criteria through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of Common Criteria evaluations performed by other CCRA members. The National Information Assurance Partnership (NIAP) was formed to administer a security

evaluation programme in the United States that utilises the Common Criteria as the standard for evaluation.

Common Criteria defines different roles (extracted from (CC 2012)):

- Consumers. The CC is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process. Consumers can use the results of evaluations to help decide whether a TOE fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different TOEs.
- Developers. The CC is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). This ST may be based on one or more PPs to show that the ST conforms to the security requirements from consumers as laid down in those PPs.
- Evaluators. The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out. Note that the CC does not specify procedures to be followed in carrying out those actions.

The common criteria approach is widely used in the world but it is also received criticism and suggestion for changes. See section 4.1 for additional details.

Proposal for changes to the existing Certification scheme has been raised by Chris Salter in (Salter 2011), where the following recommendations have been proposed:

1. To streamline and make more readable the common criteria documents themselves like the Protection Profile.
2. Definition of common *standard* protection profiles, which could be used for technologies and products, which have a similar set of features and they are subject to a common set of threats.
3. A tailored evaluation methodology has to be created for each technology area.

Some of the concepts from (Salter 2011) has been used in the new vision statement for the Common Criteria and CCRA is available at (CC 2012). One key aspect, which is also an element of the potential security certification scheme is the definition of collaborative Protection Profiles (“cPPs”) and supporting documents, in order to reach reasonable, comparable, reproducible and cost effective evaluation results.

### **3.1.2 The ISASecure Certification Programme**

ISCI (ISA Security Compliance Institute) is a not-for-profit organisation incorporated by ISA in 2006 to host certification, conformance and compliance assessment activities in the automation arena. The ISASecure certification scheme was derived from the framework of the ISA99 Standards Roadmap.

As described in (ISASecure 2016), ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities. The ISASecure program is based upon the IAC security lifecycle as defined in ISA/IEC 62443. At this time, the scope of the ISASecure certifications includes assessment of off-the-shelf IAC products and IAC product development security lifecycle practices. The overall schema of ISA/IEC 62443 is shown in Figure 3.

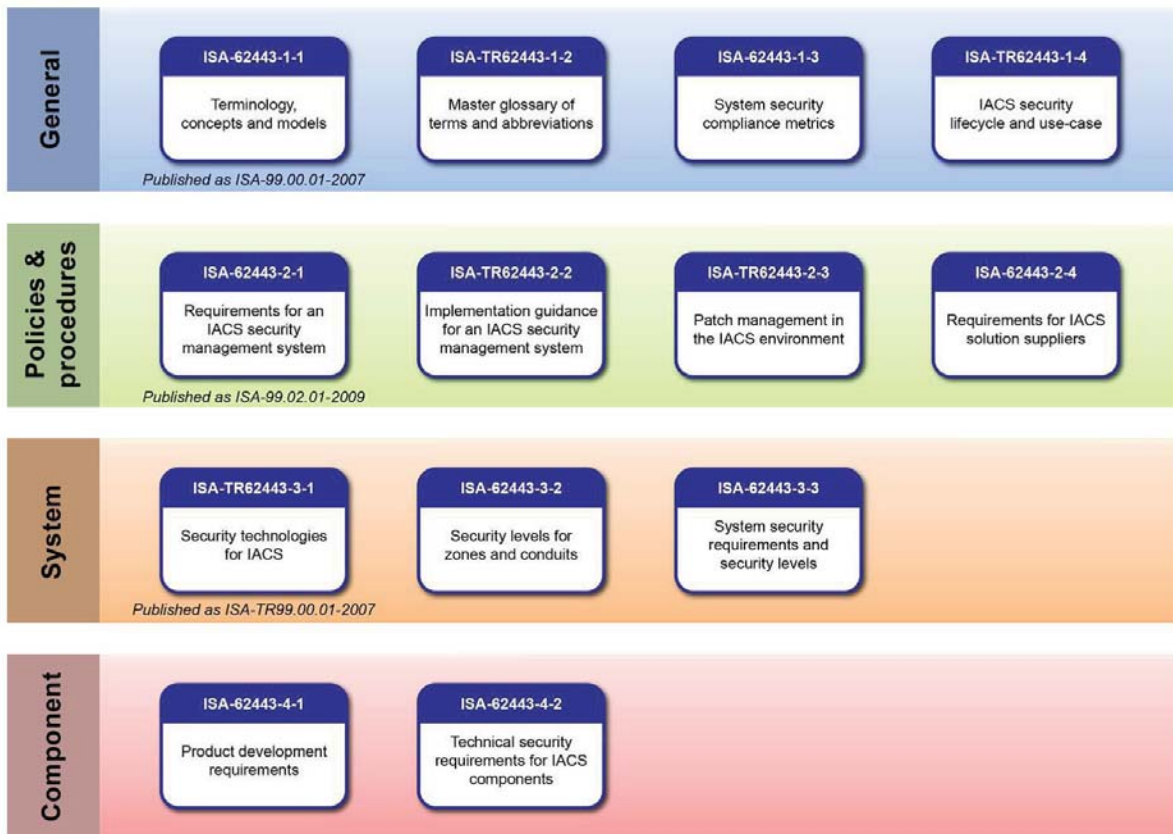


Figure 3 ISASecure certification scheme

The Security Development Lifecycle Assurance (SDLA) certification promotes security development lifecycle practices intended to improve the quality of security in IAC systems.

ISASecure does not offer assessments for integrator site engineering practices or asset owner operations and maintenance practices. ISASecure certifies off-the-shelf systems; not the site engineered / deployed systems.

ISASecure identifies four security assurance levels (SAL) as defined in ISA/IEC 62443.

### 3.1.3 Information Technology Security Evaluation Criteria (ITSEC)

The Information Technology Security Evaluation Criteria (ITSEC) was a structured set of criteria for evaluating computer security for IT products and systems. The ITSEC was first published in May 1990 in France, Germany, the Netherlands, and the United Kingdom based on existing work in their respective countries. Following extensive international review, Version 1.2 was subsequently published in June 1991 (ITSEC 1991) by the Commission of the European Communities for operational use within evaluation and certification schemes.

The ITSEC has been largely replaced by the Common Criteria and it will not be addressed further in this report.

### 3.1.4 Federal Information Processing Standards FIPS-140

The Federal Information Processing Standards (FIPS) are U.S. government computer security standards, which specify requirements for cryptography modules. The current version of the standard is FIPS 140-2, issued on 25 May 2001.

A brief history of FIPS-140 is following.

FIPS 140-1 was issued on 11 January 1994 and it was developed by a government and industry working group, composed of vendors and users of cryptographic equipment. The group identified four "security levels" and eleven "requirement areas" and specified requirements for each area at each level. The list of security levels and requirements areas is described below.

FIPS 140-2 was issued on 25 May 2001 and it is an updated version to take in account: a) the technology developments since 1994 in cryptographic technology and b) the comments received from the vendor, tester, and user communities. It was the main input document to the international standard ISO/IEC 19790:2006 Security requirements for cryptographic modules issued on 1 March 2006.

FIPS 140-3 is a proposed new version of the standard which is currently under development. It was initially scheduled for delivery in 2013, but the draft was subsequently abandoned. In the first draft version of the FIPS 140-3 standard, NIST introduced new features like software security section, one additional level of assurance (Level 5) and new Simple Power Analysis (SPA) and Differential Power Analysis (DPA) requirements. After the draft was abandoned, it is not clear if these new features will be maintained.

As described in (FIPS 2002), there are four security levels:

- 1) Security Level 1, which provides the lowest level of security. Basic security requirements are specific for a security module and no specific physical security mechanisms are required. An example of Level 1 cryptographic module is a personal computer (PC) encryption board.
- 2) Security Level 2 enhances the physical security mechanisms of security level 1 by adding the requirement of tamper evidence including seals or coating. The coating or seal must be broken to physically access the plaintext cryptographic keys. Security level 2 requires also a role-based authentication.
- 3) Security level 3 goes a step beyond level 2 by requesting to prevent the intruder from gaining access to the critical security parameters (CSP) held within the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that purges from memory all plaintext CSPs when the removable covers/doors of the cryptographic module are opened. In addition, security level 3 requires identity based authentication mechanisms, enhancing the security provided by the role based authentication mechanism specified in level 2.
- 4) Security level 4 provides the highest level of security in FIPS. At this security level, the physical security must provide a complete envelope of protection including the detection and response to all unauthorized attempts of physical access, which result in memory zeroing as in level 3. In addition, the cryptographic module must guarantee the same level of security even outside the normal environmental conditions for voltage and temperature.

In addition to the identified requirements, the different levels of security impose requirements on where the software and firmware components of the cryptographic module can be hosted and operate. More details are in (FIPS 2002).

While FIPS was designed specifically for cryptomodules, the scheme based on levels can also be adopted in other context, especially for the three main features of physical security, authenticated access control and hosting platform. Some of the concepts will be reused in this report in the following sections.

In relation to FIPS 140, FIPS 140-2 established the Cryptographic Module Validation Program (CMVP) as a joint effort by the NIST and the Communications Security Establishment (CSEC) for the Canadian government. CMVP validates commercial cryptographic modules to the Federal Information Processing Standard (FIPS) 140-2 and other cryptography-based standards.

## **3.2 National Certification schemes**

In this section, we will present the main European certification schemes at national levels. Only the main ones will be taken in consideration.

### **3.2.1 French security certification scheme**

The description of the French certification schema by ANSII is derived directly from the official ANSII document (ANSSI 2015).

The French Network and Information Security Agency (ANSSI) is responsible for examining certifications according to the directives given by the certification management committee.

The security certifications performed in France, regardless of the evaluation method and besides conformance claims verifications, systematically rely on intrusion testing to establish the security assurance level reached by the product.

Certification is based on evaluation studies conducted by laboratories licensed by the French Prime minister and accredited by the French accreditation committee (COFRAC) according to the standard NF EN ISO/CEI 17025. These laboratories are commonly referred to as Information Technology Security Evaluation Facilities (ITSEF). The evaluations are conducted in accordance with specifications or standards specified by the ANSSI.

Certification mainly addresses three types of objectives. It may be required to ensure compliance with regulations, such as European or national directives. Certification may also address a contractual objective, in cases where a customer from the public or private sectors requires such a certification. Finally, software vendors or industrials may want to differentiate from the competition by certifying their product (marketing objective).

Depending on the security needs expressed by the evaluation sponsors, the French certification scheme offers two types of evaluations:

1. The Certification de Sécurité de Premier Niveau (First Level Security Certification) is a predefined workload evaluation. Evaluation costs are therefore known in advance for a given type of product. The investment is quite limited, and the evaluation is mostly oriented towards intrusion testing, rather than conformity.
2. The Common Criteria evaluation allows to certify a product with various Evaluation Assurance Levels starting from EAL1 (basic attacker potential, script kiddie) up to EAL7 (high attacker potential) and takes into account the security of the development process.

### **3.2.2 German security certification scheme**

The German security certification scheme is described in detail in (BSI 2012).

The awarding of security certificates of IT products, protection profiles and sites is governed in the BSI.

The procedure is carried out at BSI in accordance with the quality management manual and the procedural instructions of the certification body and in accordance with the

standard DIN EN 45011, in accordance with the requirements of the international recognition arrangements (e.g., CCRA and SOGIS).

Certification is carried out as an application procedure. Following the preliminary assessment, the technical evaluation takes place based on the relevant evaluation criteria. The evaluation is performed by an evaluation facility approved by BSI and is technically monitored by the certification body.

The evaluation ends with a positive (pass) or negative (fail) evaluation result. The applicant is notified based on this vote. If the evaluation result is positive, the certificate and the certification report will be enclosed with the notice. The applicant may give notice of appeal against the notice.

In the case of a positive completion of the certification, the certification report will also be published on the BSI website, unless publication has been explicitly objected to.

Note that there are two types of certifications: system certifications and product certifications.

BSI uses the Common Criteria approach for certification. BSI develops protection profiles in order to define national security requirements in provisions for evaluation. Protection profiles are evaluated and certified in order to confirm their conformity with the concepts of the respective evaluation criteria.

### **3.2.3 UK certification scheme**

The UK security certification scheme is presented in (CESG 2016) and the following key concepts are extracted from that reference and provided here:

The evaluation criteria currently recognised by the UK certification scheme, and the methodologies associated with them, are:

1. the Common Criteria (CC) ISO/IEC 15408 and the Common Methodology For IT Security Evaluation (CEM) ISO/IEC 18045;
2. the IT Security Evaluation Criteria (ITSEC) and the IT Security Evaluation Manual (ITSEM)

CESG, as the UK's National Technical Authority for Information Assurance, operates the Scheme as part of its Industry Enabling Services (IES).

The UK security certification scheme presented in (CESG 2016) also identifies key roles. While this is background information, it is important to describe it here because similar roles will be adopted in the report:

- Senior management team. The CESG Senior Management Team provides the CB with top level direction, setting and reviewing policy and monitoring the performance of the Scheme overall.
- Commercial Evaluation Facilities (CLEFs), which carry out the evaluations, and the establishment of approved techniques and procedures. CLEF is also accredited as a testing laboratory by UKAS, against ISO/IEC 17025.
- Certification body, which appoints CLEFs and keeps their appointment under review. It also confirms the suitability of each Target of Evaluation (TOE), certifying the results of evaluations conducted under the Scheme, and publishing details of certified products and PPs on the CESG and Common Criteria Portal websites. The certification body also deals with the appropriate national and international agencies regarding the mutual recognition of certificates.
- Sponsors, which refers to the person or organisation that requests and funds an evaluation and a certification; and is entitled to receive the reports produced.
- Developers, which refers to the person or organisation that has designed, developed, implemented, tested, manufactured and produced the TOE.



- The term 'Vendor' refers to the person or organisation that sells and distributes the TOE to consumers.
- Procurement body, which refers to the person or organisation that purchases and acquires the TOE for use in an operational environment.
- Accreditor, refers to the person or organisation that is responsible for the overall security of a System in its operational environment and who takes into consideration the conclusions and recommendations of the product's Certification Report, when assessing residual risks to the System.

(CESG 2016) also defines the overall process, which is divided into Preparation, Evaluation and Certification and Assurance Maintenance phases. Details on the process are not described in this section, but key elements of the process are referred in other sections.

### 3.3 Other initiatives

Here we describe the other initiatives on security and safety certification, which are not addressed in the previous sections. These initiatives can be alternative or complementary to the certification processes described above. In addition, this section briefly describes security and safety certification schemes, which are not directly applicable to the subject matter of this report (cybersecurity), but they are historically relevant in their domains (e.g., rail, airplanes) and they can provide inputs to the analysis.

#### 3.3.1 Industrial Automation and Control Systems (IACS)

*"Cyber-attacks targeting industrial automation and control systems (IACS) have been perpetrated for some years already. STUXNET, the malware that affected Iranian nuclear installations, was probably climactic in raising the industrial community's awareness of the risk that plants, their neighbourhood and customers might suffer, should a significant cyber-attack hit them. The threat landscape indicates that the various cyber-threats targeting critical infrastructures are increasing"*<sup>1</sup>.

Thus, the ENISA's recommendations<sup>2</sup> reflected the industrial community's need to test and certify IACS' cyber-security in the following terms:

*'ICS manufacturers are starting to (or will have to) include security requirements in the design phase of ICS components and applications. However, operators indicate that independent evaluations and tests are missing to effectively guarantee that those devices are in fact secure and that interoperability has also been considered when the new security features/capabilities are included. Furthermore, penetration tests and white box audits in controlled laboratories have shown that there are basic security bugs in devices and applications that could be properly identified if security development good practices were included into the development cycle. In any case, manufacturers, ICS security tools and services providers, as well as operators cannot be completely aware of the implications a modification may have with respect to their own systems or third-party ones. Moreover, it is important to certify that ICS do comply with minimum quality requirements with respect to cyber-security programming bugs'.*

<sup>1</sup> More on this topic: *"Proposals from the ERNCIP Thematic Group for a European IACS Components Cyber-security Compliance and Certification Scheme"*, published by the European Commission's Joint Research Centre, JRC94533, 2014, p. 9.

<sup>2</sup> "Protecting Industrial Control Systems: Recommendations for Europe and Member States", Enisa, 2011. Available at the following link: <https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states>

During the last six years, in its role of flagship Project - within the European Programme for Critical Infrastructure Protection (EPCIP) - the European Reference Network for Critical Infrastructure Protection (ERNICIP) has been mainly working on the initialization and maintenance of Thematic Groups (TG) with the focus of fostering the development of more advanced security solution for Critical Infrastructures across Europe. Among the nine currently running Thematic Group, the one on Industrial Automation Control System has been established in order to explore specific issues related to cyber security. The Group, established back in 2014, has initially worked on the identification of typical IACS configurations in view to properly scan the horizon and take decision on whether to focus on the cyber security of entire systems (as integrated in the industrial environment) or of single components. The analysis of the most recurring configurations, as gathered by the group, has led to the decision to work on components' level.

In this specific field, the Group has identified a huge gap in the European landscape, characterized by a missing framework for testing (and certifying) the cyber security of the most sensitive components installed in the IACS environment. Thanks to the mandate and sponsorship of partners Directorates General, the TG has then started working on a feasibility study for the establishment of a European Framework for the Compliance and Certification of the Cyber Security of IACS' components.

The initial steps of a potential roadmap toward this objective have been laid down in the deliverable that describes the main pillars that constitute the core activities that had to be carried on by the Group. Among them: 1) a stakeholder consultation in order to gather consensus, recruit further experts and fine tune the initial proposal; 2) a collection and analysis of common cyber security requirements from existing standards; 3) the development of security profiles in order to describe the environment in which a component should operate and the desired level of cyber security; 4) the design of the compliance and certification process.

The need to undertake all of the aforementioned activities has pushed the JRC facilitators in widely promoting such effort in view to expand the Group's network. Participation to events organized by ENISA, ETSI's Cyber Technical Committee and Cen/Cenelec's Cyber Security Coordination Group (CSCG) has led to the establishment of mutual support through the designation of observers that are taking part to the ERNICIP thematic group with the aim of supporting the project's activities, the stakeholder consultation and the recruitment of qualified experts in the following areas: standardization, compliance and certification process, cyber security, penetration testing and manufacturing of IACS components.

The Group's motivation in carrying on such initiative, come from an accurate analysis of the current European landscape. EU Member States are actively working on the implementation of Certification Schemes for the Cybersecurity of both IT and OT systems and components, as consolidated experiences show that certified products can contribute to the security of modern infrastructures. Many Governments have asked Information Security Agencies to define minimal technical requirements for technical standards for IT related equipment and in the upcoming years they will be looking into methods for widening these requirements and applying them also to the Industrial Automation Control Systems. This particular field requires a granular approach that should take into account the variety of components currently integrated into the industrial systems in order to asses which of them require enhanced focus and inclusion in certification schemes. As not all of the components are pivotal for the protection and security of certain infrastructures, cybersecurity-related schemes should focus on those devices and components that are in charge of vital functions that shouldn't be lost or shouldn't suffer disruptions.

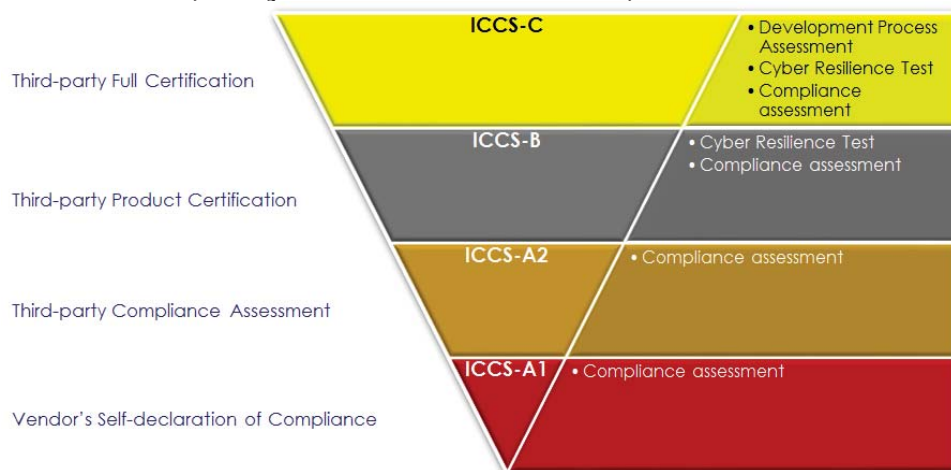
Another aspect that should also foster the establishment of certification schemes for the cyber security of IACS' components is also the possibility that the IACS' equipment manufacturers may have an easier access to the wider European market by obtaining a certification that is valid in the entire Union. Such circumstance would avoid them to

initiate a certification procedure for each of the Member States in which they'd like to offer their products. On an even wider scale, and in a later stage, the establishment of European certification framework, based on recognised technical standards, may also lead to international mutual recognitions that should enable European manufacturers to sell their products in non-EU countries without reobtaining the certification of their products twice. The work carried on by the ERNCIP TG stands as a clear use case on this specific matter as European experts are discussing the feasibility of the adoption of testing requirements from international standards such as the IEC-ISO 62443 (Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels) that is also used for the ISA secure Conformance certification (<http://www.isasecure.org/en-US/>) established in the USA.

The current picture of the ERNCIP TG's work in the field of testing and certification of components, already shows the contours and the path that should lead to the establishment of a European framework in this field.

The ERNCIP's 'IACS Compliance & Certification Framework' (ICCF), in fact, proposes **four IACS Compliance & Certification Schemes** (ICCS):

- ICCS-A1 (Compliance self-declaration);
- ICCS-A2 (Third-party compliance assessment);
- ICCS-B (Cyber resilience certification);
- ICCS-C (Full cyber resilience certification);



*Figure 4 ICCF Compliance & Certification Levels.*

The rationale behind these four levels is the following:

1. basic self-assessment only tells the customers that the vendor has checked the compliance of a product against a shared set of requirements;
2. When the same assessment is performed by an independent, accredited third party, customers are certain of the rigour of the assessment process and of the objectivity of the evaluation of the product;
3. Beyond only a formal assessment, 'on paper', a trusted third party tests the cyber-robustness of the product to check if it resists a set of commonly agreed tests (e.g. robustness tests);
4. Beyond scheme 3, assessing the development, operation and maintenance processes, associated with the evaluated IACS product, gives the customers even greater confidence in its cyber-security.

The ERNCIP's IACS Thematic Group is currently working on a second report (due in December 2016) that deepens the work in this field and should act as an orientation and feasibility study that provides:

- High level support to the implementation of the NIS directive;

- A framework to foster IACS components' cybersecurity certification;
- Four detailed schemes to motivate stakeholders to engage into certification at their own pace;
- Clear concepts and rules to help bridging with international schemes and containing certification's costs.

More in general, the ICCF aims at providing professionals within vendor, industry, laboratory and certification organisations with guidelines to make IACS components' cybersecurity certification happen more easily, at a controlled cost, and with recognition within and beyond European borders.

### **3.3.2 Common Criteria Recognition Arrangement (CCRA)**

The objective of the CCRA is to enable a context where ICT products and protection profiles which earn a Common Criteria certificate can be procured or used without the need for further evaluation. This can be achieved by a mutual recognition (i.e., arrangement) whereby the signers have agreed to accept the results of Common Criteria evaluations performed by other CCRA members. The CCRA seeks to provide grounds for confidence in the reliability of the judgements on which the original certificate was based by requiring that a Certification/Validation Body (CB) issuing Common Criteria certificates should meet high and consistent standard.

Within the CCRA only evaluations up to EAL 2 are mutually recognized. The European countries within the former ITSEC agreement typically recognize higher EALs as well. Evaluations at EAL5 and above tend to involve the security requirements of the host nation's government.

In September 2012, a majority of members of the CCRA produced a vision statement whereby mutual recognition of CC evaluated products will be lowered to EAL 2 (Including augmentation with flaw remediation). Further, this vision indicates a move away from assurance levels altogether and evaluations will be confined to conformance with Protection Profiles that have no stated assurance level. This will be achieved through technical working groups developing worldwide PPs, and as yet a transition period has not been fully determined.

An authorizing nation sponsors and oversees an evaluation scheme and authorizes the CC certificates that are issued. An evaluation scheme provides the regulatory and administrative framework for laboratories or facilities within the authorizing nation to evaluate and certify ICT products. A consuming nation agrees to recognize ICT products certified by other authorizing nations. An authorizing nation is also a consuming nation.

### **3.3.3 SOG-IS**

The Senior Officials Group – Information Systems Security (SOG-IS) agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

Participants in this Agreement are government organisations or government agencies from countries of the European Union or EFTA (European Free Trade Association), representing their country or countries.

As described in (SOGIS 2016), SOG-IS has the objective to:

1. Coordinate the standardisation of Common Criteria protection profiles and certification policies between European Certification Bodies in order to have a common position in the fast growing international CCRA group.

2. Coordinate the development of protection profiles whenever the European commission launches a directive that should be implemented in national laws as far as IT-security is involved.

For certificate producing nations there are also two levels of recognition within the agreement:

1. Certificate recognition up to EAL4 (as in CCRA)
2. Certificate recognition at higher levels for defined technical areas when schemes have been approved by the management committee for this level.

The recognition agreement is dated in January 2010 and it is available at [http://www.sogis.org/uk/mra\\_en.html](http://www.sogis.org/uk/mra_en.html).

### **3.3.4 UL 2900 certification.**

The UL Cybersecurity Assurance Program has developed a CAP certification approach, which verifies that a product offers a reasonable level of protection against threats that may result in unintended or unauthorized access, change or disruption.

UL CAP assessment is based on the requirements of the UL 2900 Standard. UL 2900-1 and the subparts of UL 2900-2 contain product requirements that will be verified during a product assessment.

As described in (UL 2016), a product assessment verifies a product's software is in compliance with required security controls. These security controls may include, but are not limited to, role-based access control, secure data storage, cryptography, key management, authentication, integrity and confidentiality of all data received and transmitted.

The UL 2900 Standard contains minimum requirements for each of these controls. The Standard contains requirements for the vendor to design the security controls in such a way that they demonstrably satisfy the security needs of the product. The Standard also describes testing and verification requirements aimed at collecting evidence that the designed security controls are implemented.

We note that the UL 2900 standards is not published and there has been critics on this lack of visibility on the standard as mentioned in (Arstechnica 2016).

### **3.3.5 Secure Change.**

The FP7 project Secure Change (<http://www.securechange.eu/>) investigated and researched new approaches for security software certification with a specific focus on the changes in the product. The project developed techniques, tools, and processes that support design techniques for evolution, testing, verification, re-configuration and local analysis of evolving software. The project results were applied and evaluated to the industrial application domains of mobile devices, digital homes, and large scale air traffic management.

### **3.3.6 EN50128.**

This standard does concern itself both with security and safety certification of software, and follows IEC61508. In particular, it specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications. It is more focused on safety rather than security as it addresses

the need to guarantee the operations of critical components like safety signalling in addition to non critical components like management information systems.

It is applicable exclusively to software testing and the interaction between software and the system of which it is part.

As in other standards, different levels of security certification are defined. They are called Security Integration Levels (SIL) and they are mapped to test coverage levels (R stands for "recommended", HR stands for "highly recommended") as for table

*Table 1 Security Integration Levels in coverage levels in EN50128 (from EN50128 standard)*

	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Statement Coverage	R	HR	HR	HR	HR
2. Branch Coverage	-	R	R	HR	HR
3. Composed conditions (MC/DC or MCC-Coverage)	-	R	R	HR	HR
4. Data Flow Analysis	-	R	R	HR	HR
5. Path Coverage	-	R	R	HR	HR

### **3.3.7 IEC61508**

This standard covers functional safety and it is aimed at the electrotechnical industry. It provides a methodology to assess the risks to systems and determine the safety requirements, and introduces both safety integrity levels and the safety lifecycle. It supports the certification of components for use in safety-critical systems. However its focus is on bounding failure probabilities, and it does not consider penetration testing or attacks from a malicious adversary.

### **3.3.8 ISO 27001/27002**

ISO 27001 sets out to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)" while 27002 has a list of possible controls. Essentially, these documents provide a framework for a large organization that seeks to measure and evaluate how well it does information security management; they make it susceptible to internal and external audit processes, and are basically seen as audit checklists. However, they are fundamentally about companies securing their own assets and operations, not about making products that protect their customers.

As a consequence, these standards are not relevant for the specific focus of security certification of products, but they could have a role for the security certification of systems.

## 4 Analysis of the existing certification schemes

This is an important section of the report as it identifies the key challenges of the existing certification schemes and the need to create alternatives.

### 4.1 Issues and challenges

The objective of this section is to describe the main issues and challenges of the existing certification schemes, which have been described in the previous sections.

While the Common Criteria approach is one of the most used approaches for security certification, it has been criticized by various stakeholders.

Table 2 identified the main issues and criticisms of the Common Criteria approach from literature. A summary and analysis will follow this table.

*Disclaimer:* The statements in the Description column in the table are extracted from the references identified in the Source column. This report does not directly endorse these statements even if they are used as an input to the analysis.

*Table 2 Identified issues and criticisms of the Common Criteria approach*

Identifier	Description	Source
1.	<i>In theory, countries that recognize Common Criteria evaluations should have considerable clout for convincing vendors to make security improvements to products. In practice, these countries have not cooperated sufficiently to agree upon requirements and many participants do not require the evaluations. The current trend is for countries to create their own testing regimens. In some cases, these competing evaluation schemes will be used to protect indigenous industries, and, more disconcertingly, as an opportunity to force vendors to disclose sensitive information.</i>	(NCSA 2011)
2.	<i>Common Criteria does not define the features or functionality that a product must have or require that the product itself be secure.</i> <i>Instead, the development of the product is evaluated against a security target, which can be a protection profile developed by a user or a company statement of what the product is intended to do.</i> <i>These are evaluated against a set of security assurance requirements to determine if the development process for the product enables it to meet its claimed security functionality. Basically, it tries to determine if the product does what it says it will do.</i> <i>This approach is a strength and a weakness of Common Criteria. By not specifying functionality requirements, it is a flexible framework that can be applied across a broad spectrum of products. But it focuses on process rather than product. Knowing what a product is designed to do does not necessarily mean it can do it well or securely, critics say.</i>	(Jackson 2007)
3.	<i>no single set of criteria can be used to produce comparable and effective evaluations for a wide range of technologies</i>	(NCSA 2011)
4.	<i>The CC evaluation process for lower assurance levels (EAL1 to EAL4), which correspond to the levels at which most products are evaluated, are essentially a paper evaluation of the development process and product documentation, not requiring</i>	(ECORYS 2011)

	<i>evaluation of software.</i>	
5.	<i>Commonly used protection profiles often do not correspond to the functionality requirements actually required by users.</i>	(ECORYS 2011)
6.	<i>Long and expensive. CC evaluation life cycle is lengthy and expensive. In fact, due to the complexity of the process and the high cost, vendors have to spend a large effort on preparation for the evaluation, which adds to the cost and time of the evaluation itself. High assurance level (as EAL4) certification can take 12 years, and, often, by the time the process is completed a new version of product is already delivered.</i>	(Kaluvuri 2014)
7.	<i>Concerns for Mutual Recognition. Though the CC scheme is a widely recognized international standard, there are several concerns regarding the consistency of the assessments by the evaluating laboratories located in different countries, since the Common Criteria Recognition Arrangement (CCRA) does not prescribe any monitoring and auditing capability. In addition, the relevance of CC certification for governmental institutions, specific national interests can impact the impartiality of the assessment.</i>	(Kaluvuri 2014)
8.	<i>Point in time certification. CC certifies a particular version of the product in certain configurations. Any changes to the configuration or any updates to the product that affect the Target of Evaluation (TOE), which is the part of the product that is evaluated, invalidate the certification. This is not a desirable situation, given that products evolve and are updated at a frantic pace and the certification must not be frozen to a specific version of the product.</i>	(Kaluvuri 2014)
9.	<i>Comparability. One of the main objectives of CC is to allow consumers to compare certified products on the market in an objective way from a security point of view. However, certification documents are filled with legalese and technical jargon. Hence, comparison is not straightforward nor easy.</i>	(Kaluvuri 2014)
10.	<i>The above discussion should have shown how the Common Criteria are not well matched to the needs of the control systems world. At the technical level, a security certification scheme must be able to cope with dynamic systems, dynamic threats and real users working in real organisations. It must complement, rather than conflict with, existing safety certification mechanisms. But above all, its function is to provide assurance to asset owners that the systems and components they buy from the vendor community are fit for purpose.</i>	(Anderson 2009)
11.	<i>Common Criteria fail to deal satisfactorily with systems that are patched frequently, as operating systems now are; observers of the operating-system patching cycle and vulnerability scene have come to the conclusion that the Common Criteria are no more than a bureaucratic exercise whose costs far outweigh the benefits.</i>	(Anderson 2009)
12.	<i>How has this CC-evaluated product improved my IT system's security?</i>  <i>The problem is that few, if any, metrics exist to support this question, and without them, it's impossible to assess the cost-benefit ratio for performing an evaluation. The CC government members believe that evaluated products provide better protection than unevaluated products, and that evaluated</i>	(Hearn 2004)



	<i>products contribute to overall system security when integrated into systems. Yet, without a system-level approach to security, and the metrics to support such an approach, these views lack a solid foundation.</i>	
13.	<i>Other significant obstacles and barriers include concerns about the comparability and competency of evaluations. Conflicts between international harmonization and national investments could be especially significant if major European nations and the US continue to follow increasingly divergent paths as they pursue national interests. Although the founding member nations were able to work through their differences to produce the CC and the CC Recognition Arrangement (CCRA), living with the result proves once again that the devil is in the (implementation) details.</i>	(Hearn 2004)
14.	<i>CC are not suitable for services e.g. Cloud and big data. This is an example of why certification of components alone is not enough; we need an overall framework for certification which includes services, personnel, systems and products as well.</i>	(ENISA 2014)
15.	<i>It is an open question if existing applications might continue running on top of certified, and properly modified of course, products. Assessments should take place to this direction. Re-writing existing application will prove to be a big challenge.</i>	(ENISA 2014)
16.	<i>Re-certification after changes being made in the product is not mandatory, but should be considered case by case</i>	(ENISA 2014)
17.	<i>Testing what the vendor wants tested rather than what the customer (or other relying party) needs tested is a pervasive problem with the Common Criteria.</i>	(Anderson 2009)
18.	<i>Common Criteria assurance requirements tend to be inspired by the traditional waterfall software development methodology, while most of the modern software is produced using modern agile paradigms.</i>	(Beznosov 2004)

From the analysis of the international security certification schemes, it is clear that the Common Criteria is endorsed by the main national bodies (France does also support Certification de Sécurité de Premier Niveau but the Common Criteria is also supported).

Then, the starting point for a European wide security certification process is the Common Criteria but the main issues, which have been highlighted before must be addressed.

From the analysis provided in Table 2, we can identify the following main issues:

1. **Re-certification and patching.** Re-certification of an already certified system or product is an issue raised in items 8,9,11, 16 and 18. This requires the definition of a new process or a modification of the existing approach for Common Criteria.
2. **Mutual Recognition.** Mutual recognition of the certification or comparability of protection profile is an issue raised in items 1,3,7,13. While, this is an important matter, the existing CCRA and SOG-IS are already addressing this matter.
3. **Security and trust coverage.** Security certification with Common Criteria may not be enough to provide full security and trust of a product. This is suggested in items 2,4,5,14.
4. **Certification costs.** Common criteria certification is considered a long and expensive process, which does not make it suitable for fast market deployment or relative short product cycles as in the consumer market (see section 3.4.2). This was raised in item 6.

5. *Non applicability to specific products and systems.* Some classes of system and products are difficult to certify due their intrinsic features and characteristics. This issue was raised in items 14.
6. *Comparability and visibility of the certification.* Users do not have a clear metric of comparison among different certified products.
7. *Usability.* The Common criteria certification does not give a clear and simple indication to the users of the provided level of trust. Metrics are missing for this purpose. This issue was raised in item 12

In addition, we can identify the two following issues, which must be addressed in the definition of an European security certification framework in the current context:

8. *Joint certification of security and privacy.* With the introduction of the General Data Protection Regulation (GDPR) (see EU 2016b), it is preferable that both security and privacy certification is implemented in the same process.
9. *Accreditation and testing laboratories.* To support an European security certification framework, it is preferable that an harmonized accreditation process is set up for testing laboratories.

The recommendations of this report will focus on the actions, which can address the issues defined above.

## **4.2 Domains applicability**

Security certification schemes were born in the defence domain, which is characterized by stringent security requirements, high costs of the equipment and very long lifecycles. Other domains do not share these characteristics and this is one of the main reason, why security certification and common criteria in particular has not been widely adopted in some domains (Anderson 2009) like the consumer market (e.g., smartphones).

On the other side, common criteria is most widely adopted security certification scheme and many products with limited capabilities like smartcards has been common criteria certified.

Indeed, the list of products and systems certified with Common Criteria is impressive and it is reported in (CCProd 2016). The list spans from smartcard and integrated circuits, database, detection systems, network and network-related devices and systems and other products used in many different domains.

As a consequence, it is not true that the Common Criteria cannot be applied a-priori to any domain, even if binding regulations in the specific domain apply and economic considerations can have an impact.

In the following paragraphs we describe the main aspects of two specific sectors: the energy sector and the cooperative intelligent transport system sector.

### **4.2.1 Specific aspects of the energy sector**

While the ICT industry or the consumer mass market industry is entrepreneurial and freewheeling, with multiple overlapping and competing standards and fairly loose compliance, the electric power industry is different for safety reasons and for the huge scale of the infrastructures and the number of serviced users. Its engineers are meticulous about complying with every relevant standard because malfunctions can produce safety hazards and even kill people. In comparison to the automotive sector, which has similar safety issues, the engineers of the energy sector have to address very complex and interdependent infrastructures, where not all the dependencies (especially at the ICT level) are clearly identified. Some of the potential security threats are still not clearly understood and there is a growing body of research on security and privacy

aspects of the energy sector including its evolutions to the Smart Grid. The complexity and scale of future

power systems that incorporate smart-grid concepts will introduce many security challenges. Currently, a large utility communicates with thousands of devices to manage the electrical grid. Both the volume of data and the number of devices with which a utility communicates will likely increase by several orders of magnitude. With these larger networks, routine maintenance, managing trust, and monitoring for cyber intrusion become challenges. Certification of electronic components has already been largely adopted in the energy sector for safety reasons, but the introduction of more sophisticated ICT components will increase the need to integrate elements of security and privacy certification.

A more detailed study of the energy sector is provided in the report drafted by the Foundation for Information Policy Research (see reference FIPR 2016).

#### **4.2.2 Specific aspects of the automotive sector**

The automotive sector has quite strong requirements related to safety, while security aspects have not been substantially addressed because vehicles are basically protected by physical security. Until recently, cars were not connected to the outside world and the vehicle manufactures have full responsibility about safety and security. The Type approval and homologation processes had a very long history and the process is quite stable now, even if it can be quite expensive for vehicle manufacturers and it is fragmented, as there are different types approval requirements around the world. One example of this context is the internal vehicle network system mostly based on the CANBus set of standards. Not only this standard is quite old, but it is also not secure. This may change in the future because vehicles will be increasingly connected and new security threats may appear as demonstrated in recent incidents. There is an ongoing discussion on what type of security certification should be adopted for the new model of Cooperative ITS in Europe and Connected Vehicles in USA and it is not clear yet if the security certification of the wireless devices should be part of the type approval or not.

Cooperative Intelligent Transport Systems (C-ITS) is the term used to describe technology which allows vehicles to become connected to each other, and to the infrastructure and other parts of the transport network. In addition to what drivers can immediately see around them, and what vehicle sensors can detect, all parts of the transport system will increasingly be able to share information to improve decision making. Thus, this technology can improve road safety through avoiding collisions, but also assist in reducing congestion and improving traffic flows, and reduce environmental impacts. Once the basic technology is in place as a platform, an array of applications can be developed (from [http://ec.europa.eu/transport/themes/its/c-its\\_en.htm](http://ec.europa.eu/transport/themes/its/c-its_en.htm)).

The European Commission decided early 2014 to take a more prominent role in the deployment of connected driving, by setting up a C-ITS Deployment Platform. The Platform was conceived as a cooperative framework including national authorities, C-ITS stakeholders and the Commission, in view to develop a shared vision on the interoperable deployment of C-ITS in the EU. Hence, it was expected to provide policy recommendations for the development of a roadmap and a deployment strategy for C-ITS in the EU and identify potential solutions to some critical cross-cutting issues.

One of the key aspects is the compliance assessment process in C-ITS, whose main principles were defined in Working Group 5 of the C-ITS Deployment Platform and they have been published in (C-ITS 2016).

The following description of the compliance assessment process has been extracted from (C-ITS 2016) and the source documents, which generated (C-ITS 2016).

The compliance assessment process is used to certify C-ITS station for their deployment in the road transportation sector. A C-ITS station is roadside equipment or vehicle or

another mobile system, which can be connected using the 5.9 GHz Dedicated Short Range Communication system. Note that this is a simplification because the formal definition of an ITS station is provided in (ETSI 2010).

The overall architecture is shown in Figure 5.

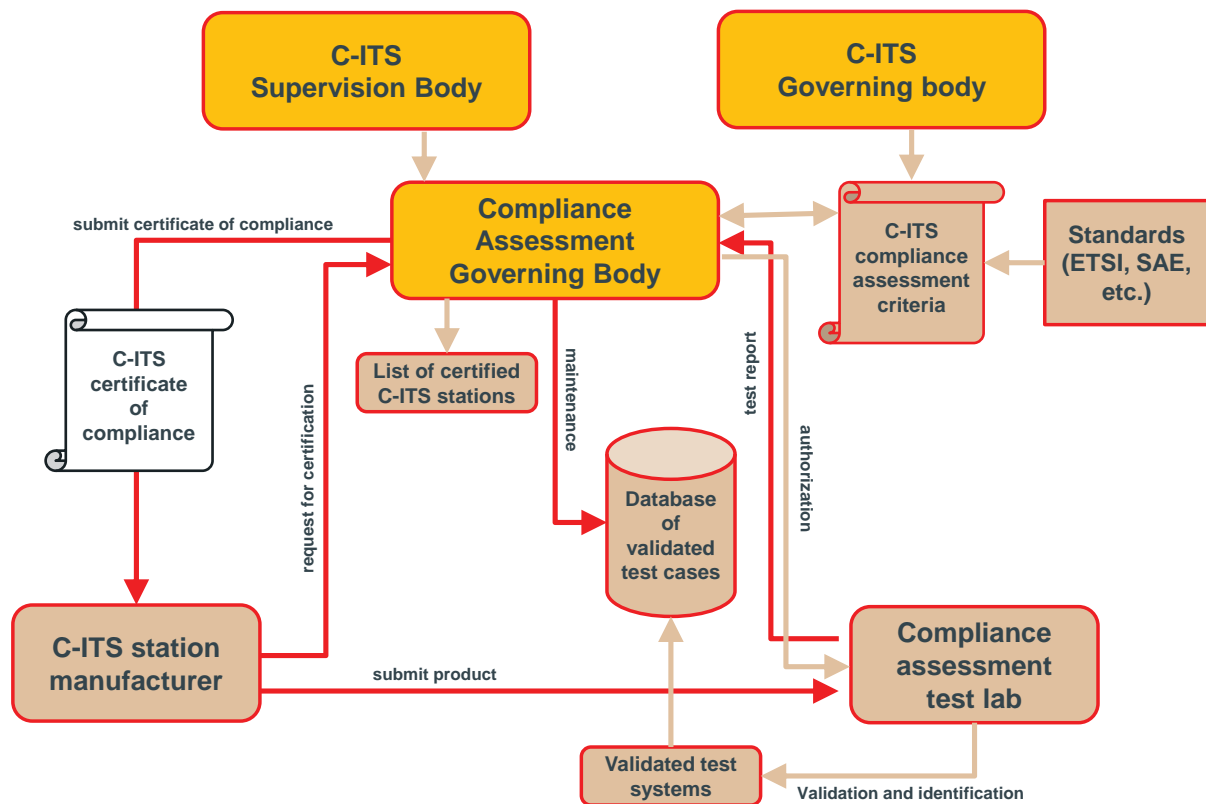


Figure 5 C-ITS European Compliance Assessment process

The main roles in the C-ITS European Compliance Assessment process are following.

The compliance assessment governing body is a centralized entity responsible for:

- Definition of compliance assessment criteria, which are compliant to and using the C-ITS Governing Body's input documents for operational and security requirements and the standards.
- handling of compliance assessment requests of C-ITS manufacturers
- definition of test scope for the compliance assessment (based on the C-ITS station type and functionality)
- definition of the minimum set of test criteria for the compliance assessment of every C-ITS station in order to be an interoperable node of the C-ITS Network
- submit certificate of compliance after successful C-ITS compliance assessment.
- maintenance of the list of certified C-ITS stations.
- authorization of ISO17025 accredited test labs (e.g. independent test labs)
  - based on frequent repetition of the accreditation in strict accordance on not yet defined certain criteria, but in accordance of the valid EU wide C-ITS Trust Model and the respective procedures:
  - nomination of qualified lab auditors
- maintenance of a database, which lists and stores validated test cases and validated test systems, which must be used for the execution of the test procedures for compliance assessment.

The Compliance Assessment Governing Body can be accredited according to the following standard:

- EN ISO/IEC 17065:2012 - Conformity assessment – Requirements for bodies certifying products, processes and services

The Compliance assessment test lab is responsible for

- the execution of test cases according to the C-ITS compliance assessment criteria.
- The testing will be performed:
  - by qualified persons
  - only on validated test systems
  - in a shielded lab environment
- validation of test cases on selected and validated test systems
- creating test reports and submission to the Compliance Assessment Governing Body

The Test Lab should be accredited according to the following standard:

- EN ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories.

In addition, in order to build and operate the databases of C-ITS stations a Compliance Assessment Function is needed. To operate the database, the minimum requirements for conformance and performance needs to be established and maintained. This will typically consist of the following elements:

- Set of test cases per C-ITS station
- Compliance assessment Criteria for each type of C-ITS station (list of subset of test cases required to be passed for a given type of C-ITS station, and the minimum criteria for every validated C-ITS station in the network)
- Database of verified test cases and test implementations
- Rules for declaration of conformance.

## 5 A way forward for a European certification scheme

### 5.1 Drivers for a new European certification scheme

The need for a European certification scheme has already been suggested by various studies including (ECORYS 2011) and (ERNCIP 2014).

In particular, (ERNCIP 2014) highlighted the need for a European certification scheme for industrial components for the main reasons:

1. Need to harmonize the current national certification schemes (Germany, UK and France) but there are others to create a common European certification scheme based on a common approach.
2. Testing and certifying the cyber-security of IACS components/devices seemed to IACS stakeholders a useful step to take as it would bring a higher level of cyber-confidence to industry buyers and users.
3. The need to establish a practical scheme guaranteeing mutual recognition of certificates across Europe and compatible with similar requirements beyond. This aspect is complementary to item 1. Note that the current collaboration schemes like CCRA and SOG-IS could be a starting point for the establishment of a common format and semantic of the certificates.
4. A common European certification scheme would bring a higher level of cyber-confidence to industry buyers and users.

We note that item 4 could be a key enabler to improve the competitiveness of the European industry because a harmonized certified device and product at European level could become an added value for cybersecurity products and a recognized label at global level (e.g., similar to the CE marking). As described in (ECORYS 2011), EU certification may be more widely recognised as an international 'quality label' and, hence, support the international competitiveness of European producers. It must be recognised however, that non-European producers that obtained the same European certification would benefit in an equal way from this 'quality label'.

In a similar way, the ECORYS report (ECORYS 2011) defined the following drivers. Note that (ECORYS 2011) makes a distinction between Type 1 and Type 2 security products. The Type 1 products represents general security products as for the mass or consumer market, while the Type 2 products represents specific high level security products like the ones used for public safety or homeland security contexts. Note that (ECORYS 2011) uses the term Conformity Assessment and Certification (CAC) to define the certification process.

1. Reduce barriers to trade in security products within the EU for Type 1 security products. Reduce fragmentation of EU markets for security products within the EU and promote a 'level playing field' for security products within the EU.
2. Reduce the burden of security requirements for certification of security products both for Type 1 and Type 2 for security manufacturers because they will have only a harmonized certification procedure across Europe.
3. Support for existing or future security policy needs and ensure common minimum performance levels for security products in EU. For example, an existing policy for security products in the road transportation sector or the energy sector could benefit from a European security certification scheme, which could be directly linked to it. An important example is the new Radio Equipment Directive (RED 2014), where links can be established between the certification of the wireless device and its security certification.

In addition, to the identified drivers, we highlight the advantage of a common European certification scheme for security certification of personnel working in the cybersecurity

industry because the procedures and processes would be the same or quite similar (at European level).

Another important advantage would be the harmonization of the security testing tools and systems used for the testing and certification process, which can reduce market fragmentation. At the moment, there are many different security certification tools for various purposes, which increase the costs and make more complex the activity of security testing workshops and certification centres. By harmonizing the certification procedures, these issues can be removed or mitigated.

Recommendation 1: A European security certification scheme should be set-up to overcome the national differences on security certification and support an european-wide cybersecurity market.

## 5.2 Key elements of the new European security certification scheme

Here we describe the key elements of a potential European security certification scheme, which can overcome the issues defined in section Issues and challenges 4.1 and address the drivers identified in section 5.1.

This new European security certification scheme can be also defined as lightweight certification scheme as it tries to streamline and make more efficient the security certification process for a wide range of ICT products. The term lightweight should not be understood as a weakening of the level of trust of the certified products but rather a more efficient way to certify the products according to different needs and different evaluation levels.

The key element of this scheme are following:

1. *A common European security certification scheme and the accompanying standard.* On the basis of the analysis of the national certification scheme described in section 3, we note that there is a convergence to the Common Criteria approach even if this is not formally decided. While there have been various attempts to propose new security certification approaches, we believe that the widespread use of common criteria at global level is a strong supportive element to propose common criteria as the basis of the European security certification scheme.
2. *A certification scheme based on different certification levels.* As proposed in (ECORYS 2011) and (ERNICIP 2014), certification can be of different levels where the basic level is a self-certification and it is not mandatory, while higher levels require that the certification is executed in a security certification centre with different types of test (see section 3.3.1 for a description of the IACS level).
3. *Labelling scheme.* A labelling scheme can be created to give a straightforward indication on the level of certified security of a product. The label concept is described more in detail in section 5.3, but the basic idea is to match labels to harmonized protection profiles at European level.
4. *Harmonized protection profiles* at European level. The SOG-IS agreement could be extended to define harmonized protection profiles in specific domains (i.e., a separate protection profile for each domain). Harmonized protection profiles at European level for devices and products are needed to support a common certification process. Harmonized protection profiles are also needed to support the labelling concept because labels must be associated to a specific protection profile, which is the same across Europe. Harmonized protection profiles should be defined to address the issue of security and trust coverage. With the term

domain, we mean a set of applications with common security requirements, which can be used to drive the definition of a common protection profile.

5. *Evolution of Common Criteria*. While the Common Criteria can be the basis for an European security certification process, some of the issues identified in section 4.1 must be addressed. In particular, the definition of a process to address changes in the protection profile is one of the highest priority tasks. The following sub-recommendations are proposed (which are similar to what proposed in (Salter 2011) (CC 2012))
  - Common set of protection profiles (“standard protection profile”) for technologies and products, which have a similar set of features and they are subject to a common set of threats.
  - A lightweight scheme to address incremental or evolutionary changes in the products.
6. *Accredited European security certification centres*. A network of European security certification centres must be set-up to support a European security certification scheme. An accreditation process must also be defined for the same purpose. In this area, the Future Internet Research and Experimentation initiative could be exploited to support this network.
7. *European Governing board*. A European governing board to support the European security certification scheme should be established to manage changes in the European security certification scheme and to coordinate aspects related to the European harmonization (e.g., harmonization of the protection profiles in each domain). See also (ECORYS 2011) for a similar recommendation of an EU body for security compliance and certification. One of the objective of the European governing board is also to address gaps in the certification of the security products and to address requests from the community (e.g., service providers, government, users, manufacturers) for the need of the definition of

Recommendation 2: The basis for the new European security certification scheme shall be mainly based on the Common Criteria but new processes/standards should be defined for re-certification after product changes.

new harmonized protection profiles.

Recommendation 3: A process to define harmonized protection profiles for specific domains should be put in place with the collaboration of existing organizations like SOG-IS or agreements like CCRA.

These elements can address the issues of the existing certification schemes identified in section 4.1 as described in the following table:

*Table 3 Key elements of the new European security certification scheme against the issues identified in section 3.4.1.*

Key elements	Issues	Comments
--------------	--------	----------



A common European security certification scheme and the accompanying standard.	Mutual Recognition	By creating a common European security certification scheme, mutual recognition is ensured.
Certification scheme based on different certification levels	Certification costs	By adopting different levels of certification, the manufacturers can choose the most cost-effective security certification scheme for their products.
Labelling scheme	Comparability and visibility of the certification Security and trust coverage	A labelling scheme linked to specific protection profiles can give a clear indication on the type of security certification to which the product has been submitted. The labels does also give an indication on the security and trust coverage of the product.
Harmonized protection profiles	<ul style="list-style-type: none"> <li>• Mutual Recognition</li> <li>• Comparability and visibility of the certification</li> </ul>	Harmonized protection profiles can support both mutual recognition and the labelling scheme to support the Comparability and visibility of the certification.
Evolution of Common Criteria	Re-certification and patching	The Common criteria process should be enhanced to address in a more efficient way the re-certification of an already certified product.
Accredited European security certification centres	Mutual Recognition	Accredited European security certification centres are a key element to guarantee an harmonized security certification process.
European Governing board	Mutual Recognition Non applicability to specific products and systems	<p>The board will ensure European harmonization of the security certification process to support mutual recognition.</p> <p>The board will also address gaps and requests from stakeholder to mitigate the risk of non-applicability to specific products and systems.</p>

The development and deployment of a new European security certification scheme based on these elements could be a step by step approach regulated by appropriate EU framework. The challenge is to resolve the dependencies among the different elements in a coordinated way. For example, the accredited European security certification centres

would require the definition of common standards and common EU-wide protection profiles in the different domains, before they can start to test and certify products.

A preliminary pictorial description on how the different key elements of the European security certification scheme are linked is provided in Figure 6.

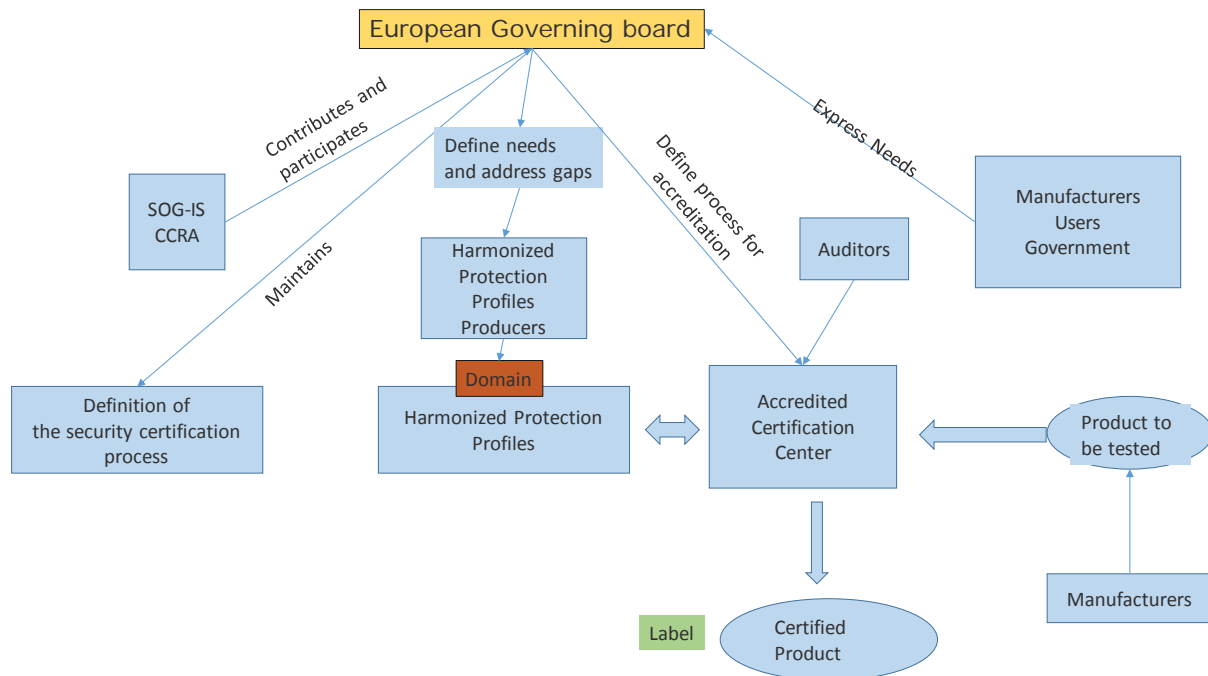


Figure 6 Overall scheme of the proposed European Security certification scheme

### 5.3 Labelling

The concept of applying a label on a product after a successful security certification is not new, as the EAL certificates from common criteria, the IACS (ERNCIP 2014), the four levels of FIPS can all be related to a labelling scheme, which gives an indication on the level of security protection or trust of a system.

The critical task is how to associate the labels in a harmonized way across different certification schemes, protection profiles and so on.

In France, the ANSSI has also defined a label system for trusted products and service providers. Currently, ANSSI recognises and issues two main types of labels. These labels are used for:

- certifying products
- qualifying products and services

The labelling concept could be extended to cover not only the traditional levels of Common Criteria (EAL), but to address specific security functions, which can be linked to specific protection profiles. For example, labels could be defined for specific security properties like confidentiality, integrity and authentication or for a specific Security Target (ST), which is defined in the related protection profile.

We can define different dimensions for which the label can be defined:

1. Level of assurance. This is the equivalent of the EAL in Common Criteria. We note that EAL level does not measure the security of the system itself, it simply states at what level the system was tested.

2. Protection profile for a specific domain (energy, road transportation and so on). Each protection profile can be associated to a specific level of assurance (dimension 1). Each domain has its own specific features and configuration environment, which must take in consideration for the security certification and deployment. For example, the security certification of a crypto-module for the road transportation may not be valid for the energy sector. This is why, the label must have a separate dimension to identify the domain.
3. To define how the certification was achieved: self-certification, third-party compliance assessment and so on how it is defined for IACS in section 3.3.1.

Figure 7 describes the label scheme and its dimensions.

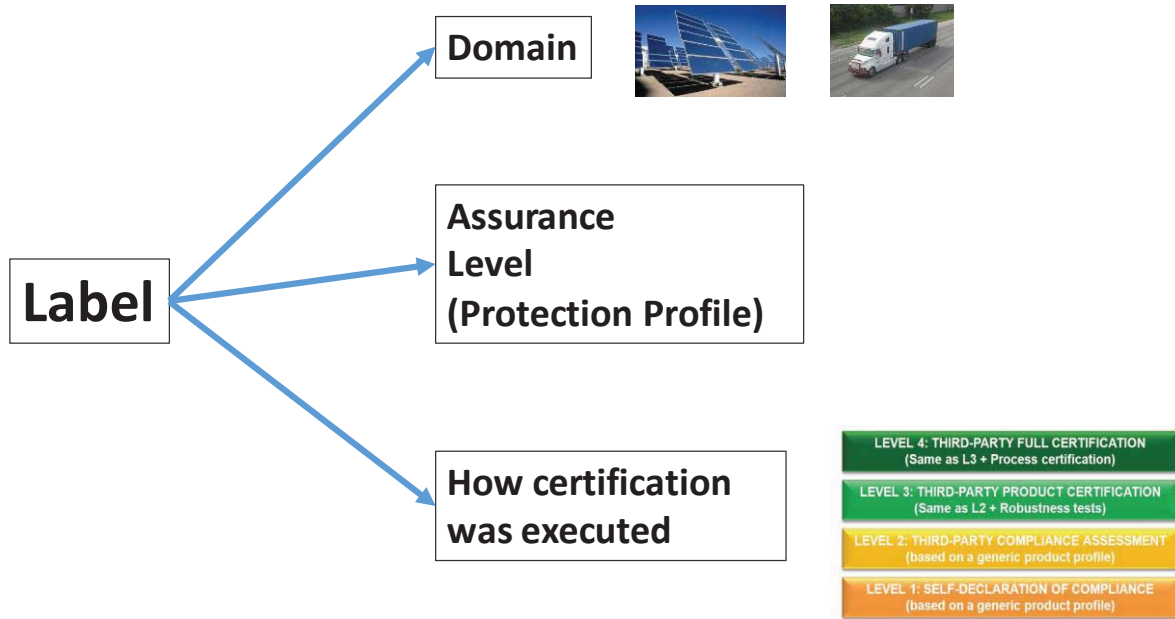


Figure 7 Label scheme and its dimensions

Recommendation 4: The definition of harmonized protection profiles is the basis for the definition of a labelling scheme to support the comparability and visibility of the security certification for end-users. A labelling scheme at European level should be put in place.

## 5.4 Security and Privacy certification

The concept of privacy certification is not new, even if security certification (or safety certification) has been historically the main priority. European Commission's General Data Protection Regulation (EU 2016b) in Recital 77 encourages the "establishment of certification mechanisms, data protection seals and marks" to enhance transparency, legal compliance and to permit data subjects [individuals] the means to make quick assessments of the level of data protection of relevant products and services.

A relevant case study for Privacy certification is the concept of Privacy Seal (EU 2013). The Privacy seal is a trans-European privacy trust mark issued by an independent third party certifying compliance with the European regulations on privacy and data

protection. See (see <https://www.european-privacy-seal.eu/> by EuroPriSe for more information on the Privacy Seal and the activities carried out by EuroPriSe. The Privacy seal concept is relatively similar to the label concept of security certification where the label is the seal itself.

The overall process to obtain a Privacy Seal could also be similar to envisaged security certification process described in section 5. Private and public manufacturers of IT products and IT-based services can apply for the certificate of the European seal. The trust mark is awarded after successful evaluation of the product or service by independent experts and a validation of the evaluation by an impartial certification authority.

Reference (EU 2013) provides an extensive description of the most common Privacy Certification processes available in the world. One of the main examples is TRUSTe, which defines processes for Privacy certifications for various products and services. In (TRUSTe 2016) are defined Privacy certification standards for Smart Grids, Enterprise and others. TRUSTe works closely with stakeholders to identify the needs for the definition of new Privacy certification standards. The standards define the Privacy Program requirements, the vendor must satisfy in its service or product. Examples of requirements defined in the TRUSTe standards are related to protection against phishing or the implementation of encryption methods for data protection and data confidentiality.

These examples already show that security certification and privacy certification cannot be disjointed but they should be combined as they often address the same or similar requirements (e.g., access control, confidentiality) or solutions (e.g., cryptographic algorithms).

We can identify the main challenges for privacy certification in the context of this report:

- 1) Privacy certification standards are highly fragmented both in the privacy context (e.g., various companies providing privacy certification for seals) and the public context (e.g., European national states)
- 2) The language used in the definition of the requirements is not harmonized across the entities providing the privacy seal. As a consequence, privacy certification suffers the same issue of security certification: lack of interoperability and mutual recognition for the security certification. In addition, we do not identify (at the time of writing this report) initiatives to define harmonization actions like SOG-IS in the privacy area apart from EuroPriSe.
- 3) At the time of writing this report, the seal is only a binary value: Yes or Not, while the security certification foresees different levels of certification. As reported in (IAPP 2016), the U.K. Information Commissioner's Office suggested that a traffic-light-style graded scale, to indicate levels of data protection could be implemented.

The authors of this report believe that such challenges could be addressed using a similar framework already defined for security certification. A critical aspect would be the integration of security and privacy requirements in the same process even if the initial drivers and sources of requirements would be different.

A possible workflow for the integration and security and privacy requirements would be as described in Figure 8.

The concept is the EDPS, Application Experts and the European Governing board work together to support the definition of the security and privacy requirements, which will be used by the Protection Profile producers. As a consequence, the privacy standards and requirements used to drive the Privacy Seal, will become part of the overall protection profile and the privacy seal is part of the final Label.

Recommendation 5: Security and privacy requirements should be validated in the same certification process and within the same harmonized protection profiles.

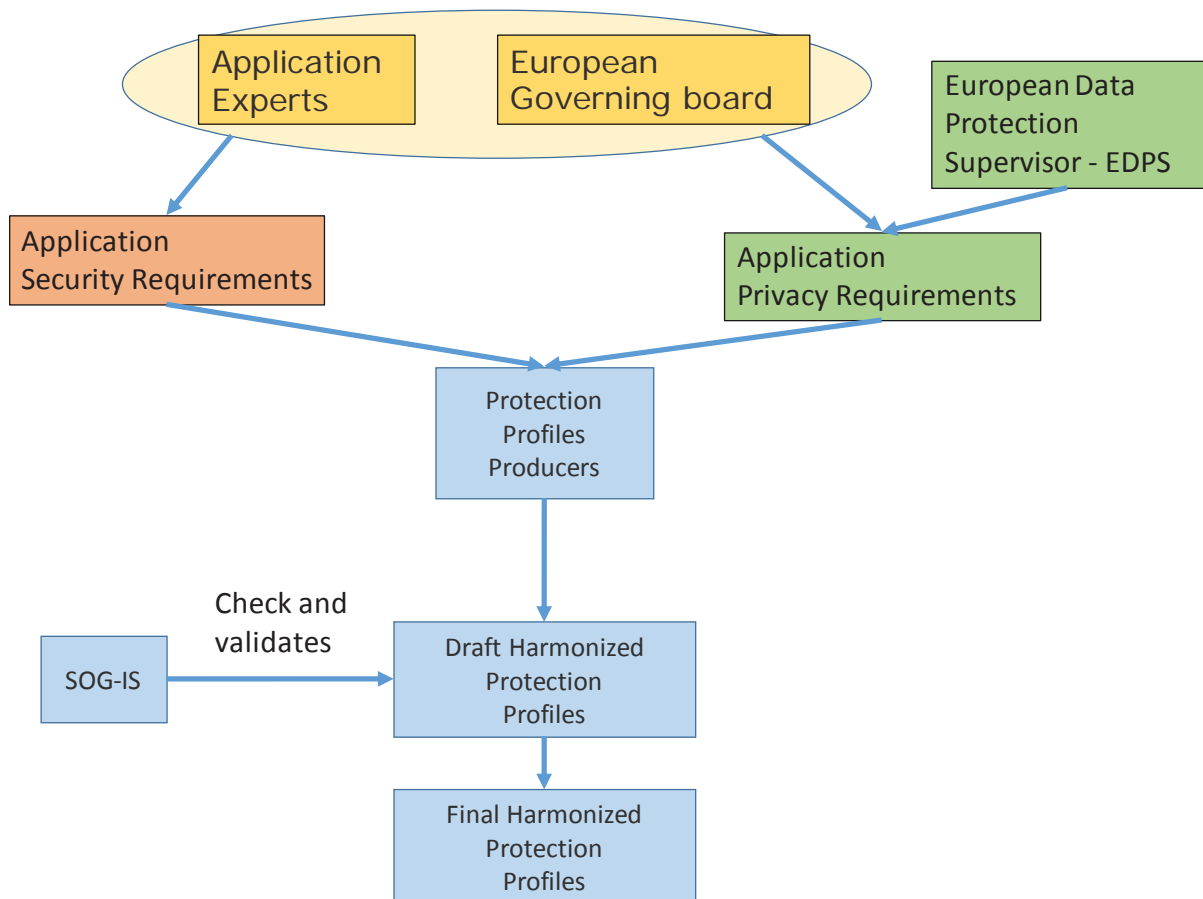


Figure 8 Security and Privacy flows

In this flow, the accreditation of test beds for privacy seals discussed in (EC 2013) would be part of the already existing accreditation process for security certification.

In fact, the section policy option proposed in (EC 2013b) for privacy seals is focused on the incorporation of the *EU data protection requirements into an existing EU certification scheme*, which is the same approach identified here.

## 5.5 Accreditation and testing laboratories

Testing laboratories are an important element of security certification. The goal of this section is to describe the role of the testing laboratories in security certification.

The Testing laboratory is where the tests needed to achieve security certification of a product or a system are actually performed. To perform such tests and provide a certificate of compliance of the product, the testing laboratory itself must be itself evaluated. This process is called accreditation and it is defined in (NIST 2016) as:

“Accreditation is used to verify that laboratories have an appropriate quality management system and can properly perform certain test methods (e.g., ANSI, ASTM, and ISO test methods) and calibration parameters according to their scopes of accreditation”.

One of the most common standard used to perform accreditation of testing laboratories is the ISO/IEC 17025 standard.

ISO/IEC 17025:2005 is a standard, which defines the requirements for the capabilities to carry out tests and/or calibrations. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods.

It is applicable to all organizations performing tests and/or calibrations. These include, for example, first-, second- and third-party laboratories, and laboratories where testing and/or calibration forms part of inspection and product certification.

In USA, the National Voluntary Laboratory Accreditation Program (NVLAP) accredits testing laboratories to meet the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme requirements and conduct IT security evaluations for conformance to the Common Criteria.

In Europe, a number of firms have been certified as Commercial Licensed Evaluation Facilities (CLEFs) under the Common Criteria in UK, as Centres d’Evaluation de la Sécurité des Technologies de l’Information (CESTI) in France and IT Security Evaluation Facility (ITSEF) in Germany.

The accreditation process in the world and especially in Europe is well deployed and based on a well-defined standard (ISO/IEC 17025:2005). Potential improvements of the accreditation process can be more focused on the way the tests are conducted in the lab. Most of the test suites and the test bed capabilities are focused on rule-based or standard-based compliance while many security failures are due to security attacks. Testing labs could become more competent and be accredited for testing of adversarial thinking by hackers. This improvement obviously requires additional capabilities and cost, so it cannot be applied to all the existing accredited labs.

Two levels of accredited labs could be foreseen, with the first level based on conventional accreditation and the second level based on the previous recommendation.

Another potential improvement of the accreditation process is that accreditation can be often focused either on safety (e.g., mechanical incidents in railways) or security (e.g., cybersecurity threat). While, in the past, this separated approach could be acceptable, the on-going evolution of ICT and its growing role in critical infrastructures or cyber-physical systems, will probably require an accreditation process, which combines safety and security.

Recommendation 6: A process to create accredited security testing centres should be defined. While existing processes can be used, they should be reviewed according to the new security certification framework.

## 5.6 Main roles

Here we describe the possible roles for a European certification scheme. Note that some of the roles have been already identified in the previous section 5.2.

- Product Manufacturer. This is the manufacturer of the product to be submitted for certification. Manufacturers can be present in different domains or a single domain (e.g., road transportation or energy).
- EU standardization bodies. They are responsible to define the standards (including test standards), which are used to support the definition of the test suites to be executed in the security certification process. They can also be responsible for the definition of the test bed requirements and configuration.
- European accreditation bodies and auditors. They are responsible for the accreditation of the certification centres and the periodic auditing.
- European Data Protection Board (EDPB), which is responsible to support the definition of privacy requirements and elements of the harmonized protection profiles.
- European Governing Board (EGB), which is responsible for managing the overall security certification process at the Europe level. The European Governing board is composed at least by the representatives of the national certification bodies and the European Commission. SOG-IS will also be part of the European Governing Board. The EGB is responsible for drafting and managing changes to the security certification process. The EGB is also responsible to define the labels in different domains.
- Accredited certification centre. This is the certification centre, which performs the test execution on the basis of the pre-defined harmonized protection profile.
- Harmonized Protection Profile producers. They are responsible for drafting the harmonized protection profiles at European level. The producers can be public or private bodies with expertise in security certification.
- Users. They are the users of the certified product. They use the label information as a metric to drive their procurement process. Users can be citizen, public (e.g., government) or private companies.
- European Commission. The European Commission would be part of the EGB to drive future evolutions of the certification framework. In addition, some parts of the EC could have a more operational role regarding some functions of the certification framework. For example, the publication of the documents describing the overall process and the list of accredited third parties test lab at any given moment.

The functions of the different roles can change depending on the policy options, which are described in section **Error! Reference source not found.**

## 5.7 Functional Architecture

The definition of the functional architecture is still premature at this stage. The objective of this section is to describe in detail figure 6 and also to describe the main information flows among the main elements of the security certifications.

This can be done only when all the other elements of the framework have been evaluated and assessed.

## 5.8 Trusted applications

This section is used to define how the security certification of products and devices can be used to enhance the trust of application or system. The main concept is that certified devices and products with a specific label can be used to build a trusted application or systems. Note that this concept has been criticized in (ERNICIP 2014) and other sources, because some security properties (authentication) may not be composed. For example, an application, which has been built only with security products, which are security certified for a specific level (and they have an appropriate label) does not automatically imply that the application will be successfully certified for that level, even if they are in the same domain. This topic is still discussed. The key issue is that the formal

modelling of a system and its components from a security certification point of view is a complex task. The Horizon 2020 ARMOUR project ([www.armour-project.eu](http://www.armour-project.eu)) has the objective to answer this question and define a formal framework for the security certification of products and systems, which links the formal definition of the system, the protection profiles, the set of tests to be executed for the certification and finally the labelling process.

## 5.9 Market surveillance and monitoring

Security certification is an important element to build trust in IoT products/systems/applications but it is disputable if it can reach full coverage.

Historically the owner of a device was responsible for maintaining it. As time went on and technology became more complex, vendor after-sales organisations and third-party maintainers have started to play a role, along with regulators. The process of patching and upgrading is part of the lifecycle of the IoT device. Even if an efficient re-certification process is put in place (as discussed in the previous section), it is not guaranteed that it resolves all the security issues. In other words, as time goes by, patching alone may not be enough. In a world of complex systems, we can expect more incidents where (as with infusion pumps) each vendor can blame others for a safety incompatibility that kills. It may not be sufficient to certify the safety and security of individual components; we have to test, certify and monitor whole systems. It is already accepted that we certify a whole car, not just its component engine, brakes, steering and so on. It is also accepted that driver training and road design are linked standards. Similarly, once we have millions of autonomous, semi-autonomous and manually-driven vehicles sharing the roads, the safety authorities had better have the authority to look at the whole picture. A similar analysis can be applied to smart city applications or infrastructures.

In addition, IoT applications could also be composed by IoT products, which are not security certified. These products could become the vulnerability of the overall IoT application even if it is mostly built on security certified products. Furthermore, security IoT certification may not include the testing of zero-day vulnerabilities and threats, which were not known at the time of security certification.

A complementary (rather than alternative) approach to support IoT lifecycle of products is to introduce post-market monitoring of IoT devices. In this approach, a monitoring system is set up to collect data (management data or traffic data), which can be used to identify security threats. This approach is not a new concept; actually, fault management or misbehaviour detection system in ICT based infrastructures (e.g., energy, telecommunication) had fulfilled a similar role for many dozens of years.

Recent analysis of security and privacy aspects in IoT have highlighted the possibility to use monitoring solutions and capabilities (Yan 2014), to enhance the overall security of IoT deployment. The challenging aspects (as reported by (Yan 2014)) and others is the scalability and heterogeneity of IoT deployments, which can reach thousands of devices with different technologies or data format. From a semantically point of view, it is also difficult to compare set of data from different IoT devices. Still, in some context like the automotive and the industry sectors where the operational requirements are usually coherent and similar across devices, the deployment of such monitoring systems could be more effective.

The potential approaches for IoT have been proposed by various authors and industry representatives as in (CISCO 2016b) and (Dickson 2016). One of the key concepts is to use machine learning techniques to identify anomalies in the behaviour of IoT deployments once they have reached a point of stability. This means that very dynamic IoT deployments or IoT deployments which are not fully formed, may not receive the benefit of this approach. Machine Learning algorithms based on the management and traffic data originating from IoT devices can be used to identify known security threats (e.g., using supervised learning algorithms) or by identifying anomalies or outliers in normal behaviour (e.g., using one class classifiers). The execution of machine learning



algorithms could be not hosted on the IoT devices themselves because of their limited computing or processing capabilities but a cloud based approach could be used, taking in consideration that cloud-based IoT deployment will be growing in the future.

A monitoring system could exploit a formal representation of the IoT application as provided by the UML schema used in MBT in ARMOUR. The UML/MBT representation of the IoT application could be used as input to the logic of the monitoring system to evaluate the potential vulnerabilities. The results from after market monitoring could also be used to feed a new iteration of the certification process because the reported threats could be used to enhance the MBT model and generate new TTCN test cases.

Recommendation 7: A post certification framework to support the lifecycle of products and to mitigate gaps in the security certification process and execution should be investigated and deployed.

## **5.10 Model based testing (MBT)**

This section has the objective investigate the application of formal and theoretical tools for testing. Research bodies have long investigated the application of formal methods for testing and many examples are provided in the research literature.

The Horizon 2020 ARMOUR project investigates the application of formal methods for testing combined with Testing and Test Control Notation (TTCN) v3 language to support security certification for IoT devices. The JRC is actively participating to this project.

The following text and figures are extracted from the deliverables of ARMOUR (deliverable D2.2). Even if the ARMOUR project is still on progress (it started in February 2016), some results are already useful for the objective of this report and they are provided here.

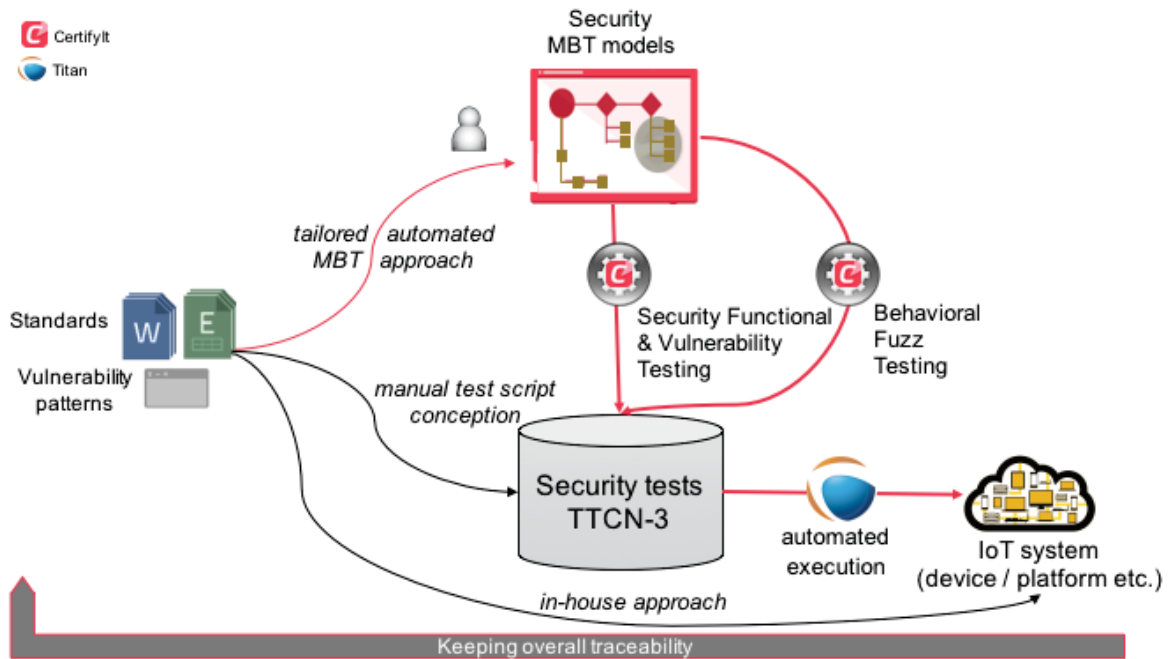


Figure 9 ARMOUR MBT Security Testing Framework

The overall framework is described in Figure 9. The framework is based on the Model-Based Testing (MBT) approach, which has shown their benefits and usefulness for systematic compliance testing of systems that undergo specific standards that define the functional and security requirements of the system.

The structure of the system is modeled by UML class diagrams, while the systems behavior is expressed in Object Constraint Language (OCL) pre- and postconditions. Functional tests are obtained by applying a structural coverage of the OCL code describing the operations of the SUT (functional requirements). This approach in the context of security testing is complemented by dynamic test selection criteria called Test Purposes that make it possible to generate additional tests that would not be produced by a structural test selection criterion, for instance misuse of the system (Model-Based Security Functional Testing) and vulnerability tests, trying to bypass existing security mechanisms (Model-Based Vulnerability Testing). These two approaches generate a set of test cases that is stored into a database and then executed on the IoT system under test. In the ARMOUR project, the tests are defined using the TTCN v.3 language, which has been widely used for many years (in the previous versions) to test large communication systems.

The advantages of using MBT in combination with TTCN are the following:

1. The automation of the test supports a faster and more uniform testing.
2. The adoption of MBT support a formal definition of the tests and the security requirements, which drives the certification. In addition, they can be used to support harmonization of the tests for security certification.
3. MBT and TTCN suites can be linked directly to the labelling concept described in the other sections of this report.

Recommendation 8: The application of testing models and automated testing suites should be investigated in security certification to improve the efficiency of the security certification process and to address the issue of re-certification after product changes

## **5.11 Inherent risks and uncertainties**

The aim of this section is to discuss the potential risks and uncertainties of the proposed certification framework and identifies the potential show stoppers.

### **5.11.1 Obstacles to implementation**

The European certification scheme described in section 5 will require the definition of various organization bodies and new processes, which will be complex and time consuming to define. Even if existing bodies (accredited labs, SOG-IS) could be key elements, which are already present today, there is a significant amount of work to be done before such a framework (or a similar framework) could be created. In addition, economic aspects could have an impact on the definition of the framework and there are trade-offs (described in this report) between a voluntary and a mandatory (e.g., regulation) approach.

The following key issues are identified:

1. On which regulatory framework, the new security certification framework will be created ? Each domain has already regulatory frameworks in place (road transportation, healthcare), which are going to impose specific requirements, procedures and organizational entities. The question is how these organization entities will interact with the elements defined in section 5.6.
2. There could be considerable resistance from the manufacturers community if security certification is imposed on a non-voluntary basis.
3. The maintenance of the protection profiles, labels and processes could be quite time consuming and complex for the involved organizations.
4. New interfaces must be defined among old organizations and new organizations for the definition of the European security certification framework.
5. Security certification of applications and services can be significantly more complex than security certification of products. While, a clear definition of services and applications is missing in this context, there is the risk that security certification may be difficult to achieve for large and complex ICT applications.

### **5.11.2 Potential negative effects**

While an European security certification framework can provide the benefits described in this report, we should also be careful to introduce negative impacts. A mandatory security certification can introduce additional costs on the manufacturer and the citizen. While some types of products would require secure certification because of safety reasons (healthcare, road transportation) other products may be based on a voluntary basis approach.

From an economic point of view, there is also the risk to introduce market distortion because large/midsize companies would be able to invest more money on the security certification process, while small companies could be excluded by some markets.

The dynamicity of specific domains or technologies (e.g., IoT) introduces the issue of the staticity of security certification, which is already described in the report. This means that if a product is submitted to frequent changes, the security certification will be not worth the effort involved in the initial phases

## 5.12 Recommendations

In this section, we list the main recommendations identified in the previous sections.

- 1) A European security certification scheme should be set-up to overcome the national differences on security certification and support an european-wide cybersecurity market. The key elements of the European certification scheme can include the ones proposed in section 5 or additional ones to be defined.
- 2) The basis for the new European security certification scheme shall be mainly based on the Common Criteria but the issues identified in section 4.1 should be addressed with the definition of new processes. In particular, for the re-certification after product changes.
- 3) A process to define harmonized protection profiles for specific domains should be put in place with the collaboration of existing organizations like SOG-IS or agreements like CCRA.
- 4) The definition of harmonized protection profiles is the basis for the definition of a labelling scheme to support the comparability and visibility of the security certification for end-users. A labelling scheme should be put in place. Labels can be defined on the basis of different dimensions as described in section 5.3.
- 5) Security and privacy requirements should be validated in the same certification process and with the same harmonized protection profiles.
- 6) A process to create accredited security testing centres should be defined. While existing processes can be used, they should be reviewed according to the new security certification framework.
- 7) A post certification framework to support the lifecycle of products and to mitigate gaps in the security certification process and execution should be investigated and deployed.
- 8) The application of testing models and automated testing suites should be investigated in security certification to improve the efficiency of the security certification process and to address the issue of re-certification after product changes.

## 5.13 Policy Options

This section has the objective to identify the main potential policy options for the implementation of the certification framework.

The three main policy options are possible:

- 1) **Encouraging and supporting the certification scheme.** This option envisages the Commission using various soft measures to stimulate and encourage the adoption of security certification in Europe. The aim is to encourage secure certification through non-binding measures, which can include the identification of objectives and the definition of general guidelines. In this policy option, security certification is still on a voluntary basis. There is no harmonization among domains for security certification but actions are put in place to support harmonization of the security certification processes. Labels are defined on a voluntary basis.
- 2) **Definition of harmonized standards and protection profiles at European level.** This option envisages the setting up of organizations and entities or the empowering of existing entities like SOG-IS and ETSI/CEN/CENELEC to define sets of harmonized protection profiles, without enforcing on the manufacturers binding measures. In other words, the EC could financially support the definition of the harmonized protection profiles, but there will not be an enforcing and binding regulation in place. Harmonized profiles across Europe for different domains are defined. Accredited test beds are identified to perform security certification with the same processes across Europe. Labels are identified and defined but only for partial sets of products (e.g., used in the government procurement).
- 3) **Full regulation.** This option envisages a full regulatory approach to secure certification for specific domains or applications. This option covers a scenario where decision-makers and other stakeholders intentionally choose to construct a fully-regulated scheme that will leave no space for derogations, disharmonised approaches or divergent implementations at the Member State or end user level. Although this could take place under other policy options too (e.g., specific policies in the energy or transportation domain), in essence this policy option refers to the intention of decision-makers not to leave the final outcome open to circumstances and the conditions in the market or the Member State level. In this option, harmonized profiles across Europe for different domains are defined and they are closely associated to labels. Labels are used by different types of users and consumers.

## 6 Conclusions

This preliminary report has investigated and identified key issues of existing security certification schemes (e.g., Common Criteria) on the basis of a literature review and input from security experts. In particular, the report has taken in consideration the input from previous reports and publications on the same topic (ESCO-cPPP, AIOTI, IACS) and direct feedback from security experts and security organizations like SOG-IS and ENISA. To address these issues, the report proposes a new European security certification framework, which is able to mitigate the identified issues and supports an European wide cybersecurity market. The key elements of this European security certification framework are based on existing entities (e.g., accredited test labs, SOG-IS) and standards (e.g., evolution of Common Criteria and CSPN) complemented by new processes and organizational structures. In particular, the report recommends the application of formal testing methods (e.g., Model Based Testing) and post-certification monitoring.

The preliminary concepts proposed in this report should be further assessed and evaluated with the directorates of the European Commission to evaluate the feasibility of the concepts in different domains (e.g., road transportation, energy), members of the industry community (ESCO-cPPP, AIOTI, IACS), member states SOG-IS and other stakeholders (ENISA).

## References

(Anderson 2008)	Anderson, R., Böhme, R., Clayton, R., & Moore, T. (2008). Security economics and the internal market. Study commissioned by ENISA.
(Anderson 2009)	Anderson, R., & Fuloria, S. Certification and evaluation: A security economics perspective. In <i>Emerging Technologies &amp; Factory Automation, 2009. ETFA 2009. IEEE Conference on</i> (pp. 1-7). IEEE. Sempptember 2009.
(ANSSI 2015)	ANSSI security certification <a href="http://www.ssi.gouv.fr/uploads/2014/10/certification_en.pdf">http://www.ssi.gouv.fr/uploads/2014/10/certification_en.pdf</a> . Last accessed 12/June/2016.
(Arstechnica 2016)	Underwriters Labs refuses to share new IoT cybersecurity standard <a href="http://arstechnica.com/security/2016/04/underwriters-labs-refuses-to-share-new-iot-cybersecurity-standard">http://arstechnica.com/security/2016/04/underwriters-labs-refuses-to-share-new-iot-cybersecurity-standard</a> . Last accessed 12/June/2016.
(Beznosov 2004)	Beznosov, K., & Kruchten, P. (2004). Towards agile security assurance. In <i>Proceedings of the 2004 workshop on New security paradigms</i> (pp. 47-54). ACM.
(BSI 2012)	Technical information on the IT security certification of products, protection profiles and sites. BSI 7138. November 2012.
(CC 2008)	Common Criteria Protection Profile Firewall V2.0 <a href="https://www.commoncriteriaportal.org/files/ppfiles/FW%20PP-93-EN.pdf">https://www.commoncriteriaportal.org/files/ppfiles/FW%20PP-93-EN.pdf</a>
(CC 2012)	Common Criteria Management Committee Vision Statement <a href="http://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRv2.pdf">http://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRv2.pdf</a> . Last accessed 12/June/2016.
(CC 2014)	Collaborative Protection Profiles. The benefits of an evolved Common Criteria Implementation. September 2014. <a href="http://www.ccusersforum.org/library/wp/cPP_White_Paper.pdf">http://www.ccusersforum.org/library/wp/cPP_White_Paper.pdf</a> . Last accessed June 2016.
(CC 2016)	Common Criteria v3.1. Release 4 Part 1: Introduction and general model at <a href="https://www.commoncriteriaportal.org/cc/">https://www.commoncriteriaportal.org/cc/</a> . Last accessed 12/June/2016.
(CCProd 2016)	Common Criteria products <a href="https://www.commoncriteriaportal.org/products/">https://www.commoncriteriaportal.org/products/</a> Last accessed 12/June/2016.
(CCSP 2015)	CCSP - Certified Cloud Security Professional. Official website. URL: <a href="https://www.isc2.org/ccsp/default.aspx">https://www.isc2.org/ccsp/default.aspx</a>
(CESG 2016)	UK ITsec Evaluation & Certification Scheme: UKSP01 - Description of the Scheme. <a href="https://www.cesg.gov.uk/documents/uk-itsec-">https://www.cesg.gov.uk/documents/uk-itsec-</a>

	<p><a href="#">evaluation-certification-scheme-uksp01-description-scheme</a>.</p> <p>Last accessed 12/June/2016.</p>
(CISA 2015)	<p>CISA – Certified Information Systems Auditor. Official website. URL: <a href="http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx">http://www.isaca.org/certification/cisa-certified-information-systems-auditor/pages/default.aspx</a></p>
(CISCO 2016)	<p>Achieve Cyber Security with the Help of Common Criteria Certification.</p> <p><a href="http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/cyber.pdf">http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/cyber.pdf</a>.</p> <p>Last accessed 12/June/2016.</p>
(CISCO 2016b)	<p>Securing the Internet of Things: A Proposed Framework</p> <p><a href="http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html">http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html</a></p>
(CISM 2015)	<p>CISM - Certified Information Security Manager. Official website. URL: <a href="http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx">http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx</a></p>
(CISSP 2015)	<p>CISSP - Certified Information Systems Security Professional . Official website. URL: <a href="https://www.isc2.org/cissp/default.aspx">https://www.isc2.org/cissp/default.aspx</a></p>
(C-ITS 2016)	<p>C-ITS Platform Final Report.</p> <p><a href="http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf">http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf</a></p>
(CRISC 2015)	<p>CRISC - Certified in Risk and Information Systems Control. Official website. URL: <a href="http://www.isaca.org/certification/crisc-certified-in-risk-and-information-systems-control/pages/default.aspx">http://www.isaca.org/certification/crisc-certified-in-risk-and-information-systems-control/pages/default.aspx</a></p>
(Dickson 2016)	<p>Machine learning will be key to securing IoT in smart homes.</p> <p><a href="https://iotsecurityfoundation.org/machine-learning-will-be-key-to-securing-iot-in-smart-homes/">https://iotsecurityfoundation.org/machine-learning-will-be-key-to-securing-iot-in-smart-homes/</a>. Last accessed January 2017.</p>
(Dusart 2008)	<p>Dusart, P., Sauveron, D., Tai-Hoon, K.: Some Limits of Common Criteria Certification.</p> <p>International Journal of Security and its Applications 2(4), 11–20 (2008)</p>
(ECORYS 2011)	<p>Security Regulation, Conformity Assessment &amp; Certification</p> <p>Final Report – Volume I: Main Report</p> <p>Brussels October 2011.</p> <p><a href="http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/secerca_final_report_volume_1_main_report_en.pdf">http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/security/pdf/secerca_final_report_volume_1_main_report_en.pdf</a>.</p> <p>Last accessed 12/June/2016.</p>
(Elmiligi 2016)	<p>Haytham Elmiligi, Fayez Gebali, M. Watheq El-Kharashi, Multi-dimensional analysis of embedded systems security, Microprocessors and Microsystems, Volume 41, March 2016, Pages 29-36, ISSN 0141-9331, <a href="http://dx.doi.org/10.1016/j.micpro.2015.12.005">http://dx.doi.org/10.1016/j.micpro.2015.12.005</a>.</p> <p>Last accessed 12/June/2016.</p>



(ENISA 2014)	Minutes of the Joint EC/ENISA SOG-IS and ICT certification workshop. October 2014 ENISA. <a href="https://www.enisa.europa.eu/events/sog-is/minutes">https://www.enisa.europa.eu/events/sog-is/minutes</a> . Last accessed 6/June/2016.
(ERNICIP 2014)	Proposals from the ERNCIP Thematic Group, "Case Studies for the Cyber-security of Industrial Automation and Control Systems", for a European IACS Components Cyber-security Compliance and Certification Scheme  <a href="https://erncip-project.jrc.ec.europa.eu/component/jdownloads/send/16-case-studies-for-industrial-automation-and-control-systems/60-proposals-from-the-erncip-thematic-group-case-studies-for-the-cyber-security-of-industrial-automation-and-control-systems-for-a-european-iacs-components-cyber-security-compliance-and-certification-scheme?option=com_jdownloads">https://erncip-project.jrc.ec.europa.eu/component/jdownloads/send/16-case-studies-for-industrial-automation-and-control-systems/60-proposals-from-the-erncip-thematic-group-case-studies-for-the-cyber-security-of-industrial-automation-and-control-systems-for-a-european-iacs-components-cyber-security-compliance-and-certification-scheme?option=com_jdownloads</a> .  Last accessed 12/June/2016.
(ETSI 2010)	ETSI EN 302 665, Intelligent Transport Systems (ITS); Communications Architecture <a href="http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf">http://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/en_302665v010101p.pdf</a>
(EU 2008)	REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93
(EU 2013)	EU privacy seals project  Inventory and analysis of privacy certification schemes. Rowena Rodrigues, David Barnard-Wills, David Wright.  <a href="http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26190/">http://bookshop.europa.eu/en/eu-privacy-seals-project-pbLBNA26190/</a>  ISBN: 978-92-79-33275-3
(EU 2014)	DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
(EU 2016)	COMMISSION NOTICE of 5.4.2016 The 'Blue Guide' on the implementation of EU product rules 2016. Brussels, 5.4.2016  C(2016) 1958 final
(EU 2016b)	General Data Protection Regulation.  Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <a href="http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679">http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679</a>

(FIPS 2002)	FIPS PUB 140-2 Security requirements for cryptographic modules. <a href="http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf">http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf</a> . Last accessed 12/June/2016.
(FPIR 2016)	Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things'. Report produced by FPIR for the European Commission – DG JRC, JRC105840.
(GFC 2016)	Global Compliance assessment Forum (GCF). <a href="http://www.globalcertificationforum.org">http://www.globalcertificationforum.org</a> . Last accessed 12/June/2016.
(Hearn 2004)	J. Hearn, "Does the common criteria paradigm have a future?," in IEEE Security & Privacy, vol. 2, no. 1, pp. 64-65, Jan.-Feb. 2004.
(IAPP 2016)	Europe's privacy seal schemes gradually taking shape <a href="https://iapp.org/news/a/europes-privacy-seal-schemes-gradually-taking-shape/">https://iapp.org/news/a/europes-privacy-seal-schemes-gradually-taking-shape/</a>
(ISASecure 2016)	IEC 62443 CONFORMANCE CERTIFICATION Certifying Industrial Control System Devices and Systems <a href="http://www.isasecure.org/en-US/Certification">http://www.isasecure.org/en-US/Certification</a> . Last accessed 12/June/2016.
(ISO 15408)	ISO/IEC 15408. ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.
(ISO 16949)	ISO/TS 16949 Quality management standard for suppliers to the automotive sector
(ITSEC 1991)	Information Technology Security Evaluation Criteria ( ITSEC ) version 1.2. 1991 <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile</a> . Last accessed 12/June/2016.
(Jackson 2007)	Under Attack <a href="https://gcn.com/articles/2007/08/10/under-attack.aspx">https://gcn.com/articles/2007/08/10/under-attack.aspx</a> . Last accessed 12/June/2016.
(Kaluvuri 2014)	"A Quantitative Analysis of Common Criteria Certification Practice" Kaluvuri, Samuel Paul, Bezzi, Michele, Roudier, Yves, Eckert, Claudia, Katsikas, Sokratis K., Pernul, Günther Trust, Privacy, and Security in Digital Business: 11th International Conference, TrustBus 2014, Munich, Germany, September 2-3, 2014. Proceedings Springer International Publishing
(Kaluvuri 2014)	Kaluvuri, Samuel Paul, Michele Bezzi, and Yves Roudier. "A Quantitative Analysis of Common Criteria Certification Practice." In Trust, Privacy, and Security in Digital Business, pp. 132-143.

	Springer International Publishing, 2014.
(Lipner 2015)	S. B. Lipner, "The Birth and Death of the Orange Book," in IEEE Annals of the History of Computing, vol. 37, no. 2, pp. 19-31, Apr.-June 2015.
(Murdoch 2012)	Murdoch, S. J., Bond, M., & Anderson, R. (2012). How certification systems fail: Lessons from the Ware report. IEEE Security & Privacy, 10(6), 40-44.
(NCSA 2011)	"Common Criteria Reforms: Better Security Products through Increased Cooperation with Industry", available at: <a href="http://www.niap-ccevs.org/cc_docs/CC_Community_Paper_10_Jan_2011.pdf">http://www.niap-ccevs.org/cc_docs/CC_Community_Paper_10_Jan_2011.pdf</a> . Last accessed 12/June/2016.
(NIST 2010)	NIST Special Publication 800-37. Guide for Applying the Risk Management Framework to Federal Information Systems. February 2010. <a href="http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf">http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf</a> . Last accessed 12/June/2016.  <a href="https://www.nist.gov/national-voluntary-laboratory-accreditation-program-nvlap/accreditation-vs-certification">https://www.nist.gov/national-voluntary-laboratory-accreditation-program-nvlap/accreditation-vs-certification</a>
(NIST 2016)	National Voluntary Laboratory Accreditation Program (NVLAP). Accreditation vs. Certification.
(Raschke 2014)	Raschke, W., Zilli, M., Baumgartner, P., Loinig, J., Steger, C., & Kreiner, C. (2014, August). Supporting evolving security models for an agile security evaluation. In Evolving Security and Privacy Requirements Engineering (ESPREE), 2014 IEEE 1st Workshop on (pp. 31-36). IEEE.
(RED 2014)	Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance <a href="http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053">http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0053</a> Last accessed 12/September/2016.
(SAAR 2008)	Saar Drimer, Steven J. Murdoch, and Ross Anderson. Thinking inside the box: system-level failures of tamper proofing. In IEEE Symposium on Security and Privacy (Oakland), pages 281–295, May 2008
(Salter 2011)	Common&Criteria & Reforms <a href="https://web.archive.org/web/20120417104556/http://www.niap-ccevs.org:80/cc_docs/CC_Community_Paper_10_Jan_2011.pdf">https://web.archive.org/web/20120417104556/http://www.niap-ccevs.org:80/cc_docs/CC_Community_Paper_10_Jan_2011.pdf</a>

(Sauveron 2007)	D. Sauveron and P. Dusart, "Which Trust Can Be Expected of the Common Criteria Certification at End-User Level?," Future Generation Communication and Networking (FGCN 2007), Jeju, 2007, pp. 423-428.
(Sauveron 2007)	Sauveron, D., Dusart, P.: Which Trust Can Be Expected of the Common Criteria Certification at End-User Level: Future Generation Communication and Networking, 2, 423–428 (2007)
(SOGIS 2016)	Mutual Recognition Agreement Senior Officials Group Information Systems Security (SOG-IS) <a href="http://www.sogis.org/">http://www.sogis.org/</a> . Last accessed 12/June/2016.
(TRUSTe 2016)	TRUSTe Privacy Certification Standards <a href="https://www.truste.com/privacy-certification-standards/">https://www.truste.com/privacy-certification-standards/</a> Last accessed 12/September/2016.
(UL 2016)	UL product testing and evaluation. <a href="http://industries.ul.com/software-and-security/product-security-services/product-testing-and-validation">http://industries.ul.com/software-and-security/product-security-services/product-testing-and-validation</a> . Last accessed 12/June/2016.
(Ware 1979)	Willis H. Ware. Security controls for computer systems: Report of defense science board task force on computer security. Report R-609-1, RAND Corporation, January 1970. Reissued October 1979.
(Yan 2014)	Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of network and computer applications, 42, 120-134.

## List of abbreviations

ANSSI	French Network and Information Security Agency
CAC	Conformity Assessment and Certification
CB	Certification/Validation Body
CCRA	Common Criteria Recognition Arrangement
CESG	Communications-Electronics Security Group
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
C-ITS	Cooperative Intelligent Transportation Systems
CLEFs	Commercial Evaluation Facilities
COAs	Certificate Of Authenticity
CRISC	Certified in Risk and Information Systems Control
CSP	critical security parameters (CSP)
DPA	Differential Power Analysis
EAL	Evaluations Assurance Levels
EDPB	European Data Protection Board
ERNICIP	European Reference Network for Critical Infrastructure Protection
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
IACS	Industrial Automation and Control Systems
IACS	Industrial Automation and Control Systems
IC	Integrated Circuits
ICCS	IACS Compliance & Certification Schemes
IoT	Internet of Things

ISMS	Information Security Management System
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
MBT	Model based testing
NVLAP	National Voluntary Laboratory Accreditation Program
OCL	Object Constraint Language
SIL	Security Integration Levels
SOGIS	Senior Officials Group – Information Systems Security
SPA	Simple Power Analysis
TOE	Target of Evaluation
TTCN	Testing and Test Control Notation

## List of figures

Figure 1 Levels of products evaluation in the Orange book .....	6
Figure 2 Definition of EALs from Common Criteria extracted from (ECORYS 2011). ....	12
Figure 3 ISASecure certification scheme .....	14
Figure 4 ICCF Compliance & Certification Levels. ....	20
Figure 5 C-ITS European Compliance Assessment process .....	29
Figure 6 Overall scheme of the proposed European Security certification scheme .....	35
Figure 7 Label scheme and its dimensions .....	36
Figure 8 Security and Privacy flows.....	38
Figure 9 ARMOUR MBT Security Testing Framework .....	43
Figure 1 Security certification presented by Prof Rannenberga.....	63
Figure 2 Four levels of certification in IACS .....	64
Figure 3 Examples of the application of the testing concepts of ARMOUR project. ....	66

**List of tables**

Table 1 Security Integration Levels in coverage levels in EN50128 (from EN50128 standard) ..... 23

Table 2 Identified issues and criticisms of the Common Criteria approach ..... 24

Table 3 Key elements of the new European security certification scheme against the issues identified in section 3.4.1..... 33



## Annex: Report on the meeting of the experts on the 6<sup>th</sup> of December 2016

### A.1. Background

This meeting was organized to support DG CONNECT Cybersecurity & Digital Privacy – Unit H1 on the definition of an European-wide security certification framework in various domains. The background of this meeting are the COMMISSION STAFF WORKING DOCUMENT Advancing the Internet of Things in Europe SWD(2016) 110/2 and the COMMISSION STAFF WORKING DOCUMENT Contractual Public Private Partnership on Cybersecurity & Accompanying Measures SWD (2016) 216 final, which recommended an improved level of security for IoT devices and applications (SWD(2016 110/2) and the definition of a framework for security certification and labelling in IoT.

In addition to the previous staff working documents, other organizations are also working on the definition of an European security certification framework for specific domains (e.g., IACS or IoT) or in general for cybersecurity products. For example, the European AIOTI (European Alliance of IoT Innovation) Working Group 4 has published a document on the security and privacy aspects of IoT<sup>3</sup> where it is advocated the need for a security certification framework at European level with the concept of IoT Trust label. In a similar way, The European IACS (Industrial Automation and Control Systems) has been working on a security certification framework for IACS products<sup>4</sup>. The European public private partnership on cybersecurity (cPPP) has also started to investigate a potential security certification framework<sup>5</sup>.

We have also to consider that security certification is not a new concept. Actually, as described in previous sections of this report, security certification has a long history of more than 40 years. Then, it is not recommended to reinvent the wheel but rather to mitigate the risks and challenges still present in the most common security certification processes and standards (which has also been described in previous sections of this report).

Representatives of the ARMOUR project were also present at the meeting.

Within this context, an expert meeting was organized on the 6<sup>th</sup> of December 2016 to gather the feedback from security experts on the potential way forward for the definition of an European security certification framework. Experts and representatives from the organizations identified above were invited to the experts meeting to provide their views and the results of their work.

### A.2. Participants

The list of experts invited to the meeting was following:

Name Surname	Company	Representative of Organization/sector
Eireann Leverett	IOActive	IoT
Jacques Olaf Kruse Brandao	NXP	cPPP, cybersecurity in general

<sup>3</sup> Report AIOTI Working Group 4 – Policy. <http://www.aioti.org/wp-content/uploads/2016/10/AIOTIWG04Report2015.pdf>

<sup>4</sup> European IACS Components, Cyber-Security Compliance and Certification Scheme <https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs>

<sup>5</sup> [http://europa.eu/rapid/press-release\\_IP-16-2321\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2321_en.htm).

Arthur van der Wees	Arthur Legal	cPPP, cybersecurity in general
Dr Paul Theron	Thales	IACS
Mr Jean-Christophe Mathieu	Siemens	IACS
Philippe Cousin	Eglobalmark	IoT
Kai Rannenberg	Goethe Universitat	cPPP - IoT
Bruno Legeard	Université de Franche-Comté	IoT
Sergio Lomban	SGS	IoT,
Georg Stuetz	NXP	cPPP, cybersecurity in general

In addition, Gianmarco Baldini, Alessandro Lazari, Ignacio Sanchez from DG JRC, Domenico Ferrara from DG CNECT H1 and Aristotelis Tzafalias DG CNECT H1 were present at the meeting.

### **A.3. Agenda of the meeting**

The agenda of the meeting was following:

<p><b>Experts Meeting on security certification and labelling</b>  <b>6<sup>th</sup> of December 2016</b>  <b>Brussels</b>  <b>avenue de beaulieu 25 - Conference Room 0/S 9</b></p>		
<b>09:00-09:30</b>	<b>Welcome and Tour the table</b>	<i>European Commission, all Domenico Ferrara (DG CNECT)</i>
<b>9:30 – 9:50</b>	<b>Presentation by representative of ECSO</b>	<i>Sergio Lomban for ECSO</i>
<b>9:50 – 10:10</b>	<b>Presentation by AIOTI representative</b>	<i>Arthur van der Wees (Arthur Legal) for AIOTI</i>
<b>10:10 – 10:30</b>	<b>Presentation by Kai Rannenberg</b>	<i>Kai Rannenberg (Goethe University Frankfurt)</i>
<b>10:30-11:00</b>	<b>Presentation by IACS + Q&amp;A</b>	<i>Paul Theron –</i>

		<i>(Thales) and Alessandro Lazari (JRC E.2) IACS</i>
<b>11:00-11:20</b>	<b>Coffee Break</b>	
<b>11:20-11:40</b>	<b>A way forward for security certification in Europe. Key elements and challenges</b>	<i>Gianmarco Baldini (JRC E.3) (presentation not given because of delay introduced by other presentations)</i>
<b>11:40-12:00</b>	<b>Model Based Testing</b>	<i>Philippe Cousin (Eglobalmark) Bruno Legiard (Université de Franche-Comté)</i>
<b>12:00 – 13:00</b>	<b>Discussion on how to address the key challenges for security certification in Europe Part 1</b>	<i>All</i>
<b>13:00-14:00</b>	<b>Lunch</b>	
<b>14:00 – 15:00</b>	<b>Discussion on how to address the key challenges for security certification in Europe Part 2</b>	<i>All</i>
<b>15:00-15:30</b>	<b>Summary of the results of the analysis and identification of the key actions</b>	<i>EC to coordinate, All to participate</i>

In the following section, are provided the presentations by each presenter and the related discussion:

#### **A.4. Presentations and discussions**

##### **Sergio Lomban: The view from the European Cyber Security Organisation of cPPP**

Sergio Lomban presented the view of Working Group 1 (Standardisation, Certification, Labelling, and Supply Chain Management) of ECSO. Mr Lomban explained that ECSO is now composed by many members (89 members) from different categories of stakeholders (government, manufacturers, service providers, certification bodies and so on).

The motivation for the work of WG1 were the following:

- Existing certification schemes can neither cope with the massive deployment and continuous maintenance of hyper-connected devices nor with the aggressive Time-To-Market situation.

- It is very important to continue with a strong focus on building upon existing unique European core expertise, such as the design, evaluation and certification of embedded devices.
- Until 2020 it is expected to have about 50 billions of IoT devices in the field. So-called physical attacks are becoming more and more relevant especially for devices which are physically accessible for an attacker. With the rise of IoT where cars communicate with each other or with critical infrastructures or where health applications are involved, such attacks will become even more dangerous as now human lives are at stake.

The objectives of WG1 are following:

- ECSO will develop a cyber security evaluation and certification framework for the benefit of the protection and security of the European citizen (made visible through a dedicated "label") and to increase the competitiveness of European industry.
- ECSO will include not only devices and products but also the ICT infrastructure, delivery of services and the continuous secure integration of devices and resulting products into larger systems.
- ECSO will draw special attention to the aspect of security & privacy by design including a minimal set of associated requirements to be covered throughout the entire ECO-system of cybersecurity.
- ECSO will take existing technology, company, process and people certification schemes into account including lessons learned regarding modern requirements (e.g. fast deployment and updates in the field, agile development, aggressive time-to-market, ...).
- ECSO will ensure to have the appropriate level of flexibility of the certification framework allowing to customize certification towards the needs of different verticals (car, health, critical infra, home, ...). This also allows to define appropriate mechanisms to protect the certification brand as well.
- ECSO aim to accomplish those tasks via a joint effort hand-in-hand with industrial, public sector, research and academic partners making sure to build upon Europe's unique security & privacy expertise.
- ECSO will leverage the capabilities and work with standardization, certification and normalization bodies while ensuring that the costs of evaluation, testing and certification and compliance does not significantly impact the cost negatively to the end customers.
- ECSO will provide a link to existing (e.g. NIS Directive, eIDAS Directive, GDPR regulations) and future regulations in the policy domain.

The roadmap of ECSO in 2017 will be:

- Evaluation of all existing testing/certification schemes across Europe and globally and to various properties such as product domain applicability, security assurance levels, type of vulnerability assessment, time to market, costs and agility.
- Benchmarking and identifying relevance of each existing scheme as per the requirements of both the public and private sectors.
- Mapping and developing opportunities for harmonization of existing schemes.

- Developing “best practices” solutions within the sub-areas, moving toward a “harmonized” approach to cyber security & privacy a consensus based environment.
- Working with public sector partners to address mutual recognition of “future” schemes.
- Accomplishing a “fast track” process to achieve actual standards.
- Implementing and piloting these testing and certification solutions to demonstrate effectiveness and cost efficiency as well as customer acceptance and trust.

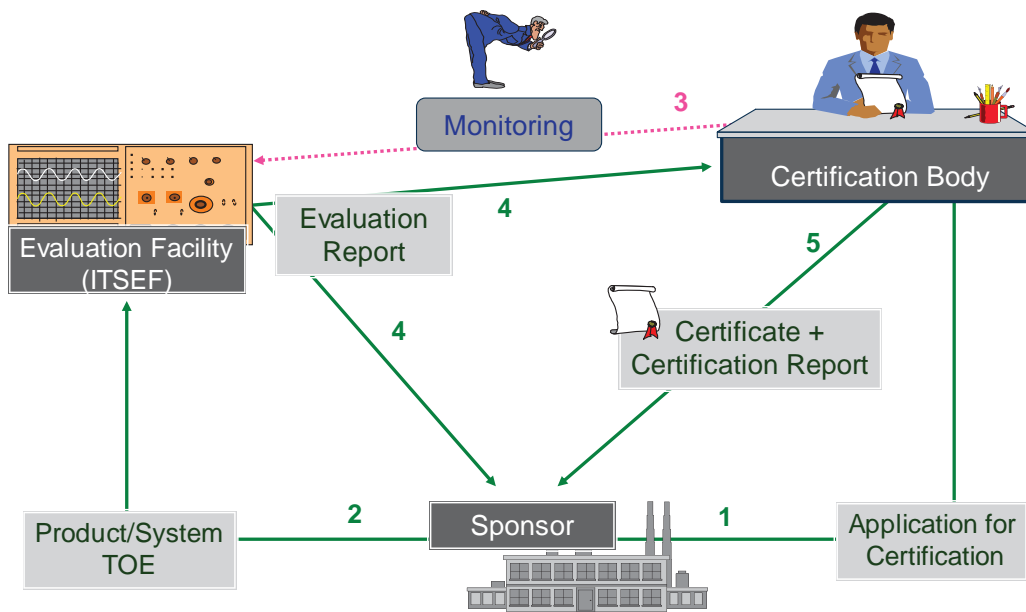
After the presentation, it was discussed how ECSO can work together with the other groups (AIOTI, IACS and the European Commission) to create synergies and harmonize the different efforts.

### **Arthur van der Wees (Arthur Legal)**

Dr Arthur van der Wees provided a multi-angle view about security and data protection in IoT . The presenter said that a multi-angle approach should be pursued because many different stakeholders may be involved. In addition, security experts should focus on the exposed devices: the ones with minor security capabilities or more exposed to external attacks. The rationale is that central infrastructures will be probably protected with physical security and powerful cryptographic solutions while IoT devices with limited power and storage capabilities will not have the same degree of protection. The presenter also linked security to safety in Cyberphysical systems (CPS) or IoT devices used in critical infrastructures. The presenter also supported a vision where security should be a solution rather than a problem also from a business/economic point of view. Better cybersecurity will enable new markets, promote innovation, and give consumers confidence to use new technologies that improve the quality of life. Poor security will likely cause the IoT market to eventually collapse on itself as consumers and other users begin to lose trust in technology from compilations of horror stories & market failure. The presenter also highlighted the need to address the patching process in security certification as software update will be quite common in IoT. He also stressed the value of monitoring of IoT devices after deployment.

### **Kai Rannenberg (Goethe University Frankfurt)**

Prof Rannenberg focused on the complexity of the security certification process as shown in the figure below:



5

Figure 10 Security certification presented by Prof Rannenber

Many different stakeholders are involved in the certification and evaluation process. The presenter also described the need for security certification: people use more and more complex technology to interact in the information society and the users need help or need to know what technology to trust:

- Does the offered system, product or service meet the requirements?
- Does it fulfil legal requirements?
- Is the given organization trustworthy?

Vendors' marketing information does not (always) help as it may be biased. Some kind of independent evaluation and certification is needed, which check products, systems, services or even organization and report on their security/privacy properties. A key issue is how to compare certification results.

From the user point of view, many existing ICT applications and products do not provide transparency on trust. The presenter cited a study from the Federal Ministry of Food, Agriculture and Consumer Protection that 37% of people who don't use a smartphone, explain their refusal with a lack of trust in smartphone devices<sup>6</sup> and they do not have confidence that a smartphone application respects their privacy either. To this purpose the researcher team of the presenter conducted a study to monitor and analyse the behaviour application on a smartphone (project called Privacy4AppMarkets<sup>7</sup>). The application provides a privacy score on the users' app-behaviour ratings. Regarding security certification and labelling, the presenter explained that certification and labelling based on meaningful evaluation is a useful investment but the questions are:

- Who pays and who sets priorities ?
- What to certify/label ?
- What is security in criteria ?
- Is privacy considered/included/covered ?

<sup>6</sup> BMELV 2012, Sicherheit und Datenschutz bei Smartphones, Hintergrundpapier zur Verbraucherumfrage vom Mai 2012. Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz / Federal Ministry of Food, Agriculture and Consumer Protection (Germany).

<sup>7</sup> Gökhan Bal, Kai Rannenber, Jason Hong: Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns; Pp. 187-202 in Computers and Security, Volume 53, September 2015, doi: 10.1016/j.cose.2015.04.004.

From an economic point of view, the smaller the user (citizen/SME) is and:

- more is in need of help with the assessment of products
- more is in need of help with understandings certifications and the meaning of labels
- less budget (directly or indirectly) is seemingly available for certification

Then, the economics aspects are quite important.

### Paul Theron (Thales)

Paul Theron from Thales provided a presentation on the activities of the IACS group, which has been going on for the last two years.

The starting points of the discussion are that:

- IACS & the IoT will be (are already) extremely pervasive & attractive to attackers
- The security of a system is far more complex than that of a component
- So many factors enter into account here (human, technical, physical, processes)
- This is why we have to start by building the foundations of cybersecurity. A SYSTEM will never be secure if its COMPONENTS are not.

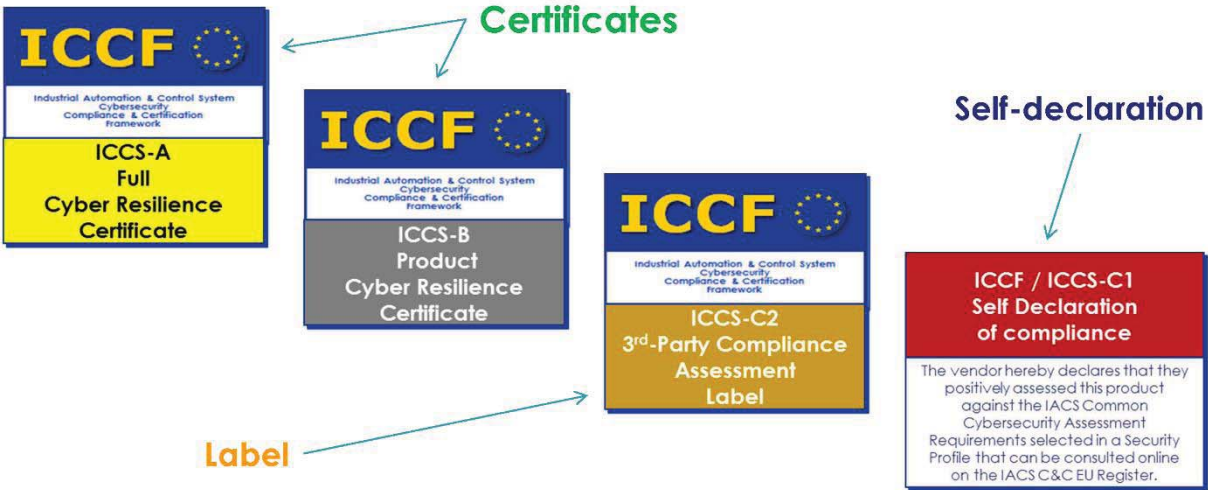


Figure 11 Four levels of certification in IACS

The four levels of certification defined in IACS are shown in Figure 11. The first two levels are the highest level of certification with intrusion testing or other high levels type of test (Cyber Resilience Testing). The last level is a self-declaration of compliance. The first two levels provides a certificate, the third a label and the fourth is a self declaration of compliance.

A technical report, which describes in detail the overall security certification process has already been published by the IACS group. The future steps in 2017 and 2018 are:

1. Global project management and stakeholder engagement;
2. Stakeholders recruitment and liaison (including national agencies, vendors, user industries, certifiers and labs);

3. A one day of ICCF training (for recruited pilot-participants, so as to introduce everyone to the ICCF mindset, concepts, upcoming challenges and vocabulary);
4. Focused pilot projects performed together with vendors, users, national cybersecurity agencies, (National) Labs and Accreditation & Certification bodies;
5. ICCS-A development process assessment;
6. ICCF governance body and processes;
7. Feedback and improvement of the ICCF

The conclusion of the presentation is that the security framework defined by IACS is already a mature process, which could be adopted in other contexts or domains.

**Philippe Cousin (Egloalmark), Bruno Legiard (Université de Franche-Comté):  
ARMOUR project for security certification in IoT and Model Based Testing**

Philippe Cousing and Bruno Legiard provided a presentation on the Horizon 2020 ARMOUR project. The fundamental elements of ARMOUR are Model Based Testing (MBT) and TTCN-3. The first defines the model of the test bed configuration and devices to be tested, while the TTCN-3 test suite is used to implement the test execution.

The presenters believe that the ARMOUR approach could enhance the security certification process by addressing the following main issues, which are present in today certification processes:

1. How to make the testing part of the labelling and certification process cheaper ?
  - By building the process on reusable, configurable security test patterns and automated test generation.
  - By easing the work for certification bodies through a common model language, which can also be easy extended.
  - By directly correlating the certification scheme with the test patterns to be used.
2. How to ensure the quality and reproducibility of the assessment?
  - The security test patterns (models of MBT and test suites of TTCN-3) should be agreed by the certification authorities.
  - Test automation ensure the replicability of the test execution and test results.
3. How to deal with change?
  - Using the automated testing for continuous monitoring and testing at running stage to keep the certificate update. This means that the models could be used not only to support incremental testing but also to facilitate the monitoring of IoT devices after certification and deployment in the field.

Then, the presenters have shown an example of large scale testing, where these concepts have been applied:



TP_ID	Security Test Patterns
TP_ID 6	Run unauthorized software
TP_ID 8	Resistance to eaves dropping and man in the middle
TP_ID 10	Resistance to Injection Attacks
TP_ID 11	Detection of flaws in authentication

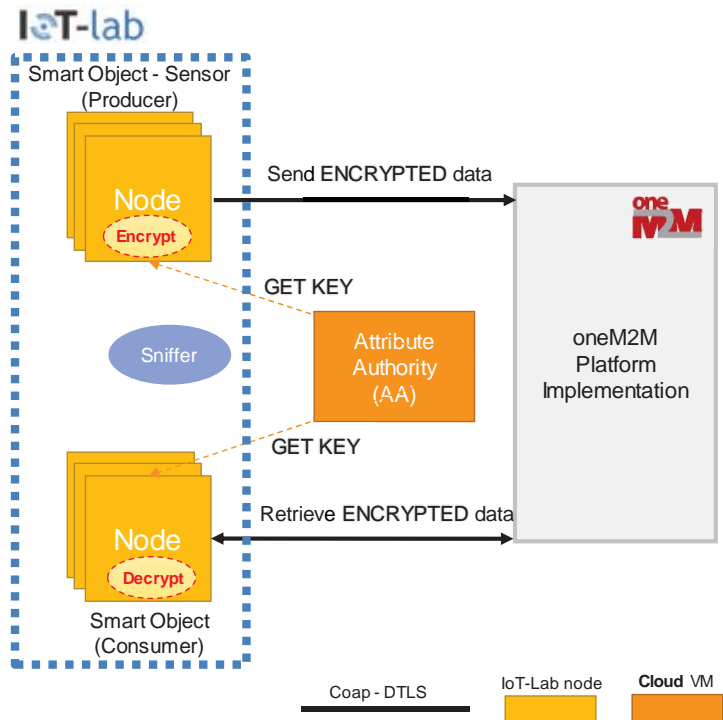


Figure 12 Examples of the application of the testing concepts of ARMOUR project.

In this example, test suites are executed against real IoT devices (based on oneM2M platform implementation) in an IoT test bed. The test bed has been previously modelled using MBT. This is to show that the concepts of ARMOUR are not abstract, but they are applied to real systems and devices.

### Eireann Leverett of IOActive

Eireann Leverett of IOActive provided a presentation on Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things'.

The big challenges identified by the presenter were:

- Established non-IT industries usually have a static approach with pre-market testing to standards that change slowly if at all. The time constant is typically a decade
- Malicious adversaries who can scale bugs into attacks mean we need a dynamic approach with patching, as in IT. The time constant is typically a month

To address these challenges and the need to improve security of IoT products in domains where security threats become safety hazards (e.g., healthcare, road transportation, cyber-physical systems), the presenter provided a set of detailed recommendations:

- Update Product Liability Directive to cope with systems that involve multiple products and services.
- Require vendors to self-certify, for their CE mark, that products are secure by default. This self-certification can be updated if needed to an higher level of certification in a second phase.
- Update NIS Directive to report breaches and vulnerabilities to safety regulators and users.
- Move safety standards bodies towards assessing security and safety together.

- Safety regulators should require a secure development lifecycle with documented vulnerability management following ISO 29174 and ISO 30111 at a minimum
- There is the need move from certifying single products to support the assurance of whole systems including the lifecycle and patch cycle
- Create a European Security Engineering Agency to support policymakers and regulators.

## A.5. Discussion

After the presentations, there was an extensive discussion on how to integrate the different approaches and how it should be the way forward. One of the objectives of the discussion was to identify the main work items and actions items to support DG CNECT in the definition of a roadmap for security certification in Europe.

The following items were identified, grouped by categories:

### 1. Starting point: Which framework to start from ?

It was agreed that the definition of the framework should be based on the following main requirements and features:

- Scalable and flexible framework to foster harmonization of evaluation at European level;
- Flexible choice of reference standards (e.g. sectorial, procurement driven) for security certification. This means that common criteria may be adopted for some domains but other security certification schemes like CSPN could be adopted in other domains.;
- The same framework model to be promoted all over EU;
- Application of concepts from ARMOUR like Model Based Testing and TTCN v3;
- Metrics of evaluation and security requirements are identified by the domain's stakeholder. In other words, the benchmarks are domain specific.
- Human factor has to be considered in the definition of the security profiles. In other words, the security profiles could be adapted to the context where the ICT product or device is used.
- Certification effort should be proportional to the objective (kind of use) of the product.

### 2. Economics of security. Who is going to pay for the security certification costs ?

This topic is focused on addressing the problem of economics of security where users do not purchase the most secure products because they are more expensive than others. In this topic, it was agreed to focus on the following work items:

- Case by case issue. Very dependent on the image factor of the manufacturer;
- Mass market Vs. specific client. Mass market may be based on different security certification levels (self-certification) than specific clients or domains (e.g., energy critical infrastructures).
- Investigate if a procurement-driven approach by government could support the bootstrap of the security certification framework.
- Disrupt the economic model of the attackers. Prioritize the security certification on the threats, which give economical gains to the attackers and mitigate these threats.

### 3. Prioritization of domains (there's no consensus and the question is unclear)

This topic was related to a discussion on the prioritization of the domains. In other words, the security certification framework should be applied to which domains in a first

phase. In addition, the security framework should be focused on products certification, applications or service certification ? The following items/considerations apply:

- Consumer protection Vs. Critical Infrastructures. The item is related to the choice of focusing in a first phase to consumer mass market products for consumer protection or on critical infrastructures.
- Avoidance of social dislocations is the key. The priority could be based on the social impact and disruption (e.g., weak categories of citizens, financial fraud).
- IPR. The priority could be based on the protection of Intellectual property rights.
- Highly sensitive data. The priority could be based on the protection of sensitive data.
- Safety related (e.g. transportation). The priority could be based on the mitigation of safety risks. This means that high priority domains could be transportation, energy or cyber-physical systems.
- Anybody too small to assess security by themselves. The priority could be on the support of small companies or users, who do not have the capabilities to protect themselves in an adequate way (e.g., SME).

#### 4. Security and Privacy

The discussion was on the need to support security certification both for security and privacy requirements.

- It was agreed that we need to refer to the GDPR and investigate further how privacy requirements could be jointly implement with security requirements.

#### 5. Certification based on the processes (e.g., development processes)

The discussion was on the possibility to include the development process (white box testing) as part of the certification but there was no agreement.

#### 6. Governance

- Short, practical steps toward a European Governance should be investigated

#### 7. Role of specific regulations in each domain? What about Radio Equipment Directive (RED) and other regulations/directives ?

- Landscaping the relevant certifications
- Avoid perverse incentives by understanding the regulatory environment before changes for security and privacy.

#### 8. Dynamic changes of products (e.g. patches)

The discussion was focused on how to better support changes of the products like patching.

- Related to the lifetime support of the product
- Product to be recertified only when a substantial change is applied

- What is more valuable? Fast patching or keeping certification valid? Depending on type of products (domain specific).

9. Is a voluntary approach self-sustainable?

- Encouraging stakeholder should lead to voluntary engagement of certification
- Potential issue of international law and market related agreements (import/export)

10. Only security certification of products or also systems and services, which are intrinsically more complex? (There was no clear consensus)

- Focus on certification of products as certifying system is too complex at the moment
- Modular approach starting from products
- Two phases approach? We could focus on security certification first and then certification of application and services.
- We need a definition of products, services and applications to better clarify the categories.
- Post market monitoring can be useful ? The idea is that security certification could be complemented by monitoring of certified products and systems in the field.
- Not every combination of products is more complex than single products.

11. How to align ECSO, AIOTI, SOG-IS, IACS, FIRE

- Action on EC to coordinate the collaboration among the different organizations.

## **A.6. Conclusions of the meeting**

The meeting was successful as it provided a list of work items and issues for the future roadmap on security certification. Each expert provided his opinion on how to define an European security framework for certifications. The overall consensus is that we have to strengthen the security and privacy of connected devices in the future and security certification could be one of the tools. A key aspect is related to harmonization of the security certification processes at European level to support the European Single Market for cybersecurity related products. It was also highlighted the need for complementary tools like the monitoring of the security products after post market deployment. The experience of IACS (Industrial Automation and Control System) in security certification is quite valuable because they have already worked on this topic for years and their lesson learnt could be quite valuable for the definition of a security framework in other domains as well. Another aspect was the distinction between security certification of products and services. Security certification of services or applications can be significantly more complex than security certification of products. At the end of the meeting, a list of key elements to investigate for the future roadmap on security certification and labelling was defined. This is an important input to DG CNECT.

***Europe Direct is a service to help you find answers  
to your questions about the European Union.***

**Freephone number (\*):**

**00 800 6 7 8 9 10 11**

(\* The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (<http://europa.eu>).

## **HOW TO OBTAIN EU PUBLICATIONS**

### **Free publications:**

- one copy:  
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:  
from the European Union's representations ([http://ec.europa.eu/represent\\_en.htm](http://ec.europa.eu/represent_en.htm));  
from the delegations in non-EU countries ([http://eeas.europa.eu/delegations/index\\_en.htm](http://eeas.europa.eu/delegations/index_en.htm));  
by contacting the Europe Direct service ([http://europa.eu/europedirect/index\\_en.htm](http://europa.eu/europedirect/index_en.htm)) or  
calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (\*).

(\* The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

### **Priced publications:**

- via EU Bookshop (<http://bookshop.europa.eu>).



## JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



**EU Science Hub**  
[ec.europa.eu/jrc](https://ec.europa.eu/jrc)



@EU\_ScienceHub



EU Science Hub - Joint Research Centre



Joint Research Centre



EU Science Hub





**Annex 9:**  
**Mapping of cybersecurity sectorial  
initiatives  
at the EU and international level**

*Deliverable prepared by the European Commission and ENISA  
for the Cooperation Group under NIS Directive within the context of the task  
'Discussions related to the security measures for operators of essential  
services'*

***Version 2.0, last updated July 2017***

# Contents

- I. ABOUT THIS DOCUMENT ..... 6
- II. INTRODUCTION ..... 7
  - A. NIS Directive in a nutshell ..... 7
  - B. Key horizontal actors at the EU level ..... 9
- III. .... SECTORS  
10
  - A. ENERGY SECTOR .....10
  - B. TRANSPORT SECTOR.....15
    - 1. Air Transport.....15
    - 2. Land Transport (Rail & Road transport) .....20
    - 3. Maritime Transport.....22
  - C. FINANCE AND BANKING SECTORS .....24
  - D. HEALTH SECTOR .....29
  - E. DRINKING WATER SECTOR .....32

# I. ABOUT THIS DOCUMENT

## ➤ Context

The Directive on Security of Network and Information Systems (NIS Directive)<sup>8</sup> is a major milestone towards building cybersecurity resilience at the European level as it lays out the first EU-wide rules on cybersecurity. Its objective is to achieve a high common level of security of network and information systems within the EU.

The Directive creates the '**Cooperation Group**' between Member States, in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them.

Given that the NIS Directive gives the Member States a certain degree of discretion related to Directive transposition, the Cooperation Group will have a very important role in ensuring that the Directive is transposed and implemented in a convergent manner across different sectors as well as cross borders, to ensure coherent approach across the Union.

During the second informal meeting of the Cooperation Group on 25 October 2016 an agreement was reached on the initial working plan for the first year of work of the Cooperation Group. Among others, the European Commission and the European Network and Information Security Agency (ENISA) were tasked with presenting a **mapping of relevant sectorial initiatives** at the EU and international level in the field of cybersecurity to ensure that both the members of the Cooperation Group and relevant actors at the Member State level involved in the transposition process have a clear overview of work that has already been conducted in the field. This should help coordinate different efforts, ensure coherence and avoid duplication.

## ➤ About this paper

This document, prepared by the European Commission and ENISA, maps ongoing initiatives in the field of cybersecurity across key sectors covered by Chapter III of the NIS Directive: energy, transport, banking and finance, health, drinking water.

Each section presents the most relevant actors in the field - the European Institutions (including relevant experts groups), key agencies (EU and whenever relevant international) involved in the area as well as stakeholder organisations.

Each section also presents a brief policy and regulatory context and enlists key initiatives in the field. Whenever possible, links to relevant documents and information sources are provided to facilitate more detailed information search.

This document is conceived as "**a living document**" and will be regularly updated by the Commission services and ENISA to inform the Cooperation Group about any developments that might be relevant for the transposition process.

Please note that this document focuses on cybersecurity work and initiatives that might be directly related to the transposition of the NIS Directive as this is the main focus of the Cooperation Group work for the next months.

Moving forward and in case the Cooperation Members find it useful, this document could be also extended to take stock of other cybersecurity policy initiatives, which might have an indirect link to the implementation of the NIS Directive (cybercrime and cyber defence activities, cybersecurity market measures, training and education, etc.).

---

<sup>8</sup> <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

## II. INTRODUCTION

### A. NIS Directive in a nutshell

**The Directive on Security of Network and Information Systems** (NIS Directive)<sup>9</sup> was formally adopted on 6 July 2016 and entered into force on 8 August 2016. Member States will have **21 months** to implement the directive into their national laws and **6 months** more to identify operators of essential services.

#### ➤ Cornerstones of the NIS Directive

##### 1) *Improving National Cyber Security Capabilities*

Member States are required to adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cyber security. Member States are also required to designate a national competent authority for the implementation and enforcement of the Directive, as well as **Computer Security Incident Response Teams** (CSIRTs) responsible for handling incidents and risks.

##### 2) *Improving Cooperation*

The Directive creates '**Cooperation Group**' between Member States, in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them. The Commission provides the secretariat for the Cooperation Group.

The Directive also creates the **CSIRTs Network**, in order to promote swift and effective operational cooperation on specific cyber security incidents and sharing information about risks. **The EU Agency for Network and Information Security** (ENISA) provides the secretariat for the CSIRTs Network.

##### 3) *Security and Notification Requirements for Operators of Essential Services*

Businesses with an important role for society and economy, referred in the Directive as "Operators of Essential Services", will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

The Directive covers such operators in the following sectors (ANNEX II of the Directive):

- Energy: electricity, oil and gas
- Transport: air, rail, water and road
- Banking: credit institutions
- Financial Market Infrastructures: trading venues, central counterparties
- Health: healthcare providers
- Water: drinking water supply and distribution
- Digital Infrastructure: internet exchange points (which enable interconnection between the internet's individual networks), domain name system service providers, top level domain name registries

Member States will need to carry out a so-called **identification process** in which they have to define which entities mentioned in Annex II will fall under the scope of the NIS Directive. This identification process will be based on criteria laid down in the directive, such as whether the service provided by the entity is essential for the maintenance of critical societal or economic activities.

---

<sup>9</sup> <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

#### 4) Security and notification requirements for digital service providers

Important digital businesses, referred to in the Directive as "digital service providers" (DSPs), will also be required to take appropriate security measures and to notify incidents to the competent authority. The Directive will cover the following providers:

- Online marketplaces;
- Cloud computing services;
- Search engines

**Table 1: NIS Directive Transposition & Implementation Timeline**

Date	Entry Into Force +	Milestone
<b>Dec. 2016</b>	4 months	Submission of the draft of the first implementing act laying down the procedural arrangements necessary for the functioning of the Cooperation Group to the Network and Information Systems Security Committee <sup>10</sup>
<b>Feb. 2017</b>	6 months	Cooperation Group and CSIRT network begin to perform their tasks
<b>Aug. 2017</b>	12 months	Adoption of implementing acts related to the security and notification requirements for DSPs <sup>11</sup>
<b>Feb. 2018</b>	18 months	Cooperation Group establishes work programme
<b>May 2018</b>	21 months	Transposition into national law
<b>Nov. 2018</b>	27 months	Member States to identify operators of essential services
<b>Nov. 2018</b>	27 months	Member States to submit information to Commission necessary to enable the Commission to assess the implementation of the Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services.
<b>May 2019</b>	33 months (i.e. 1 year after transposition)	Commission report assessing the consistency of Member States' identification of operators of essential services
<b>May 2020</b>	45 months	Member States to review and, where appropriate, update the list of identified operators of essential services
<b>May 2021</b>	57 months (i.e. 3 years after transposition)	Commission review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as well as the scope in relation to operators of essential services and digital service providers

<sup>10</sup> Pursuant to Article 11 (5) of the NIS Directive, the formal deadline for the submission of the first draft is 9 February 2017. The Commission's intention with this early submission is to have the procedural arrangements adopted before the formal launch of the Cooperation Group so that a swift functioning of the Group is ensured from the very beginning.

<sup>11</sup> A first rough draft of the implementing act is planned to be presented to the members of the NIS expert group (which includes representatives of Member States advising the Commission) by end of December 2016 / January 2017.

## **B. Key horizontal actors at the EU level**

In order to avoid repetition, the roles of horizontal actors in the EU-level cybersecurity landscape are described below. Their work applies to all sectors presented in the rest of this document.

**The Directorate General for Communications Networks, Content and Technology**, or **DG Connect** is the Directorate-General of the European Commission responsible for managing policy, regulation and research in the area of information and communication technology. DG Connect and, particularly, its Cybersecurity and Digital Privacy Unit (Unit H.1), is the entity responsible for the support to the transposition and implementation of the NIS Directive and provides Secretariat for the Cooperation Group.

This Unit is also responsible for the contractual Public Private Partnership on cybersecurity, which was signed in July 2016 with the cybersecurity industry represented by the European Cybersecurity Organisation. One of the working groups under the partnership will focus on sectorial dimension of cybersecurity.

ENISA is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA's relevant work across different sectors is mentioned in relevant sections of this document.

The NIS Directive envisages an important supporting role for the Agency for the transposition and implementation of the NIS Directive. In particular, ENISA provides the secretariat to the CSIRTs network, the cornerstone of operational cooperation, and it is also called to assist the Cooperation Group, dealing with strategic cooperation, in the execution of its tasks.

### III. SECTORS

#### A. ENERGY SECTOR

The energy infrastructure is inarguably one of the most complex and most critical infrastructures of a modern society and serves as the backbone for its economic activities and for its security. Given that the energy sector delivers crucial inputs to other sectors, there are important implications also for other parts of the economy.

One of the particularities of the traditional energy sector are its operational technologies, which are historically composed of control systems specifically tailored to operate the physical networks. However, through the increasing shift towards renewable energies and decentralised production, the energy sector of today is undergoing a very rapid change in terms of infrastructure and market.

Digital technologies play an increasingly important role in the energy sector. An ever smarter energy system can perform power generation, transmission, network management and marketing related tasks with much better precision and faster response times than human- dependent systems, thereby saving energy, prioritizing usage, and setting policies for quick response to outages.

But the new efficiency in supply services comes at a price: increased exposure to cyber-attacks and a higher risk for personal data. In a truly cross-sectorial manner, these threats apply to all - generation, transmission and distribution technologies, and to energy market services.

Therefore, ensuring resilience of the EU energy supply system against cyber-threats is becoming increasingly important as wide-spread use of IT and data traffic becomes the foundation for the functioning of infrastructures underlying the energy system.

##### ➤ Relevant European Commission DGs

- The **Directorate-General for Energy (DG ENER)**<sup>12</sup> focuses on developing and implementing policies aiming to deliver a secure, sustainable, and competitive energy for Europe. In particular:
  1.
    - The **Smart Grids Task Force** was set up by DG ENER in 2009 to advise on policy and regulatory issues related to smart grid deployment and development. It consists of five Expert Groups which focus on specific areas. Expert Group 2 aims to mitigate the risks to personal data and security of smart metering systems. This Working Group, under the supervision of DG ENER and DG Joint Research Centre (JRC), has delivered in October 2016 a report on the Identification and Selection of Best Available Techniques<sup>13</sup> that addresses risks related to privacy and security. As a direct action of the Commission Communication "Clean Energy for All Europeans" (COM/2016/0860 final), the European Commission set up a stakeholder working group under the Smart Grids Task Force in spring 2017 to prepare the ground for a network code on energy-specific cyber security until end of 2018.
    - From December 2015 to February 2017, the Energy Expert Cyber Security Platform (EECSP)-Expert Group analysed the energy specific needs in terms of cyber security. This group, set up by DG ENER in cooperation with other Commission services, identified the challenges and the specific needs of the

---

<sup>12</sup> <https://ec.europa.eu/energy>

<sup>13</sup>[https://ec.europa.eu/energy/sites/ener/files/documents/bat\\_wp2\\_techniques\\_mapping\\_and\\_clustering.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/bat_wp2_techniques_mapping_and_clustering.pdf)



energy sector not currently covered under EU legislation. The final report – aiming to advice DG ENER – was published February 2017 at the Commission Website<sup>14</sup>.

2.

- In spring 2017, DG ENER launched a study on the evaluation of risks of cyber incidents and on costs of preventing cyber incidents in the energy sector. The subject matter of the study is to provide a risk assessment of cyber threats in the energy sector as well as an analysis of existing or planned measures to mitigate these risks and their implementation and operational costs. It is planned to finalise and publish the study in the second half of 2018.

- **DG Joint Research Centre (JRC)** supports EU policies providing independent evidences and advices throughout the whole policy cycle. DG JRC's activities also cover the energy and cyber-security sectors.

DG-JRC conducts experimental and research activities in the cyber-security and data protection of the Energy Sector. This includes cyber-security research on smart-metering systems, energy Generation, transmission and distribution infrastructures, the interactions between the grid and smart-home devices, as well as the analysis of the cybersecurity maturity of new energy architecture paradigms (renewable energy micro-grids, distributed ledgers based approaches etc). To conduct its on-field research activities JRC take advantage of some dedicated laboratories and platforms:

- The Energy Distributed Ledger platform
- The Cyber-Security Open Space Laboratory
- The Energy Smart-Grid interoperability laboratory
- The Experimental Platform for ICT Contingencies (EPIC)

3.

Moreover, JRC run also the **Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)**<sup>15</sup> - an initiative of DG ENER, run by DG JRC - made up of European owners and operators of energy infrastructure in the electricity, the gas and the oil sectors. It allows energy sector operators to exchange information on threat assessment, risk management and cyber security.

#### ➤ **Relevant EU Agencies**

EU policy activities in the **energy sector** are undertaken by the Commission in cooperation with EU Agencies.

**ENISA** supports the EU's initiatives in the field of cybersecurity through awareness raising activities and technical reports. In the energy field, ENISA has, for example, published a report on Smart Grid Security Certification in Europe<sup>16</sup>.

ENISA has published several reports regarding Smart Grids<sup>17</sup>, including:

- Smart Grid Security Certification in Europe
- Smart Grid Security: Recommendations for Europe and Member States
- Appropriate security measures for smart grids
- Communication network interdependencies in smart grids

---

<sup>14</sup> [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

<sup>15</sup> <https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure>

<sup>17</sup> <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids>

ENISA has also published several reports related to ICS/SCADA<sup>18</sup>, including energy aspects:

- A study on Communication Network Interdependencies in ICS/SCADA<sup>19</sup>
- Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors
- Certification of Cyber Security skills of ICS/SCADA professionals
- Good Practices for an EU ICS Testing Coordination Capability
- Window of exposure... a real problem for SCADA systems?
- Can we learn from SCADA security incidents?

Finally, in 2016 ENISA conducted a preparatory study regarding the identification criteria of Operators of Essential Services (OES). ENISA's on-going work for 2017 in the Energy Sector envisages the following reports (to be published in 2017)

- Security measures for OES
- Incident reporting requirements for OES
- Methodology for the identification criteria of OES

The [European Agency for the Cooperation of Energy Regulators](#) (ACER) aims to complement and coordinate the work of national energy regulators at EU level. Among others, ACER supports the implementation of cybersecurity regulation at national level. It also advises the European Commission on the development of network codes for gas<sup>20</sup>.

➤ **Key external European organisations/stakeholder fora in the Energy sector**

- **Council of European Energy Regulators** (CEER)<sup>21</sup>: is a non-profit association which represents the interests of the energy national regulators in the EU. CEER has a dedicated Work Stream on cybersecurity through which national regulators aim to promote exchange of best practices in this area.
- **European Safeguards Research and Development Association** (ESARDA)<sup>22</sup>: is an association of European organisations in the area of safeguards which provides a forum for the exchange of information between nuclear facility operators, safeguards authorities and research bodies. The Commission is fostering regional and international cooperation on cybersecurity in the framework of ESARDA.
- **European Network of Transmission System Operators for Electricity** (ENTSO-E)<sup>23</sup> - **European Network of Transmission System Operators for Gas** (ENTSO-G)<sup>24</sup> represent the interests of transmission system operators for electricity and gas. Both organisations have an interest in cybersecurity, among others.  
For example:
  - ENTSO-G advises the European Commission on the development of network codes for gas<sup>25</sup>.
  - ENTSO-E covers cybersecurity in one of its major projects such as Emergency and Restoration<sup>26</sup> and Regional Security Coordinators<sup>27</sup>. In addition, members of ENTSO-E undertake regular training sessions on how to respond quickly to

---

<sup>18</sup> <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada>

<sup>19</sup> <https://www.enisa.europa.eu/publications/ics-scada-dependencies>

<sup>20</sup> <https://ec.europa.eu/energy/en/topics/markets-and-consumers/wholesale-market/gas-network-codes>

<sup>21</sup> [http://www.ceer.eu/portal/page/portal/EER\\_HOME](http://www.ceer.eu/portal/page/portal/EER_HOME)

<sup>22</sup> <https://esarda.jrc.ec.europa.eu/>

<sup>23</sup> <https://www.entsoe.eu/Pages/default.aspx>

<sup>24</sup> <http://www.entsog.eu/>

<sup>25</sup> <https://ec.europa.eu/energy/en/topics/markets-and-consumers/wholesale-market/gas-network-codes>

<sup>26</sup> <https://www.entsoe.eu/major-projects/network-code-development/emergency-and-restoration/Pages/default.aspx>

<sup>27</sup> <https://www.entsoe.eu/major-projects/RSC/Pages/default.aspx>

any potential attacks and how to protect critical infrastructures<sup>28</sup> .

- **European Associations for Distribution System Operators:** there are four European associations representing electricity distribution system operators, (CEDEC<sup>29</sup>, EDSO<sup>30</sup>, EURELECTRIC<sup>31</sup> and GEODE<sup>32</sup>). Relevant activities in the field of cybersecurity include:
  - Partnerships with relevant stakeholders. For example, in 2016 EDSO and the European Network for Cyber Security (ENCS) signed a Memorandum of Understanding on knowledge exchange for security regulations, effective cyber security practices and standardisation for energy distribution companies<sup>33</sup>.
  - Publication of reports such as Smart grid cybersecurity<sup>34</sup>.
  - Organisation of events such as Cybersecurity in Electricity Distribution Grids<sup>35</sup>.

#### 4.

- **Incident and Threat Information Sharing EU Centre (ITIS-EUC)<sup>36</sup>:** it collects analyses and disseminates information on incidents and vulnerabilities in the energy sector, with the aim to improve the situational awareness of Critical Energy Infrastructures (CEIP). ITIS-EUC relies on a web application through which members (European Agencies and Institutions, TSOs, DSOs, utilities from the gas, electricity and oil sector, etc.) share relevant information.
- **European Energy – Information Sharing Analysis Center<sup>37</sup> (EE-ISAC):** the EE-ISAC was created as result of the DENSEK project<sup>38</sup> (Distributed Energy Security Knowledge) launched by DG Home of the European Commission in 2015. The EE-ISAC provides a platform for members to share information on cyber security and cyber resilience in the energy sector. Members include European utilities, service providers, academia as well as governmental and non-profit organizations

#### 5.

##### ➤ Key Agencies and Organisations at international level

- **The International Energy Agency (IEA)** is an intergovernmental organisation established in the framework of the OECD. It comprises of 29 member countries. Relevant activities in the field of cybersecurity include:
  - Roadmap for the development of smart grids, which also cover cybersecurity aspects<sup>39</sup>
  - Participation in the G7 Workshop on Cyber Security in the Energy Sector<sup>40</sup>

---

<sup>28</sup><https://www.encs.eu/2016/12/01/entso-e-participants-trained-to-better-defend-the-critical-infrastructure-from-cyber-attacks/>

<sup>29</sup> <http://cedec.com/>

<sup>30</sup> <http://www.edsoforsmartgrids.eu/>

<sup>31</sup> <http://www.eurelectric.org/>

<sup>32</sup> <http://www.geode-eu.org/>

<sup>33</sup> <http://www.energycentral.com/c/iu/edso-encs-join-forces-cybersecurity-standardization-europe>

<sup>34</sup> [http://www.eurelectric.org/media/304600/smart\\_grid\\_cyber\\_security\\_report-2016-030-0652-01-e.pdf](http://www.eurelectric.org/media/304600/smart_grid_cyber_security_report-2016-030-0652-01-e.pdf)

<sup>35</sup> <http://www.eurelectric.org/events/2015/cybersecurity-in-electricity-distribution-grids/>

<sup>36</sup> <https://ec.europa.eu/jrc/en/scientific-tool/incident-and-threat-information-sharing-eu-centre-energy-sector-itis-euc>

<sup>37</sup> <http://www.ee-isac.eu/>

<sup>38</sup> <http://www.densek.eu/>

<sup>39</sup> [https://www.iea.org/publications/freepublications/publication/smartgrids\\_roadmap.pdf](https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf)

The **International Atomic Energy Agency (IAEA)**<sup>41</sup> works to promote the safe, secure and peaceful use of nuclear technologies. Though established independently of the United Nations, the IAEA reports to both the UN General Assembly and Security Council. It has set up a **Computer Security Programme** aiming to provide its Member States with expertise and guidance at all stages of the development of an information and computer security programme. As part of this programme, the Agency conducts advisory missions and trains inspectors<sup>42</sup>.

### ➤ **EU Policy & Regulatory environment**

The Energy and Climate for 2030<sup>43</sup> and the Energy Security Strategy<sup>44</sup> are the main EU policy and regulatory framework in this area and cover the internal and external dimension of energy policy. As regards the internal energy market, the creation of Energy Union is a priority of the Juncker's Commission. Launched in February 2015, it covers various five dimensions: energy security, solidarity and trust; a fully integrated European energy market; energy efficiency contributing to moderation of demand; decarbonising the economy; and research, innovation and competitiveness. The aim of the Energy Union is to lead to a sustainable, low carbon and environmentally friendly economy, putting Europe at the forefront of renewable energy production and the fight against global warming. In light of the increasing digitalisation of the energy sector, the Commission intends to develop the Energy Union in synergy with the creation of the Digital Single Market agenda. This includes taking measures to ensure privacy protection and cyber-security.

The recent (2016) Directive on Security of Network and Information Systems (NIS Directive) put specific obligations on providers of essential services including the energy sector (electricity, oil, gas). The EECSP-Expert Group (12/2015-02/2017) was set up to advise the Commission and to reinforce the implementation of the NIS Directive at energy sector level. The group identified the challenges and the specific needs of the energy sector that are not currently covered under EU legislation and proposed the way forward to secure energy systems that provide essential services to European society.<sup>45</sup>

At the same time, cybersecurity has also started to be mainstreamed in energy-specific policy and regulatory initiatives. In 2016, the European Commission presented a package of measures to keep the European Union competitive as the clean energy transition is changing global energy markets. This "Clean Energy for all Europeans" package of 30 November 2016 acknowledges the importance of cyber security for the energy sector, and the need to duly assess cyber-risks and their possible impact on the security of supply. The "Clean Energy for all Europeans" proposals will also require the adoption of measures to prevent and mitigate the risks identified as well as further technical rules for electricity (i.e. a Network Code) on cyber-security to be adopted in the future. The revised security of gas supply regulation also acknowledges the importance of cyber security in gas.

---

<sup>40</sup> <https://www.iea.org/media/topics/engagementworldwide/g7/IEAPresentationonCybersecurityatG7.pdf>

<sup>41</sup> <https://www.iaea.org/>

<sup>42</sup> <https://www.iaea.org/topics/computer-and-information-security>

<sup>43</sup> [http://ec.europa.eu/clima/policies/strategies/2030\\_en](http://ec.europa.eu/clima/policies/strategies/2030_en)

<sup>44</sup> <https://ec.europa.eu/energy/en/topics/energy-strategy/2030-energy-strategy>

<sup>45</sup> Final report: [https://ec.europa.eu/energy/sites/ener/files/documents/eecsp\\_report\\_final.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf)

## B. TRANSPORT SECTOR

The present section focuses on cybersecurity in the three subsectors of the transport sector, namely air transport, maritime transport and land transport (rail and road transport).

### ➤ Key highlights for transport sector

Transport is one of the sectors especially vulnerable to cyber-attacks, in particular through the increasing use of electronic data communication. Digitalisation is expected to become a major enabler of the much needed transformation of today's transport system. The digitalisation in the transport sector is a critical feature in the effort to improve the efficiency and connectivity of transport, and ranges from the design of specific complex IT architectures to the use of off-the-shelf IT products. Transport moves people and goods, therefore and contrary to other sectors that may be also prone to cyber-attacks any failure might have serious consequences including massive loss of lives.

### 1. Air Transport

There is a general consensus among the aviation community that the air transport system needs to be protected against cyber-incidents, and there is a need to provide a holistic response at EU level, which is based on existing policies (such as the EU Cybersecurity Strategy, NIS Directive, EASA Basic Regulation, SES, AVSEC rules) and will be done in close coordination with other parties (Member States, ICAO, ECAC, and like-minded countries).

### ➤ Relevant EU Institutions and other actors

The **European Commission**<sup>46</sup> works together with Member States and stakeholders in addressing vast array of transport policies. Cyber security and cyber resilience in different modes of transport is an emerging issue.

The Commission's Aviation Strategy for Europe<sup>47</sup> highlighted the increasing vulnerability of the aviation system to cybersecurity or cyber safety risks and the need for the Commission and the **European Aviation Safety Agency** (EASA, see below) to address cyber risks for the aviation system. It also insisted on the need for EASA to cooperate with other competent bodies to this effect and proposed to clarify and strengthen EASA's role in the area of cybersecurity under the New Aviation Safety Regulation.

There are a number of regulatory committees and advisory groups the Commission is closely cooperating with, where resilience and cyber security issues are addressed. For aviation these are:

- **Regulatory Committee for Civil Aviation Security (AVSEC)**<sup>48</sup> is addressing the evolving threat to civil aviation. Appropriate authorities (e.g. Civil Aviation authorities, Ministry of transport, etc.) of each Member State are represented including observers from EEA states and ECAC<sup>49</sup>.

---

<sup>46</sup> The department in charge within the European Commission is the 's Directorate-General for Mobility and Transport (DG MOVE), cf. [http://ec.europa.eu/transport/index\\_en.htm](http://ec.europa.eu/transport/index_en.htm)

<sup>47</sup> [COM \(2015\) 598 final](#)

<sup>48</sup> created by Article 19 of Regulation (EC) No. 300/2008

<sup>49</sup> European Civil Aviation Conference

- **Stakeholders Advisory Group on Aviation Security (SAGAS)**<sup>50</sup>, is a formally constituted consultation body that meets approximately 4 times a year, shadowing meetings of AVSEC. It consists of European representative organisations engaged in or directly affected by aviation security including Member States. SAGAS members are very active in the field of cyber security and a re-occurring point on cyber in aviation is regularly on its agenda.

6.

➤ **Relevant Agencies, Key external EU actors and International Organisations**

EU policy activities in **air transport** are undertaken by the Commission also in close cooperation with other bodies such as:

- **European Aviation Safety Agency (EASA)**<sup>51</sup> is an agency of the European Union (EU) with regulatory and executive tasks in the field of civilian aviation safety.

The vulnerability of the aviation system will significantly increase with the implementation of new technologies, with the use of commercial off the shelf software, e-enabled technologies and increasingly interconnected transport and air traffic management systems. Against this background, EASA, in close cooperation with the Commission, developed a roadmap on cyber security<sup>52</sup> in aviation that follows the Commission priorities outlined in the 2015 Digital Single Market Strategy<sup>53</sup> and in the 2013 EU Cybersecurity Strategy.

As a first concrete measure EASA launched a screening of the current rules and practices in aviation and carried out a preliminary impact assessment of underlying rules related to modern aircraft design structures as regards their vulnerability to cyber-attacks.

Furthermore, EASA intends to set up the so-called European Centre for Cyber Security in Aviation (ECCSA) which will build on cooperation with all actors involved from both public and private sector: Member States, airlines, manufactures of aircraft, avionics and ground systems, airports, ANSPs. A link with ENISA<sup>54</sup>, with law enforcement authorities (E3C<sup>55</sup>) and intelligence (INTCEN) is also envisaged.

A Memorandum of Understanding with EU-CERT<sup>56</sup> that has been signed constitutes the 'engine' of ECCSA, i.e. it will provide secured IT infrastructure, but also cybersecurity tools and management services. This shall allow ECCSA to offer specific services to its constituents such as an assessment of cyber incidents and assistance for coordinating the response.

The Roadmap for cooperation between EASA and Eurocontrol also contains a detailed description of the activities led by both organisations in the field of cybersecurity.

<sup>50</sup> created by Article 17 of Regulation (EC) No. 300/2008

<sup>51</sup> <https://www.easa.europa.eu/>

<sup>52</sup> The Roadmap outlines the main areas for action. Two key elements of the programme can be highlighted: (i) creation of the European Center for Cybersecurity in Aviation (ECCSA): This new sectorial structure is intended primarily to serve as a cyber-threat and incident information management platform. Beyond its primary role it is also intended to take proactive, preventive action such as awareness raising or detection. It is foreseen that Members of ECCSA act as key cybersecurity experts in different aviation industry domains, including manufacturers, operators and ANSP; (ii) Rulemaking activities: the proposal for a new Aviation Safety Regulation (foreseen as a successor to current Regulation (EC) No 216/2008) suggests to strengthen the role of EASA. A revision of the relevant implementing regulations covering all domains of the aviation sector (design, manufacturing, maintenance, operation, ATM, airports, licensing) has been launched by EASA and is expected to result in amendments, by the Commission, of existing rules by 2018.

<sup>53</sup> COM(2015) 195 final

<sup>54</sup> European Network and Information Security Agency

<sup>55</sup> Europol's cybersecurity branch

<sup>56</sup> Computer Emergency Response Team for the EU institutions, bodies and agencies

In parallel, the Commission proposes in the amended Aviation Safety Regulation<sup>57</sup> to clarify the role and mandate of EASA related to cyber security and to outline essential cyber security requirements.

- **Single European Sky Air Traffic Management Research (SESAR)**<sup>58</sup>

The SESAR Joint Undertaking (SJU) study on a cybersecurity strategy in aviation<sup>59</sup> concluded on a number of recommendations which need to be followed in the development and deployment of the future Air traffic management system. Currently, SJU is preparing internal standards to ensure that the risks related to cybersecurity are appropriately addressed in all projects. Cybersecurity is now an integral part of the new EU ATM Master Plan<sup>60</sup> and of the SESAR 2020 Work programme. In addition, the SESAR Deployment Manager addresses cybersecurity in SESAR implementation activities following the Deployment Programme specific requirements.

In this light, modernisation of the EU ATM infrastructure will mean that cyber security is taken into account in the design, right from low maturity levels to the actual deployment of the technology.

- **European Civil Aviation conference (ECAC)**<sup>61</sup>

ECAC Cyber study group produced a working paper including the new ECAC Document 30 Recommendations on cyber security and guidance material on security response measures to cyber risks, utilising Member State and industry input. The work of the study group is the result of a joint collaboration between various national bodies and authorities, associations, agencies and experts in the field of ATM and safety.

- **International Civil Aviation Organisation (ICAO)**<sup>62</sup>

The 39<sup>th</sup> ICAO Assembly held in autumn 2016 adopted Cybersecurity Resolution A39-19, based on a joint EU-US submission<sup>63</sup>. It insisted mainly on the need for a holistic approach on cybersecurity involving all domains and for sharing information/best practices at ICAO level. The paper received unanimous support while it recognised that a consistent and coherent strategy for managing cyber threats and risks still needs to be developed. Furthermore, ICAO organised a Cyber security summit in April 2017<sup>64</sup>.

The European Commission works with like-minded countries on a meaningful follow up to the ICAO's Cybersecurity Resolution A39-19 and the recent summit. Clearly, there is the need for a consistent and coherent global strategy.

- **EUROCONTROL**

Eurocontrol<sup>65</sup> is a European intergovernmental organisation. Its aim is to run safe, efficient and environmentally-friendly air traffic operations throughout Europe and to build a Single European Sky that will deliver the air traffic management (ATM) and improve the system's performance in the medium- and long-term.

---

<sup>57</sup> Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC, OJ L 79, 19.3.2008, p. 1–49

<sup>58</sup> <http://www.sesar.eu/>

<sup>59</sup> <http://www.sesarju.eu/newsroom/all-news/study-details-rd-roadmap-atm-cyber-security>

<sup>60</sup> Air Traffic Management

<sup>61</sup> <https://www.ecac-ceac.org/> comprising of 44 European states, DG MOVE is an observer in the study group

<sup>62</sup> International Civil Aviation Organisation, a specialised UN Agency [www.icao.int](http://www.icao.int)

<sup>63</sup> [http://www.icao.int/Meetings/a39/Documents/WP/wp\\_493\\_en.pdf](http://www.icao.int/Meetings/a39/Documents/WP/wp_493_en.pdf)

<sup>64</sup> The ICAO Cybersecurity summit and exhibition, a joint safety and security event with the theme "Making sense of cyber" took place on 4-6 April 2017 in Dubai, UAE.

<sup>65</sup> <https://www.eurocontrol.int/>

When talking about the role of EUROCONTROL in cyber security, there are different aspects to consider. From the Network Manager perspective, EUROCONTROL has a resilience, monitoring and response role. EUROCONTROL is also responsible for crisis response activities. In this regard, through its European Aviation Crisis Coordination Cell, it ensures a proper coordination and response to crisis, including those deriving from cyber-incidents, impacting the EU aviation network.

In terms of non-operational tasks, EUROCONTROL is engaged in raising awareness around cyber-security related issues and supporting Member States in the oversight of ATM security. In addition, EUROCONTROL's training centre in Luxembourg<sup>66</sup> allows for the organisation of ATM security training activities.

Cybersecurity is part of the NEASCOG<sup>67</sup> work programme, which is aimed at developing a cyber-defence policy and recommending the cyber security base line for ATM. But it is also a part of the Education, Awareness and Training plan, which includes 'Promoting awareness through workshops and seminars on topics of interest.

In the context of the Centralised Services (CS)<sup>68</sup> currently under development, the CS 6-7 includes the deployment of a European ATM CERT (Computer Emergency Response Team) and a SOC (Security Operations Centre). The ATM CERT main functions are to collect, generate and distribute ATM relevant cyber intelligence and coordinate pan-European ATM response to ATM relevant cyber-security events/incidents. It will work in coordination with EASA ECCSA.

➤ **EU/International regulatory and policy environment**

7. • **ICAO Chicago Convention, Annex 17<sup>69</sup>**
8. • **ECAC Doc 30, guidance material**
9. • **Regulation (EC) No 300/2008** of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002<sup>70</sup>
10. • **Commission Regulation (EU) No 18/2010<sup>71</sup>** regards Common specifications for the national quality control programme in the field of civil aviation security
11. • **Commission Regulation (EU) No 72/2010<sup>72</sup>** regards the Minimum Standards on Aviation Security
12. • **Commission Implementing Regulation (EU) No 2015/1998<sup>73</sup>** which sets out the detailed measures for the implementation of the common basic standards for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation

---

<sup>66</sup> Accredited as Regional Training Centre of Excellence by ICAO

<sup>67</sup>The NEASCOG was jointly created by Eurocontrol and NATO in the aftermath of 9/11 as the European forum for ATM security in response to new and evolving threats to ATM. It is a civil/military forum bringing together ATM regulators, security authorities and Military from Member States, including NATO Partners (e.g. Mediterranean Dialogue, Ukraine, Russia, etc.); ICAO, ECAC, EC, IATA, IFALPA, IFATCA, CANSO, ANSP, Industry, FAA, and NATO and EUROCONTROL Agencies and Units.

<sup>68</sup> <https://www.eurocontrol.int/centralised-services>

<sup>69</sup> <http://www.icao.int/Security/SFP/Pages/Annex17.aspx>

<sup>70</sup> OJ L 97/72, 9.4.2008

<sup>71</sup> OJ L 7, 12.1.2010, p. 3–14

<sup>72</sup> OJ L 23, 27.1.2010, p. 1–5

<sup>73</sup> OJ L 299, 14.11.2015, p. 1–142



- **Regulation (EC) No 1592/2002<sup>74</sup> which proposes to establish a uniformly high level** of civil aviation safety in Europe as part of creating the single European sky
- 13.
- **Regulation (EC) No 1108/2009<sup>75</sup> which extends EASA's activities towards a "total system approach"**
- 14.
- **Commission Implementing Regulation (EC) No 1035/2011<sup>76</sup> regards common requirements for the provision of air navigation services. It is being revised in order to incorporate last ICAO recommendations for ATM operator's management system. It includes provisions on security management systems**
- 15.
- **Commission Implementing Regulation (EC) No 923/2012<sup>77</sup> regards common rules on air traffic flow management (ATFM)**
- 16.
- **Commission Regulation (EU) No 677/2011<sup>78</sup> regards detailed rules for the implementation of air traffic management (ATM) network functions**
- 17.
- **Commission Regulation (EU) No 551/2004<sup>79</sup> regards the organisation and use of the airspace in the single European sky**
- 18.
- **Commission Regulation (EU) No 376/2014<sup>80</sup> regards the reporting, analysis and follow-up of occurrences in civil aviation**
- 19.
- **Commission Regulation (EU) No 73/2010<sup>81</sup> regards requirements on the quality of aeronautical data and aeronautical information for the Single European Sky**

#### **Additional sources:**

ENISA's report on the cybersecurity aspects for Smart Airports<sup>82</sup>

---

<sup>74</sup> OJ L 240, 7.9.2002, p. 1–21

<sup>75</sup> OJ L 309, 24.11.2009, p. 1–20

<sup>76</sup> OJ L 271, 18.10.2011, p. 1–19

<sup>77</sup> OJ L 196, 21.7.2016, p. 3–43

<sup>78</sup> OJ L 185, 15.7.2011, p. 1–29

<sup>79</sup> OJ L 96, 31.3.2004, p. 20–25

<sup>80</sup> OJ L 122, 24.4.2014, p. 18–43

<sup>81</sup> OJ L 23, 27.1.2010, p. 6–27

<sup>82</sup> <https://www.enisa.europa.eu/publications/securing-smart-airports>

## 2. Land Transport (Rail & Road transport)

### ➤ EU/International regulatory and policy environment

The state of play as regards a comprehensive cyber-security strategy for land transport is far less mature in comparison with the aviation and maritime sectors. There is no effective formal international forum (comparable to ICAO or IMO) leading discussion on land transport security including cyber-security issues. The EU does not have a specific competence on rail cyber security other than that referred to in the NIS Directive.

Land transport covers a range of modes of transport that includes passenger transport by rail, public and urban transport, private vehicles and also freight transport by both road and rail. It is therefore not a homogenous sector and the different forms of transport can have differing security issues and needs which will require some tailoring of the likely solutions.

There are two main challenges for the sector: avoiding the interruption of transport itself in order to assure the flow of freight and passengers and avoiding those transport systems themselves being used as a means for harming people. Additionally, transport operators are very concerned with the risk of financial loss from cyber-attacks, whether this is from hacking with accompanying ransom demands or from fraud targeting revenue transfer systems.

### ➤ Specific issues

- **Moving from legacy to internet linked systems**

The rail and public transport sector is increasingly moving from a pre-internet standalone era of control systems that manage the infrastructure (e.g. signalling developments such as ERTMS and train speed control) to one which is highly connected and dependent on connected technology and internet, in some cases wireless, based communications which significantly increases the potential risks of an incident occurring.

20.

21. There is a risk that such safety critical systems could be the target of jamming or spoofing attacks or remotely taken control of by external parties with the intent of directly causing damage, harm to travellers or for demanding a ransom payment from the operator.

22.

23. Road vehicles and road infrastructure are also developing to become cooperative, connected and highly automated systems. Connectivity is technically known as "Cooperative Intelligent Transport Systems (C-ITS)", which are a group of technologies and applications that enable effective data exchange through wireless technologies, allowing vehicles to become connected with each other, with the road infrastructure and with other road users, including vulnerable road users such as pedestrians, cyclists or motorcyclists.

24.

25. The cyber-security of upcoming vehicle-to-vehicle and vehicle-to-infrastructure communications in terms of C-ITS services is critical, and requires action at European level. Without clear rules, adopted at the Union level, C-ITS deployment in the EU will be delayed as investors are looking for a common approach for the internal market.

26.

- **Disruption of communications**

Although railway systems are designed according to a fail-safe approach, interruption of signals would lead to train stops, but the failure of communications with the train would increase the vulnerability of the system and ability to manage an incident.

27.

- **Cyber-interoperability**

As the EU develops the single European railway area, it is important that all elements of the network move towards interoperability underpinned by common certification systems. However the development of national cyber security strategies and solutions which are not coordinated at the European level increase the risk of the creation of new barriers being put in place. Also in the case of C-ITS, fragmented security solutions will put interoperability and the safety of end-users at risk.

28.

- **Staff Expertise**

There is a general lack of expertise of people who both understand traditional security issues and how to manage them and more specific IT knowledge needed to really understand cyber risks for which they are also responsible.

- **Fraud**

Transport companies are concerned about increasing amounts of fraud being committed by the use of cyber-attacks against their revenue systems.

29.

➤ **Relevant EU Institutions and other actors**

The **European Commission** works together with Member States and stakeholders in addressing a vast array of transport policies. Cyber security and cyber resilience in different modes of transport is an emerging issue.

The principal forum for discussing and collaborating on these issues is through the Commission's **Land Transport Security Experts Group (LANDSEC)**, which assists in formulating and implementing the European Union's activities aimed at developing security policy for land transport. Member States and transport sector stakeholders have voiced their concern about the risk of a harmful attack on the IT systems of the European rail industry. The Group regularly discusses sector and national approaches to cybersecurity amongst the full range of security issues that affect land transport systems.

The Commission commissioned a study for the LANDSEC group which developed guidelines on managing cyber risks for SCADA control systems, data flows in container transport and the outsourcing of IT services. The guidelines were shared with LANDSEC group members in early 2016 via the group's online web-portal (accessible by Member State representatives).

Since October 2014, the Commission has also been working to define clear and common rules on Intelligent Transport, including a common security and certificate policy, allowing for interoperability. In order to enable secure, interoperable and safe operation of C-ITS in Europe, the Commission has adopted the **European strategy on Cooperative Intelligent Transport Systems**<sup>[2]</sup>. This communication includes specific actions on the topic of cyber security. In particular, as announced in the strategy, the Commission is currently working on a delegated act on C-ITS under the **ITS Directive 2010/40/EU**<sup>[3]</sup> and on guidance documents regarding the European C-ITS security and certificate policy, which are expected to be published already in 2017.

➤ **Relevant Agencies, Key external EU actors and International Organisations**

---

<sup>[2]</sup> COM(2016) 766 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0766&from=EN>

<sup>[3]</sup> EC, "Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport", 2010.

The **European Union Agency for Railways (ERA)**<sup>83</sup> is the agency of the European Union (EU) that develops mandatory requirements for European railways and manufacturers in the form of Technical Specifications for Interoperability (TSI). The adoption of a TSI falls into Commission competence. Through the development of technical safety and interoperability standards, the Agency contributes to the implementation of European Union legislation and monitors and disseminates best practices to ensure the interoperability of the rail system. ERA is developing a common approach to safety on the European railway system and contributing to creating a Single European Railway Area without frontiers guaranteeing a high level of safety. While the mandate of ERA does not include security, it can assess the safety consequences that could follow from a security threat.

**ENISA** has created an expert group to cover security and resilience of Intelligent Public Transports in the context of Smart Cities with the aim of contributing to relevant position and policy papers on security topics and to exchange knowledge in the domain of Intelligent Public Transports. It also published two studies in 2016 that set out good cyber security practices of Intelligent Public Transport operators within the context of smart cities<sup>84</sup> and recommend security measures that could be deployed to protect critical assets of Intelligent Public Transport systems<sup>85</sup>.

**The Shift2Rail Joint Undertaking** has identified cyber-security within its Strategic Master Plan as a priority research and innovation activity, specifically in the area of Advanced Traffic Management and Control Systems and has an objective to establish a network of Railway Cyber Security Experts.

**The railway sector** differs in its capabilities in dealing with this issue and is dependent to an extent on the significant differences in both the understanding of and the development of capabilities to manage the cyber security risk across the 28 Member States. However some key railway bodies have been active in developing security guidelines for their members i.e. UIC for railway sector and UITP for urban public transport.

### **3. Maritime Transport**

#### ➤ **Key highlights for the maritime sector**

Maritime cyber security awareness is probably not as advanced, as in the civil aviation sector. It is necessary to undertake and support targeted maritime sector awareness, reinforcing the dialogue with the Shipping industry and the Member States, raising campaigns and cyber security training of shipping companies, port authorities, national authorities including cyber security offices, flag states, etc.

Due to the high ICT complexity, it is a major challenge to ensure adequate maritime cyber security. A common strategy and development of good practices for the technology development and implementation of ICT systems would therefore ensure “security by design” for all critical maritime ICT components.

As current regulatory or best practices initiatives and developments are mainly taking place at international level (IMO and industry/international associations) and focusing mainly on the ships side, further efforts should be deployed in relation to the cyber-security developments from the (port) infrastructure side.

As maritime governance is conducted and enforced at different levels (i.e. international, European, national, other), the International Maritime Organization together with the EU Commission and the Member States are strengthening their efforts in order to progress

---

<sup>83</sup> [www.era.europa.eu/](http://www.era.europa.eu/)

<sup>84</sup> <https://www.enisa.europa.eu/publications/smart-cities-architecture-model>

<sup>85</sup> <https://www.enisa.europa.eu/publications/good-practices-recommendations>

on the cyber-security file (to protect ships as well as infrastructure side), in an effort also to align international and EU policies and initiatives in this sector<sup>86</sup>.

➤ **Relevant EU Institutions and other actors**

As part of its activities in the area of transport, the **European Commission** develops policies in the transport security field. In this context, it is leading a number of initiatives regarding cybersecurity in the transport sector, including maritime.

- **Maritime Security** (MARSEC Committee), **Stakeholders Advisory Group on maritime security** (SAGMAS)

For Maritime, the Commission conducts a regular dialogue with the Member States and Stakeholders in the field of maritime security, through the MARSEC Committee and SAGMAS meetings respectively, where cyber-security issues are also discussed and views and experiences exchanged.

➤ **EU/International regulatory and policy environment**

In the maritime transport, cybersecurity is starting to grow momentum but remains less advanced than in aviation. The first main initiatives have been taken by industry at a global level notably through its main associations BIMCO, ICS-International Chamber of Shipping<sup>87</sup>, by developing for example voluntary Guidelines<sup>88</sup> to help the industry to handle or be prepared for cyber-security threats or how to react to incidents and attacks.

At the international level the 2002 IMO International Ship and Port Facility Security Code (ISPS Code) includes requirements covering the cyber-security dimension of ships.

The IMO guidance document focuses on shipping only, and does not bring ports into the picture, beyond what is the simple ship/port interface, and without entering into the port area, from an infrastructure approach and dimension. This is then an important area (port infrastructure) where developments on cyber-security at global/IMO level are not occurring in parallel with shipping and in which the Commission would like to move forward on as well, with a possible EU initiative.

The Commission is keen to drive this issue forward and as such would already like to base its work in the field on what has been discussed in the IMO and with Industry too. The documents already produced should be used as the basis and foundation of work to be done in the Commission.

---

<sup>86</sup> <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/dependencies-of-maritime-transport-to-icts>

<sup>87</sup> notably through its main associations BIMCO, ICS-International Chamber of Shipping

<sup>88</sup> [https://ec.europa.eu/maritimeaffairs/policy\\_en](https://ec.europa.eu/maritimeaffairs/policy_en)

## C. FINANCE AND BANKING SECTORS

This section focuses on the Finance and Banking sectors which are jointly presented. Finance is considered to include traditional financial institutions (e.g. depository, contractual – insurance companies and pension funds - and investment institutions and FMIs) as well as payment services, which may extend beyond banking.

### ➤ Key highlights for the Finance and Banking sector

The Finance and Banking sector is among the most mature sectors of Operators of Essential Services as defined in the NIS Directive in terms of cybersecurity practices. Cybersecurity is a key concern and security and operational risk and resilience are an integral part of European Commission's DG FISMA's ongoing discussions with the financial sector, national and international regulators. The sector exhibits the following opportunities and challenges in relation to the implementation of the NIS Directive:

#### Opportunities:

- Improve information sharing on cybersecurity incidents between public and private organisations, as well as between private entities.
- Improve/increase governmental support to financial services cybersecurity and resilience through national, sectorial or European-level CSIRTs and ISACs.
- Harmonization of cybersecurity leading-practices and incident reporting procedures across the EU; possibly also across related regulatory requirements (NIS, GDPR, etc.).
- Increased collaboration among EU institutions and authorities on cyber-security related matters: in defining the strategy, requirements and interdependencies.
- Collaboration with other regulators from other sectors: (a) with sectors on which the financial services industry relies on (e.g. telecommunications, energy etc.), and (b) authorities supervising regulation impacting directly or indirectly the cyber-security requirements, e.g. data protection.

#### Challenges:

- Increased regulatory complexity and uncertainty regarding legislation applicable and/or implementation and enforcement.
- Partial coverage of the financial sector by the NIS (only credit institutions, trading venues and central clearing parties) and application of *lex specialis* requirements. Other financial sectors (e.g. payments, insurance, asset management, ...) fall outside scope of NIS.
- Renewed regulatory and oversight fragmentation of financial services sectors due to national approaches in cybersecurity.
- Fragmentation and divergence in security requirements at national, EU and/or international level
- Double-reporting of incidents to a variety of competent authorities possibly in different formats and under different thresholds of significance
- Limited buy-in at Board and senior management level of the importance of the cyber-security issues both at the supervised entities and at the regulators / supervisory authorities.

### ➤ Relevant EU Institutions /bodies

- The **Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA)**<sup>89</sup> is a Directorate-General of the European

---

<sup>89</sup> <http://ec.europa.eu/dgs/finance/>

Commission charged with initiating and implementing EU policy in the area of financial services, including Banking and Finance. As such, DG FISMA is also tasked with sector-specific legislative initiatives regarding or including cybersecurity. Specifically, DG FISMA works on payment security and on the implementation on the financial acquis, which also covers other cyber-security aspects strictly related to financial services.

➤ **Relevant Agencies, Key external EU actors and International Organisations**

- The **European Banking Authority** (EBA)<sup>90</sup> advises both the Financial Institutions but also the legislative authorities (e.g. DG FISMA) and is mandated to assess risks and vulnerabilities in the banking sector which could include cyber security.
- The **European Central Bank** (ECB)<sup>91</sup> as operator and overseer of key financial market infrastructures and via the **Single Supervisory Mechanism** (SSM)<sup>92</sup> has a supervisory role regarding the financial stability for all the banks subject to the Single Supervisory Mechanism; While cybersecurity is not mandated per se, it be considered an implicit part of the mandate within the context of operational risk.
- The **European Securities and Markets Authority** (ESMA)<sup>93</sup> is an independent EU authority whose purpose is to improve investor protection and promote stable, orderly financial markets. In this context, ESMA identifies cyber-attacks as a key risk in the Joint Committee Report on Risks and Vulnerabilities in the EU Financial System<sup>94</sup>.

The **European Insurance and Occupational Pensions Authority** (EIOPA)<sup>95</sup> is a European Union financial regulatory institution whose core responsibilities are to support the stability of the financial system, transparency of markets and financial products as well as the protection of policyholders, pension scheme members and beneficiaries. In its Financial Stability Report of June 2016<sup>96</sup>, EIOPA addresses the increasing exposure of companies to cyber risk.

➤ **Key agencies and organisations at EU level**

- **The European Financial Institutes – Information Sharing and Analysis Centre** (FI-ISAC)<sup>97</sup>, is an independent organisation. ENISA initiated a multi-stakeholder discussion on setting up a European ISAC for the financial sector in 2008, and have contributed to this initiative growth and development ever since. The mission of the European FI-ISAC is information exchange on e-channel, cards, central systems and all ICT related topics including cyber-criminal activity affecting the financial community, vulnerabilities, technology, trends, threats, incidents and case-studies. This information exchange helps each member and the banks in the Member States, to raise awareness on potentials risks, and provides an early warning on new threats and vulnerabilities. Membership consists of country representatives coming from the financial sector, national CSIRT's and Law Enforcement Agencies. Other organisations represented are

---

<sup>90</sup> <https://www.eba.europa.eu/>

<sup>91</sup> [www.ecb.europa.eu/](http://www.ecb.europa.eu/)

<sup>92</sup> [http://ec.europa.eu/finance/general-policy/banking-union/single-supervisory-mechanism/index\\_en.htm](http://ec.europa.eu/finance/general-policy/banking-union/single-supervisory-mechanism/index_en.htm)

<sup>93</sup> [https://europa.eu/european-union/about-eu/agencies/esma\\_en](https://europa.eu/european-union/about-eu/agencies/esma_en)

<sup>94</sup> [https://www.esma.europa.eu/sites/default/files/library/2015/11/jc\\_2015\\_007\\_jc\\_report\\_on\\_risks\\_and\\_vulnerabilities\\_in\\_the\\_eu\\_financial\\_system.pdf](https://www.esma.europa.eu/sites/default/files/library/2015/11/jc_2015_007_jc_report_on_risks_and_vulnerabilities_in_the_eu_financial_system.pdf)

<sup>95</sup> <https://eiopa.europa.eu/>

<sup>96</sup> [https://eiopa.europa.eu/Publications/Reports/Financial\\_Stability\\_Report\\_June\\_2016.pdf](https://eiopa.europa.eu/Publications/Reports/Financial_Stability_Report_June_2016.pdf)

<sup>97</sup> <https://www.fsisac.com/>

ENISA, Europol, the ECB, the European Payments Council (EPC) and the European Commission.

- **FS-ISAC should also be mentioned (is international but has a European chapter)**

30.

➤ **Key agencies and Organisations at International level**

- The **Bank for International Settlements (BIS)**<sup>98</sup> is an international financial institution owned by central banks which fosters international monetary and financial cooperation and serves as a bank for central banks. It hosts the Basel Committee for Banking Supervision (BCBS) and the Committee on Payments and Market Infrastructures (CPMI):
- The **Basel Committee on Banking Supervision (BCBS)** is a committee of banking supervisory authorities that provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide.
- The **Committee on Payments and Market Infrastructures (CPMI)**<sup>99</sup> promotes the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and the wider economy.
- The **International Organization of Securities Commissions (IOSCO)**<sup>100</sup> is an association of organisations that regulate the world's securities and futures markets.
- The International Association of Insurance supervisors performs a similar role for the insurance sector.

31.

- The **G7 Finance Ministers and Central Bank Governors expert group on cybersecurity** was launched by the G7 Leaders to enhance policy coordination and practical cooperation to promote security and stability in cyberspace<sup>101</sup>.
- The **Basel Committee on Banking Supervision (BCBS)**<sup>102</sup> is a committee of banking supervisory authorities that provides a forum for regular cooperation on banking supervisory matters. Its objective is to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide.
- The **Financial Stability Board (FSB)**<sup>103</sup> is an international body that monitors and makes recommendations about the global financial system within the G20 context. The FSB promotes international financial stability by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies.

32.

➤ **EU/international regulatory and policy environment**

The current and evolving regulatory requirement is predominantly characterised by the complexity and uncertainty regarding legislation applicable and/or implementation and enforcement. Specifically, there are two key factors that should be addressed:

---

<sup>98</sup> <https://www.bis.org/>

<sup>99</sup> <https://www.bis.org/cpmi/>

<sup>100</sup> <https://www.iosco.org/>

<sup>101</sup> <http://researchcenter.paloaltonetworks.com/2016/05/cso-in-2016-g7-makes-cybersecurity-a-priority-and-paves-the-way-for-track-1-5-multi-stakeholder-discussions/>

<sup>102</sup> <https://www.bis.org/bcbs/>

<sup>103</sup> <http://www.fsb.org/>



- Double-reporting of incidents to a variety of competent authorities possibly in different formats and under different thresholds of significance;
- Ambiguity in how the NIS Directive and PSD2 – which is intended to serve as *Lex Specialis* for the payment services, superseding the NIS Directive – and GDPR will apply in practice, i.e. what the final reporting landscape would look like for organisations that must report incidents under either framework.

At the regulatory level, several EU legislative initiatives in the Finance and Banking services sector implicitly relate to cybersecurity requirements, even though such requirements may not be explicitly mentioned. Examples of this include:

- **Directive EU/2015/2366** on payment services in the internal market (**PSD2**) addresses secure communication, secure customer authentication and incident reporting jointly to EBA and ECB. ENISA is mentioned as an advisor to EBA and ECB in Articles 95 & 96 of the PSD2. PSD2 foresees that Financial Institutions are obliged to report cybersecurity incidents to the assigned National Authority, which in turn reports the incident to the EBA and the ECB, who facilitate information sharing among the Member States if needed. In fact, information sharing is mandated in PSD2 between the National Competent Authorities and EBA/ECB.
- The **Central Securities Depositories (CSD) Regulation** (Article 45) which states the need for CSDs to apply appropriate IT tools in order to identify, monitor and manage sources of operational risk, both internal and external;
- The **European Markets Infrastructure Regulation (EMIR)** and the Commission Delegated Regulation 153/2013 (Article 9) which contain provisions on the need for central counterparties (CCPs) to maintain adequate IT systems for dealing with the complexity of services provided and to ensure high standards of security and confidentiality of the information they hold;
- The **Capital Requirements Regulation** (Regulation 2013/575/EU on Prudential Requirements for Credit Institutions and Investment Firms) and the **Capital Requirements Directive** (Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms) (**CRR/CRD IV**) whose operational risk requirements for financial institutions are relevant to IT-related risks, and are complemented with 'soft law' (e.g. guidelines) issued by the EBA;
- Article 16 of the **Markets in Financial Instruments Directive (MiFID)** which requires investment firms to 'have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, effective control and safeguard arrangements for information processing systems (Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU);
- The **Solvency II Directive** which contains provisions on the specification of the operational risk module of the standard formula; Article 107 of Solvency II sets out capital requirements for operational risk for insurance and reinsurance undertakings, which also includes risks from IT incidents and cyber-attacks;
- **Regulation 909/2014** on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012;

- **Directive 2013/34/EU** of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC;
- **Regulation (EC) No 462/2013** Of the European Parliament and of the Council of 21 May 2013 amending Regulation (EC) No 1060/2009 on credit rating agencies;
- Commission **Delegated Regulation (EU) No. 449/2012** of 21 March 2012 supplementing Regulation **(EC) No 1060/2009** of the European Parliament and of the Council with regard to regulatory technical standards on information for registration and certification of credit rating agencies;
- International level (regulatory example/brief explanation about what it is) and how it links with the European context.

At a policy level, DG FISMA addresses security and operational risk and resilience are an integral part of their ongoing discussions with the financial sector, national and international regulators. Among DG FISMA's ongoing activities in terms of policy are the following:

- Commission Fintech Taskforce work stream on cybersecurity and operational risk
- DG FISMA is involved in the work of Financial Services Committee
- Payment Services Directive II implementation

The EBA's policy activities in this sector include the following:

- The EBA published and submitted to the Commission its final draft Regulatory Technical Standards specifying the Advanced Management Approach in December 2015 (EBA/RTS/2015/02).
- EBA Guidelines on the security of internet payments
- EBA security-related mandates under PSD2, including Guidelines on incident reporting under PSD2, RTS on strong authentication and secure communication, Guidelines on Operational Risk & Security Measures and Opinion on use of Cloud services in the banking sector
- EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) – consultation paper published

ENISA's activities, publications and recommendations in the domain include, among others:

- Guidelines for security in Mobile Payments and Digital Wallets
- Guidelines for secure use of cloud computing in the Finance Sector
- Network and Information Security in the Finance Sector - comparative analysis across Member States
- Security of blockchain
- Ongoing reports (to be delivered in 2017) on the recommendations and support for the implementation of the NIS Directive, including the finance and banking sector

CPMI/IOSCO are also active in the Guidelines and regulatory technical standards for the sector:

- CPMI-IOSCO Principles for FMIs
33. CPMI-IOSCO Cyber resilience guidance for FMIs

## D. HEALTH SECTOR

### ➤ Key highlights for the Health sector

Overall, the level of cybersecurity maturity in the health sector is lower than that of other sectors as the topic has only in recent years started to get significant traction beyond the Data Protection aspects. The NIS Directive is the first legislative initiative to establish a specific regulatory environment for cybersecurity in the Health sector.

The cybersecurity challenge in the health sector is amplified by the variety of actors involved in the respective processes (outpatient care providers, inpatient care providers, medical device manufacturers, pharmaceutical industry etc.) and the varying degrees of cybersecurity maturity across the different actor categories.

Due to the heterogeneity and complexity of the health sector and the resulting landscape of cybersecurity considerations, a number of different actors are involved in policy making, each addressing a different facet of cybersecurity in health.

### ➤ Relevant EU Institutions /bodies

#### 34.

- The **Directorate-General for Health and Food Safety (DG SANTE)**<sup>104</sup> has a horizontal role in healthcare for legislative initiatives. Specifically unit B3 on cross-border healthcare and eHealth deals with eHealth related topic in the context of cross-border healthcare. The unit is placing much emphasis on the improvement of eHealth interoperability and standardisation through the building of the eHealth Digital Service Infrastructure (eHDSI). The eHDSI allows Member States to exchange health data (ePrescriptions and Patient Summaries) with other Member States.
- **The Directorate-General for Communications Networks, Content & Technology (DG Connect)** has established a specific Unit for eHealth within the Digital Society, Trust and Cyber Security Directorate, namely the **e-Health, Well-being, and Ageing Unit (Unit H.3)**. Unit H.3 leads the Mobile Health (mHealth)<sup>105</sup> initiative as a sub-segment of eHealth which covers medical and public health practice supported by mobile devices. It especially includes the use of mobile communication devices for health and well-being services and information purposes as well as mobile health applications.
- The **Directorate-General for the Internal Market, Industry, Entrepreneurship and SMEs (DG GROWTH)** leads legislative initiatives regarding the medical devices aspect of healthcare<sup>106</sup> within the context of its SME initiatives related to the industry for medical devices, where cybersecurity of these devices is identified as a key aspect.

#### 35.

### ➤ Relevant Agencies, Key external EU actors and International Organisations

#### 36.

- In accordance with the Cross-border Healthcare Directive (2011/24/eu), DG SANTE has created and is managing the **eHealth Network**<sup>107</sup>, a voluntary network of Member State representatives dealing with eHealth in the EU. The

<sup>104</sup> [http://ec.europa.eu/dgs/health\\_food-safety/index\\_en.htm](http://ec.europa.eu/dgs/health_food-safety/index_en.htm)

<sup>105</sup> <https://ec.europa.eu/digital-single-market/en/mhealth>

<sup>106</sup> [https://ec.europa.eu/growth/sectors/medical-devices\\_en](https://ec.europa.eu/growth/sectors/medical-devices_en)

<sup>107</sup> [http://ec.europa.eu/health/ehealth/policy/network/index\\_en.htm](http://ec.europa.eu/health/ehealth/policy/network/index_en.htm)

eHealth Network's activities are related to strategic aspects concerning eHealth. The Cross border healthcare and eHealth Unit of DG SANTE provide the secretariat, supported by e-Health, Well-being, and Ageing Unit of DG CNECT.

- **JAsEHN<sup>108</sup>** or the **Joint Action supporting the eHealth Network** serves as the main preparatory body for the eHealth Network to develop political recommendations and other instruments for cooperation in the four specific priority areas that are defined in the eHealth Network's Multiannual Work Plan (MWP) 2015-2018, namely interoperability and standardization, monitoring and assessment of implementation, exchange of knowledge and global cooperation and positioning.

37.

➤ **EU regulatory and policy environment**

There is no significantly developed regulatory framework when it comes to cybersecurity in the Health sector. Data Protection is traditionally considered to be of great importance for electronic patient and health data so the **Data Protection Directive 95/46/EC<sup>109</sup>** and its successor the new **General Data Protection Regulation (GDPR)<sup>110</sup>** are of particular relevance.

The main regulatory framework on which eHealth is based is the **Directive 2011/24/eu<sup>111</sup> on the application of patients' rights in cross-border healthcare**. Cybersecurity is however not included for consideration in this Directive.

The Commission has published a Staff Working Document<sup>112</sup> on the existing EU legal framework applicable to lifestyle and wellbeing apps, providing legal guidance on EU legislation in the field to app developers, medical device manufacturers, digital distribution platforms, etc. Other European mHealth initiatives include the **Privacy Code of Conduct for mHealth apps<sup>113</sup>**, led by the EC based on the 2014 Green paper on mHealth<sup>114</sup>, with the support of industry and based on the GDPR which covers the topics of privacy and security in mHealth apps and the **mHealth assessment guidelines working group<sup>115</sup>**, comprising representatives of patients, health professionals and providers, payers, industry, academia and public authorities which is appointed to provide common quality criteria and assessment methodologies that could help different stakeholders, in particular end-users, in assessing the validity and reliability of mobile health applications.

A new **Medical Devices Regulation (MDR)<sup>116</sup>** is currently under evaluation to replace the existing Medical Device Directive<sup>117</sup> (Council Directive 93/42/EEC of 14 June 1993) concerning medical devices. The MDR will include specific cybersecurity requirements for medical device manufacturers.

ENISA's activities, publications and recommendations in the domain include, among others:

- Report on Security and Resilience in eHealth Infrastructures and Services<sup>118</sup>
- Report on Cyber security and resilience for Smart Hospitals<sup>119</sup>

---

<sup>108</sup> <http://jasehn.eu/>

<sup>109</sup> <http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046>

<sup>110</sup> [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)

<sup>111</sup> <http://data.europa.eu/eli/dir/2011/24/oj>

<sup>112</sup> <https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-existing-eu-legal-framework-applicable-lifestyle-and>

<sup>113</sup> <https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps>

<sup>114</sup> <https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth>

<sup>115</sup> <https://ec.europa.eu/digital-single-market/en/news/new-eu-working-group-aims-draft-guidelines-improve-mhealth-apps-data-quality>

<sup>116</sup> <http://data.consilium.europa.eu/doc/document/ST-11662-2016-INIT/en/pdf>

<sup>117</sup> [https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices\\_en](https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/medical-devices_en)

<sup>118</sup> <https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services>

- Report of Cloud Security for eHealth (to be delivered in 2017)
- Self-assessment cybersecurity maturity questionnaire for Healthcare Organisations (to be delivered in 2017)
- Ongoing reports (to be delivered in 2017) on the recommendations and support for the implementation of the NIS Directive, including the Health sector

38.

## E. DRINKING WATER SECTOR

The present section focuses on cybersecurity issues in Sector 6 of Annex II, namely Drinking Water Supply and Distribution.

### ➤ Key highlights for the Drinking Water Sector

The key challenge for the drinking water sector in terms of cybersecurity is the risk of possible malicious contamination of drinking water with chemicals. A further concern is the security of supply, meaning that the drinking water distribution could be interrupted by cyberattacks on control systems, pumps, etc.

### ➤ Relevant EU Institutions /bodies

- The European Commission's DG ENVIRONMENT (Unit C2) is responsible for the Drinking Water Directive (DWD) 98/83/EC<sup>120</sup>. Please note that the implementation in Member States is almost exclusively done by the Ministries of Health.
- An Expert Group is established under the Directive to provide advice and expertise to the Commission and its services in relation to its implementation. The Group meets every 6-9 months. Documents are available on CIRCABC<sup>121</sup>.
- Security issues are also tackled by the European Reference Network for Critical Infrastructure Protection (ERNICIP), Thematic Group Drinking Water, run by the Joint Research Center<sup>122</sup>.

## 39.

### ➤ EU/international regulatory and policy environment

- DWD regulates the quality of drinking water (drinking water safety), but not its supply. It does not address security or emergency issues<sup>123</sup>.
- The directive puts an obligation to inform consumers and to prohibit or restrict the supply if drinking water constitutes a potential danger to human health. The Directive refers to Drinking Water Supplies (= supply zones with uniform water quality). It distinguishes between large supplies > 1000 m<sup>3</sup>/day (or serving more than 5000 people, ~ 11,000 zones in the EU, reporting obligation to the Commission), and small supplies < 1000 m<sup>3</sup>/day (~ 85,000 zones in the EU).
- The Drinking Water Directive is currently under Revision. The REFIT Evaluation was completed on 1 December 2016 (SWD (2016)428 final). The revision of DWD was officially included in Commission Work Programme for 2017<sup>124</sup>. Currently, an Impact Assessment is under preparation (proposal scheduled for end 2017).
- There is currently no intention to extend the scope of the Drinking Water legislation towards security/cybersecurity. However, one of the identified changes to the DWD that is currently being analysed in detail is to introduce a risk-based approach and water safety planning. Thereby it should be taken into account that safety planning and security planning have commonalities. The coherence of responsibilities and measures under both Directives should be ensured.

<sup>120</sup> [http://ec.europa.eu/environment/water/water-drink/index\\_en.html](http://ec.europa.eu/environment/water/water-drink/index_en.html)

<sup>121</sup> <https://circabc.europa.eu/w/browse/79c232d0-c393-43f2-a0e2-1244d0380397>

<sup>122</sup> <https://erncip-project.jrc.ec.europa.eu/networks/tgs/water>

<sup>123</sup> [ENV-DRINKING-WATER@ec.europa.eu](mailto:ENV-DRINKING-WATER@ec.europa.eu)

<sup>124</sup> COM(2016)710 final

- The analogy between 'essential services' and 'very large drinking supplies' should be further analysed as the size of a supply and the number of citizens affected or possibly affected are important factors for the criticality and the risk assessment. Therefore the identification of operators of essential services under the NIS Directive as required under Article 5 of the NIS Directive should take the size and definitions of drinking water supplies/suppliers of the Drinking Water Directive and of a future revision proposal into account.

**Annex 10: Who Is Affected by the Initiative and How?**



This annex describes the practical implications of the preferred option<sup>125</sup> identified in the Impact Assessment for stakeholder groups likely to be directly or indirectly affected by the initiative.

For each stakeholder group, the relevant impacts of the preferred option will be discussed. Wherever possible, potential costs that may be incurred will be indicated.

### **Member States**

Member States are expected to significantly benefit from the initiative. They could count on long-term support of a reinforced agency focusing on areas where it would bring the most added value: i.e. policy development and implementation; information knowledge and awareness raising; research; operational cooperation and crisis management; market related tasks (certification, standardisation). In particular, as an essential part of its activities to support the internal market, ENISA would support EU policy in the field of ICT security certification, by ensuring an administrative maintenance and technical management of a European ICT security certification framework.

The overall expected impact on Member States would include increased capabilities and preparedness to face cyber threats as well as improved cooperation and coordination across Member States on issues of common interest. This should in turn result in increased cybersecurity resilience across the EU and help build trust in the digital single market. At the same time, the preferred option would leave sufficient room for national actions in sensitive areas such as national security.

More in detail, within Member States, two categories of stakeholders would be in particular impacted by the initiative:

#### **1. National Authorities**

They would benefit from various ENISA's products and services, including, among others:

- long-term strategic analyses of cyber threats and incidents helping Member States to identify emerging trends and ways to adapt their cybersecurity efforts;
- EU-wide independent guidance and reports on cybersecurity matters,
- brokerage of expertise and good practices between Member States
- support for review of the national security strategies,
- trainings and training material.

National authorities would be also positively impacted by having ENISA's assistance in the implementation of the NIS Directive and subsequent legislation in cybersecurity. In particular, ENISA's contribution to policy development and implementation in the area of NIS is expected to support cooperation amongst national authorities and regulators across all sectors in the NIS Directive and the telecoms sector to promote best practices and exchange lessons learned amongst sectors.

As far as ICT security certification and labelling is concerned, national authorities would benefit from:

---

<sup>125</sup> The preferred option is a combination of **Option 2** ('Enhanced ENISA') with regard to **ENISA** and **Option 3** (Establishing a European ICT security certification and labelling framework) for **certification and labelling**.

- technical expertise provided by ENISA
- the establishment of an institutional framework that enables to identify common priority areas for security certification and labelling.

An important impact can be also foreseen for national authorities as buyers of ICT products and services. The promotion of certification and labelling under the Framework, would allow national authorities to make more informed purchase decisions. They could e.g. decide to procure ICT solutions with a certain cybersecurity assurance and, thanks to the mutual recognition system, they would reap the full benefits of unfettered competition and cross-border free trade across the Union.

## 2. Computer Security Incident Response Teams (CSIRTs)

National CSIRTs have already strong ties with ENISA, which helped nurturing their capabilities and build their community in the EU. They are expected to benefit from the preferred option as the enhanced ENISA would be able to respond to their needs in a more comprehensive way. In particular, the support would be structured linking the key areas of:

- **capacity building** including e.g. trainings, training material, guidance on improving maturity and establishing KPIs,
- **operational cooperation**, including:
  - technical support for back-end services (e.g. information portal that enables CSIRTs to exchange information on best practices and actual incidents and threats and support voluntary cooperation in case of incidents<sup>126</sup>);
  - drafting and updating CSIRT Network Standard Operating Procedures;
  - pan-European cyber exercises;
  - back-end support for analysis of vulnerabilities, artefacts and incidents in cooperation with CERT-EU and
  - crisis management (for instance, in the context of the Cybersecurity Blueprint collect and aggregate national operational reports and produce a common situational awareness report for decision makers in case of large scale cross-border cybersecurity incidents).

It is estimated that the costs of the initiative for Member States would be limited. In particular, most of the expenses would be borne under the EU budget<sup>127</sup> within the Multiannual Financial Framework. Member States could provide voluntary contribution to ENISA (as it is the case today) and would be required to pay fairly small amounts for the maintenance of the European ICT Security Certification Framework<sup>128</sup>. Additional costs could be expected for those national authorities that intend to participate in the development of future European certification schemes within the Framework.

---

<sup>126</sup> ENISA will host key elements of the Core Service Platform, funded through the CEF programme, which provides the CSIRT Network communication tools and a cooperative environment on which to analyse cybersecurity incidents.

<sup>127</sup> Reference to Annex 6 for the estimates on the costs for ENISA and Annex 7 for the estimates on the costs for the ICT

<sup>128</sup> It is estimated to be approximately EUR 58,000 per year per each Member State.

## **Businesses**

Businesses are expected to be affected by the initiative from different perspectives: as potential victims of cyber incidents, as producers of ICT products (cybersecurity products and/or ICT products that could be certified), as buyers of ICT products. While the changes related to ENISA's mandate are likely to impact businesses across the board, the set-up of the ICT security certification framework impacts in particular the producers and buyers of ICT products and services.

First, the enhanced ENISA would positively impact businesses across different sectors, in particular those operating in critical sectors. A permanent mandate would ensure that ENISA supports businesses in a sustainable manner, providing opportunities both to the Agency and to its constituents for a long term vision and planning of the work. The suggested revision of the Agency's governance, giving more prominent voice to the Permanent Stakeholder Group in defining priorities for the work programme, would allow businesses to receive support better adjusted to their real needs related to increasing cybersecurity capabilities and preparedness. As presented earlier with regard to Member States, businesses would also benefit from the provision of reliable, robust analyses on the threat landscape, incidents and the related existing market solutions as well as from guidance on cyber hygiene that could help better protect their organisations. In particular, the operators of essential services covered by the NIS Directive would benefit from EU-wide good practices, guidelines and recommendations on security measures and incident reporting.

Second, businesses operating in the cybersecurity sector could benefit from the information provided by the Agency's playing the role of a market observatory. ENISA would make available analyses of the main trends in the EU cybersecurity market in order to enhance alignment of the demand and supply sides and thus help enhance the competitiveness of the companies in the sector.

Third, a positive impact can be inferred on the capabilities of private actors, operating within Member States and cross borders, through the contribution of ENISA to the establishment of Information Sharing and Analysis Centres (ISACs) in various sectors. This would include providing best practices and guidance on available tools, procedures as well as appropriately addressing regulatory issues related to information sharing.

Fourth, producers of ICT products that already certify their products and sell them across the EU would be positively impacted by the establishment of the European ICT security certification and labelling framework. The mutual recognition system would allow them to enjoy costs savings by reducing to one the number of certification processes their products need to undergo. The same applies to companies that will be certifying their products in the future. The mutual recognition would also boost the competitiveness of firms operating cross-borders - by providing an incentive to certify their products and thus helping them reap the advantages of increased trust in the digital solutions as well as by gaining access to market segments where certification is required (e.g. some areas of public procurement). As the preferred option is based on voluntary certification and labelling, it would not impose additional costs for producers.

Fifth, the businesses that are buyers of ICT products and services would be positively impacted by the expected increase in the number of certified products/services, stimulated by the policy in this field and the establishment of the framework. This would also increase the amount of available information on the level of assurance of the security properties of products/services and thus increase trust in the digital solutions. In addition, the ICT security certification framework will provide a strong incentive for operators of essential services to require that the products they buy are certified.

Finally, as the ICT security certification framework will provide the possibility for a variety of stakeholders to contribute to future certification activities, industry representatives as well as consumers associations are expected to participate in regular meetings. Such a multi-stakeholder approach would increase transparency and inclusiveness of the process to develop European certification schemes, as well as trust among actors operating in the Digital Single Market.

## **SMEs**

For SMEs and micro-enterprises, the access to free, high quality and independent information, analyses and recommendations provided by the enhanced ENISA can significantly release their budgets, for which investments in cybersecurity can represent a significant burden. This particularly applies to the dissemination of good practices of cyber-hygiene, since this could help limit the overall number of incidents affecting companies, which are currently often due to incorrect human behaviours. However, it has to be noted that the overall positive impact on SMEs and microenterprises might be significantly limited due to the linguistic barriers. Unless the Agency would be able to devote a bigger part of its resources to translation services or national experts cooperating with the agency take on the responsibility for translation, the dissemination of material exclusively in English limits its accessibility throughout the EU.

With regard to certification and labelling, the proposed option would significantly reduce costs and administrative burden for SMEs that already certify (or are willing to certify) their products and services. Even more importantly than in case of big businesses that have usually more resources, the mutual recognition system would allow SMEs to enjoy costs savings by reducing to one the number of certification processes their products need to undergo. It would also eliminate a potential market-entry barrier (for both new business and SMEs) and enable access to a wider cybersecurity market.

### **EU institutions, Agencies and bodies**

The preferred option would positively impact the EU institutions, Agencies and bodies as they could count on an enhanced agency that would better support the EU policy development and implementation, as well as the definition of research priorities on cybersecurity by providing expertise, guidelines and recommendations. This would benefit the institutions, agencies and bodies addressing cybersecurity at both horizontal and sectoral level, including by providing a reference point to ensure coherence between the two.

EU institutions, Agencies and bodies, in their capacity as buyers, would also benefit from the expected increase in the number of certified products and services; and thus from increased information on the level of assurance of the security properties of ICT products and services they procure.

## **Citizens**

A positive, although indirect, impact can be expected on the citizens with regard to their cybersecurity. An enhanced EU agency can contribute to improving cybersecurity resilience, which in turn should increase trust of EU citizens and businesses in the digital society. This is in particular relevant for the protection of citizens' access to essential services, such as energy, healthcare, water, transport, as well as the security of personal data. In addition, the expected increase in the number of certified devices, including consumer goods, could reduce the exposure of citizens to cyber threats.

Furthermore, the preferred option is expected to contribute to raising citizens' awareness of cyber threats and ways to handle them. An enhanced ENISA would engage in a series of activities that are expected to positively impact the overall level of information and knowledge on cyber issues. It would include: the promotion and sharing of best practices from across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies; the provision of advice, guidance and best practices for the cyber hygiene within the organisations; and the regular organisation of awareness raising campaigns in coordination with the responsible authorities in the Member States.

Finally, the promotion of certification and labelling under the ICT security certification Framework, would allow citizens to make more informed purchase decisions related to ICT products and services. This would also enhance a chain of trust among manufacturers and buyers of ICT solutions.

## ***The ICT security certification landscape***

### ***International schemes and other initiatives***

<b>International Scheme and relevant standards</b>	
<b>Scheme</b>	<b>Brief Description</b>
<b>SOG-IS</b>	The Senior Officials Group – Information Systems Security (SOG-IS) agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria. Currently, SOG-IS MRA is the main certification mechanism existing at European level. However, it only includes 12 Member States plus Norway and has developed only a few protection profiles <sup>129</sup> regarding digital products (such as digital tachograph, digital signatures and smart cards).
<b>Common Criteria (also known as ISO 15408)</b> <sup>130</sup> .	The Common Criteria for Information Technology Security Evaluation (commonly known as CC) is an international standard (ISO/IEC 15408) for computer security evaluation. It is based on third party evaluation and envisages 7 Evaluation Assurance Levels (EAL). The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that CC certificates are recognized by all the signatories of the CCRA. Within the current version of CCRA only evaluations up to EAL 2 are mutually recognized.
<b>Information Technology Security Evaluation Criteria (ITSEC)</b>	The Information Technology Security Evaluation Criteria (ITSEC) is a structured set of criteria for evaluating computer security within products and systems. It is still used for some evaluation in the classified information but it has to be considered superseded by the publication of ISO 15408 Common Criteria for ICT security product evaluations.
<b>ISA Secure Certification Programme</b> <sup>131</sup> .	ISASecure is scheme that independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities. The government of Japan has adopted ISASecure as part of their critical infrastructure protection scheme and has set up an

<sup>131</sup> <http://www.isasecure.org/en-US/>

<b>International Scheme and relevant standards</b>	
<b>Scheme</b>	<b>Brief Description</b>
	accredited test lab to process certifications locally in Japan.
<b>Federal Information Processing Standards FIPS-140</b> <sup>132</sup> .	Federal Information Processing Standards (FIPS) are standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.
<b>Industrial Automation and Control Systems (ISA/IEC-62443 /IACS)</b> <sup>133</sup> .	ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). It applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.
<b>EN50128.</b>	It specifies procedures and technical requirements for the development of programmable electronic systems for use in railway control and protection applications
<b>ISO 27001</b> <sup>134</sup> .	ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. The ISO 27001 standard provides a framework that helps organisations: protect clients and employee information; manage risks to information security effectively; achieve compliance; protects the company's brand image.
<b>ISO/IEC 19790 and ISO/IEC 24759</b>	ISO/IEC 19790 and ISO/IEC 24759 are applicable to validate whether the cryptographic core of any security product is properly implementing an approved suite of cryptographic protocols, modes of operation and key sizes, while protecting this implementation and the critical security parameters, such as keys, in accordance to the design and specification requirements laid out in the standards. There are four levels of security defined, and ISO/IEC 19790 includes a variety of possible implementations, both software and hardware.
<b>IECEE CB Scheme</b> <sup>135</sup>	It is operated by the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), is an international system for mutual acceptance of test reports and certificates dealing with the safety of electrical and electronic components, equipment and products. It is a multilateral agreement among participating countries and certification organizations, which aims to facilitate trade by promoting

<sup>132</sup> <http://csrc.nist.gov/groups/STM/cmvp/standards.html>

<sup>133</sup> See: <https://www.isa.org/isa99/>

<sup>134</sup> <https://www.iso.org/standard/54534.html>.

<sup>135</sup> <https://www.iecee.org/about/cb-scheme/>.



International Scheme and relevant standards	
Scheme	Brief Description
	harmonization of national standards with International Standards and cooperation among accepted National Certification Authorities (NCBs) worldwide.

National Scheme	
Member State	Brief Description
<b>France</b> <sup>136</sup>	<p>Certification Sécuritaire de Premier Niveau (CSPN) is an IT Security Certification Scheme established by the National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d'information – ANSSI) in 2008. Its main purpose is to offer a faster and cheaper alternative for IT Security Certification as compared to the CC approach. The security criteria, as well as the evaluation methodology and process are based on an ANSSI created standard. The cost of each CSPN certification is in the region of 25.000 – 35.000 euro while duration of process is approximately of 3 months ( CC evaluation of a smart card can take from 6 months to 1 year). Yearly, ANSSI receives around 50 submissions for certification under CSPN. It issues around 25 CSPN certificates (mainly on software) and 100 CC certificates (mainly hardware) per year. Currently, ANSSI recognises and issues two main types of labels. These labels are used for:</p> <ul style="list-style-type: none"> <li>- certifying products</li> <li>- qualifying products and services</li> </ul>
<b>Germany</b> <sup>137</sup>	The German Federal Office for Information Security (BSI) is developing an approach for low level assurance to improve the efficiency of Common Criteria evaluation.
<b>UK</b>	<p>The <i>Commercial Product Assurance</i> (CPA)<sup>138</sup> is the UK national scheme for commercial off-the-shelf products; products successfully evaluated according to CPA obtain a Foundation Grade certification, meaning that they proved to be good commercial security practice and are suitable for lower threat environments. CPA is open to all vendors, developers and suppliers of security products with a UK sales base. There is no Mutual Recognition Agreement (MRA) for CPA, which means that products tested in the UK will not normally be accepted in other markets. CPA is similar to common criteria, however not so widely recognised outside of UK.</p> <p>Originated in the UK, Cyber Essentials is a government backed cybersecurity scheme designed to guide businesses in protecting themselves against data breaches and cyber threats. Originating from the internet aimed at</p>

<sup>136</sup>Based on information from website (<http://www.ssi.gouv.fr/administration/produits-certifies/cspn/>) and from official case study presentation (ANSSI, 2015).

<sup>137</sup> Based on information reported in the JRC study, Baldini et al. (2017).

<sup>138</sup> <https://www.cesg.gov.uk/scheme/commercial-product-assurance-products-foundation-grade>

<b>National Scheme</b>	
<b>Member State</b>	<b>Brief Description</b>
	<p>an organisation's IT structure.</p> <p>IASME is a UK-based standard for information assurance at small-to-medium enterprises (SMEs). It provides criteria and certification for small-to-medium business cyber security readiness</p>
<b>The Netherlands</b>	<p>The Dutch Baseline Security Product Assessment (BSPA) scheme is intended to judge the suitability of IT security products for use in the "sensitive but unclassified" domain. The BSPA scheme is in pilot phase since 2015. The pilot is expected to end in 2017 and then the scheme will be operational. In the pilot phase 6 requests for certification were received. The average cost of a certification under BSPA is € 40.000. The overall process can take up to 2 months.</p>
<b>Italy</b>	<p>A recent Italian decree (February 2017) promotes the establishment of a national centre for the evaluation and certification of ICT products used in critical infrastructures.</p>
<b>Norway</b>	<p>Norway has intention to develop a protection profile based on Common Criteria.</p>

## **Annex 12: Case studies**

## Case Study – “The impact of an EU wide Certification Scheme on the Smart-Meter Industry”

**A smart-meter company, which wants to sell its products in two Member States e.g. France and UK.**

	<b>Now</b>	<b>Future</b>
<b>Requirements</b>	<ul style="list-style-type: none"> <li>• <i>In order to sell in UK and France manufacturers have to certify against different schemes:</i> <ul style="list-style-type: none"> <li>○ <i>CPA (Commercial Product Assurance) in UK,</i></li> <li>○ <i>CSPN (Certification de Sécurité de Premier Niveau) in France</i></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Manufacturers will need to undergo a single certification process, as envisaged in the future European certification scheme for smart meters. The resulting certificate will be accepted by all public authorities in Member States.</li> </ul>
<b>Cost</b>	<ul style="list-style-type: none"> <li>• The overall cost is at least 300 thousand euros for the two markets (about 150 thousand euro in UK and about 150 thousand euros in France).</li> </ul>	<ul style="list-style-type: none"> <li>• The estimation of costs saving ranges up to <b>80% of current costs</b></li> </ul>
<b>Time</b>	<ul style="list-style-type: none"> <li>• <b>6 to 18 months.</b> This estimate takes into account: <ul style="list-style-type: none"> <li>○ Completion of multiple certifications processes and supporting documentation</li> <li>○ Identification of various requirements that a vendors needs to comply with.</li> <li>○ limited number of conformity assessment bodies able to certify against the requirements of different schemes.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Faster process</b> that takes into account: <ul style="list-style-type: none"> <li>○ Role of ENISA that provides information needed for compliance with the European scheme (e.g. specialised conformity assessment; documentation)</li> <li>○ Completion of single process : no multiple certifications are needed and capacities of existing CABs can be used more efficiently</li> </ul> </li> </ul>
<b>Other</b>	<ul style="list-style-type: none"> <li>• <b>Different methodologies</b> for risk assessment and definition of security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Standard methodologies</b> for risk assessment and definition of security requirements</li> </ul>

## Full Description:

**Methodology:** The research methodology of this case study is based on literature retrieved from desk research and on the analysis of multiple interviews with cybersecurity experts and professionals working in the Smart-Meter industry.

**Background:** By May 2014, Member States committed to rolling out close to 200 million smart meters for electricity and 45 million for gas by 2020 at a total potential investment of €45 billion. By 2020, it is expected that almost 72% of European consumers will have a smart meter for electricity while 40% will have one for gas. Up to date, 80 million smart meters have been installed in the EU28 and Norway, which constitutes 30% of the overall European electricity metering points<sup>139</sup>. With potentially millions of networked end-points, there are significant cyber threats organizations and consumers will be exposed to.

**Fragmentation of the Smart Meter Industry:** Various and not fully coordinated certification initiatives across Europe are increasing fragmentation in the domain of ICT certification and therefore also for Smart-Meter industry, resulting in duplication of efforts and waste of resources. The non-exhaustive list of certification schemes applicable to Smart Meters across Europe includes, among others:

- CPA (Commercial Product Assurance) is the certification scheme recognised in UK,
- CSPN (Certification de Sécurité de Premier Niveau) is the certification scheme recognised in France,
- A protection profile based on Common Criteria is the certification scheme recognised by BSI in Germany.

These three European Countries **do not recognise** each other's certification scheme.

The processes of certification are based on national requirements. In the UK, they are called security objectives. Based on these requirements and objectives, each MS has defined a security certification approach at a national level. There is also national communications infrastructure for devices connected to smart-meters, including interfaces with the different stakeholders involved such as the German Smart Meter "**Gateway**" and in the UK the so-called "**Communication Hub**". Other national initiatives are emerging as the **Dutch Smart Meter Requirements** (DSMR) developed by the Dutch national organization of DSO's "Netbeheer Nederland". If Member States across Europe continue not to accept each other's certification schemes, each Member State will continue to improve its own certification scheme and this could create a strong legacy, making harmonisation more difficult. Another problem regards a European agreement on minimum requirements, on documentations and tests results for the same functionality and in the same language, ready and accepted by the different authorities of different countries. Furthermore, such fragmentation is also happening on the evaluation side; the three different certification schemes mentioned above require three different evaluation methodologies and it's not always sure that they give the same results. There are only limited numbers of Conformity Assessment Bodies (CAB) that are able to certify against the requirements of different schemes and the evaluation period for smart meters products, as mentioned above, can usually last from **6 months to 18 months**. In this way, additional market entry barriers are created.

**Cost for Certification:** The proliferation of national certification schemes increases the costs for businesses operating cross-border and is likely to create obstacles for the internal market, as it raises the costs for companies/vendors operating across borders. This barrier is more significant for small and medium sized enterprises, which usually have less resources to dedicate to certification programmes.

To provide a concrete example, considering that the cost of certification depends on products, evaluation assurance level needed or components to be evaluated, the cost of certification can reach up to more than 1 million euros and the SMEs are out of this gain. For BSI "**Smart Meter Gateway**" certificate the cost is much more than **one million euros**. The cost for smart meters certification in

---

<sup>139</sup> USmartConsumer Project, European Smart Metering Landscape Report, "Utilities and consumers", 2016

UK is almost **150 thousand euro**. In France, the cost is similar to the UK, about **150 thousand euros or more**. In the Netherlands, the average costs of a certification under Baseline Security Product Assessment (BSPA) scheme are approximately **40 thousand euros**. The significant difference of costs for certification between Germany and other Member States have various reasons. France is for instance more focused on testing in a fixed time; i.e. given a fixed time the device has to pass all the security tests during that time. At the end of the fixed time, a final report is sent on whether it is working fine or not. The German approach has a higher level of tests and assurance. On the other hand in the UK and in France a security assessment is performed on one product, while in Germany the whole infrastructure needs to be tested and certified. Considering that these national certification schemes are not mutually recognised, smart metering companies should sustain additional costs in order to enter another Member State's market. In fact, the total cost for certification usually ranges **from 150 thousand euros to 1 million euros and more**. Only one of the biggest smart-metering companies is starting a certification to enter other markets and all the other companies are present only in the German market. In this context, one of the most important barriers to trade for the smart metering industry is the costs for certification. In the absence of an EU wide certification framework a smart metering company that wants to access the French market must certificate its products under the CSPN scheme and once again under the CPA scheme to enter the UK market, therefore it would pay **300 thousand euros**. With an EU wide framework, as the product certification of France deemed as equivalent to the one in the UK, the smart-meter company will have to certificate only once but will access the French and English market paying a cost of around 150 thousand euros and a **direct saving of 150 thousand euros**. More in general, it is estimated that the introduction of an EU wide certification framework could lead to smart meters companies **saving up to 80% on costs**.

**Benefits for the Smart Meter Industry of an EU wide Certification Framework:** For the smart-meters industry a European scheme would be a valuable policy option. It would make certification schemes mutually recognised across Europe, and standardise a methodology on how risks are assessed and how security requirements are defined. Moreover, it would be very important to have flexibility in certification scheme, determined also by the risk connected to the product evaluated and the risk connected to the location of the product. The introduction of an EU wide certification scheme will produce many benefits for the smart meters industry including:

- The reduction of fragmentation;
- The reduction of market barriers; and
- The reduction of the costs for certification.

**Conclusion:** There is no common baseline set of security requirements that can be recognized by all participating EU Member States. At least three Member States have defined their own protection profiles. These requirements are different per country, based on different standards and adopted by technical committees. There is no scheme that includes all aspects and enables a pan European approach<sup>140</sup>. In order to improve the current situation and to reduce the market fragmentation and the costs for certification, the introduction of an EU wide certification scheme could have a positive impact for the smart meter industry. A European framework would also reduce the information asymmetry on security requirements of ICT products and make the European market less fragmented.

---

<sup>140</sup> ENISA, Smart grid security certification in Europe, December 2014

## Case Study – “The impact of an EU wide Certification Scheme on Cloud Computing Industry”

	Now	Future
Requirements	<ul style="list-style-type: none"> <li>In order to sell Cloud Computing Products / Services in France and Germany providers have to certify against: <i>SecNumCloud and Compliance Controls Catalogue (C5)</i></li> </ul>	<ul style="list-style-type: none"> <li>Providers need to undergo a single certification process, as envisaged in the future European certification scheme for cloud computing. The resulting certificate will be accepted by all public authorities in Member States</li> </ul>
Cost	<ul style="list-style-type: none"> <li>Costs associated to compliance with different technical rules and multiple testing is estimated around 1.2 billion euro, that accounts for <b>2% to 10%</b> of companies' annual expenditures.</li> </ul>	<ul style="list-style-type: none"> <li>An increased level of competition, introducing an EU wide Certification Scheme, would result in a <b>yearly saving of € 1.1 billion in the EU public sector alone</b></li> </ul>
Time	<ul style="list-style-type: none"> <li><b>Around 7-9 months</b> due to the multiple audit and testing processes to obtain several certifications</li> </ul>	<ul style="list-style-type: none"> <li><b>Reduced time:</b> duration of a single process is estimated to take around 4 to 6 months. ENISA would accelerate the process by providing the information needed for compliance with the European scheme</li> </ul>
Other	<ul style="list-style-type: none"> <li>Faced with co-existence of multiple schemes and standards<sup>141</sup>, end-users (esp. in the banking sector) are not able to compare and judge which scheme or standard would best satisfy their particular security requirements. This deteriorates the trust in cloud computing services.</li> </ul>	<ul style="list-style-type: none"> <li>The existence of a security certification scheme for cloud computing agreed at EU level, increases the trust in this service</li> <li>Competitive gain for cloud providers due to cost and time reduction</li> </ul>

<sup>141</sup> ECSO has published a State-of-the-Art Syllabus listing 8 different schemes and standards to certify the security of cloud computing services. See here: [www.upm.es/observatorio/vi/gestor\\_general/recuperar\\_archivo.jsp?idf=642&tipo=2](http://www.upm.es/observatorio/vi/gestor_general/recuperar_archivo.jsp?idf=642&tipo=2)

## Full Description:

**Methodology:** This case study is based on information obtained from secondary sources (literature review), from the analysis of the European landscape of cloud computing industry conducted on the basis of an online search and from interviews conducted with different impacted stakeholders.

**Background:** The ongoing digital transformation is strategically affecting both private and public sector organisations also in terms of cybersecurity<sup>142</sup>. Cloud computing has the potential to reduce IT expenditure and boost organisational flexibility while at the same time improving the scope for delivering flexible high-quality new services. Some of the general benefits are reducing costs, increasing the storage capabilities and the chance to adapt in a flexible way to the changing business conditions<sup>143</sup>. These benefits can be applied in a lot of different domains and fields.

The increase in the use of cloud globally is also visible from the market, over the last two years<sup>144</sup>. In 2017, spending on public cloud infrastructure as a service hardware and software is forecast to reach **61 billion U.S. dollars worldwide**<sup>145</sup>. According to Gartner, Inc., the highest growth will come from cloud system infrastructure services (IaaS), which is projected to grow **36.8 percent in 2017 to reach \$34.6 billion**. Cloud application services (SaaS) is expected to grow 20.1 percent to reach \$46.3 billion<sup>146</sup>.

Despite its growing influence, concerns regarding cloud computing still remain. There are in fact challenges that it still has to face, such as: **data protection, data recovery and availability, management capabilities and regulatory and compliance restrictions**<sup>147</sup>.

Incidents related to cloud computing services worry the companies especially for sectors such as finance where a data breach can cause huge economic and reputable damages. According to representatives from European banks, they are not very sure if the data are stored in a secure way, especially according to the various jurisdictions of different countries.

Cloud computing is going to be fundamental for the future. For this reason, it is necessary that it as secure as possible.

**Fragmentation of the Cloud Computing Industry:** Cloud service providers offer their services internationally in several markets. Therefore, national approaches for certification and assurance are of limited use to them. National cyber security authorities can usually only set national standards, even if other countries use them too<sup>148</sup>. ANSSI (Agence nationale de la sécurité des systèmes d'information) and the BSI have been very intensively involved with the security of cloud computing in recent years. Both authorities arrived at a very similar understanding of the cloud security standards that need to be met, and both initiated new ways of verifying secure cloud computing, since the existing certifications failed to adequately meet the needs in this area. However, both authorities pursued different paths<sup>149</sup>.

- **Compliance Controls Catalogue (C5)** - The BSI developed the Cloud Computing Compliance Controls Catalogue (C5). This catalogue, which is closely oriented to tried and tested standards, defines the requirements for the secure provision of services critical to businesses, which the cloud provider must meet. Additionally, the provider must make their offer transparent, such as the location of data processing and the subcontractor. The auditing process is conducted in line with the international recognised standard, the ISAE 3000. The audit report is based on standards such as the ISAE 3402 and SOC 2. Auditors and cloud experts conduct this audit and issue an audit opinion, for which the auditor bears liability. The C5 also contains standards for greater protection needs and can be individually extended – for example for a specific industrial sector. The BSI sets the standards and specifies criteria for the audit, but has no further supervisory role with regard to specific procedures.

---

<sup>142</sup> <https://www.enisa.europa.eu/publications/exploring-cloud-incidents>

<sup>143</sup> [http://picse.eu/sites/default/files/ProcuringCloudServicesToday\\_March2016\\_web.pdf](http://picse.eu/sites/default/files/ProcuringCloudServicesToday_March2016_web.pdf)

<sup>144</sup> <https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#51dfa21b2187>

<sup>145</sup> <https://www.statista.com/statistics/507952/worldwide-public-cloud-infrastructure-hardware-and-software-spending-by-segment/>

<sup>146</sup> <http://www.gartner.com/newsroom/id/3616417>

<sup>147</sup> <http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf>

<sup>148</sup> [https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel\\_node.html](https://www.bsi.bund.de/EN/Topics/CloudComputing/ESCloudLabel/ESCloudLabel_node.html)

<sup>149</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin\\_2016-02.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4)



- **SecNumCloud** - The ANSSI takes a very different approach. The Référentiel SecNumCloud, which is strongly oriented to the ISO/IEC 27001 standard and which supplements it with several specifications of its own, defines the standards required for secure cloud computing. In the Référentiel, there are two levels: *sécuré* and *sécuré plus*, whereby the latter sets higher security standards and limits to France the service provided. Taking this as a basis, the ANSSI has developed a completely new certification of its own, which it has established in France. Cloud providers receive a certificate which is issued by the ANSSI and on which an audit report produced by ANSSI certified auditors is based. For example, providers who want to be certified with SecNumCloud can be audited by AFNOR Certification<sup>150</sup>.

While the security levels which the BSI and ANSSI would like to see in place are very similar, **the two very different approaches towards certification and attestation appear to contradict each other**. Moreover, the list of applicable standards and certification schemes for cloud computing across Europe includes, among others: ISO 27001/2, ISO 20000 (ITIL), CSA Open Certification Framework (OCF), Eurocloud, Star Audit, SOC 1-2-3, PCI – DSS, Europrise, FISMA, Cloud Industry Forum Code of Practice, ISACA COBIT, Security Rating (Leet security), TUV certified.

Motivated by the German-French business consultations<sup>151</sup> and based on a high level of mutual trust, the idea therefore emerged of generating a **new Cloud Label**. It stands for the joint cloud security standards and is suitable evidence that they have been met. The underlying principle on which the label is based is a joint short catalogue with security targets (“core rules”). Naturally, the attestation in accordance with the BSI’s C5 and the ANSSI certification are sufficient to meet these standards. **A provider who already has one of the two certifications can receive this label and as such advertise the security level of their product very easily on both markets**. The Cloud Label is regarded by the ANSSI and BSI as being an explicitly European initiative, which can also incorporate the certifications of other countries. In this way, the expertise and independent nature of the BSI and ANSSI, as well as their cooperation based on trust, are of benefit to the whole of Europe.

Another European initiative towards a unique approach for ICT security certification schemes comes from **Horizon 2020 Programme**: the project EU-SEC<sup>152</sup>. The EU-SEC, started at the beginning of 2017, will last until 2019 and aims to create a framework under which existing, certification and assurance approaches can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the cloud.

**Cost Analysis:** An economic paper by economists of DG ECFIN estimated that the cost associated to differences in technical rules and multiple testing/certification are between **2% to 10% of companies annual turn-over**<sup>153</sup>. According to this paper inadequate standards and insufficient mutual recognition, including in the ICT sector, is among the main barriers to the single market. For example, the costs of an ISAE 3000 implementation project, in order to be certified under the Cloud Computing Compliance Controls Catalogue (C5) Scheme, can vary from **ten thousand USD up to a million USD or even more**<sup>154</sup>. The costs for enterprises of product conformity assessment can be substantial and there is lack of mutual recognition which implies the multiplication of such costs: for companies offering several product types on a national market of a receiving Member State the costs amount to approximately 2% of their entire annual turnover on that market, whereas they can reach up to 10% for companies specialized in one specific product type because they do not benefit from economies of scale<sup>155</sup>. Even applying the lower bound of 2% only to 60% of the cyber security market to be conservative (i.e. assuming 40% of the market concerns products for which certification is not required) **the costs of lack of mutual recognition reach a figure in the range of 1.2 billion euro**.

<sup>150</sup> <http://www.afnor.org/en/news/cybersecurity-vigilance-required/>

<sup>151</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin\\_2016-02.pdf?\\_\\_blob=publicationFile&v=4](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2016-02.pdf?__blob=publicationFile&v=4)

<sup>152</sup> [http://cordis.europa.eu/project/rcn/207439\\_en.html](http://cordis.europa.eu/project/rcn/207439_en.html)

<sup>153</sup> Ilzkovitz, F. Dierx, A. Kovacs, V. & Sousa (2007) Steps towards a deeper economic integration: the internal market in the 21st century”, European Economy, Economic Papers, No. 271. European Commission.

<sup>154</sup> <https://www.isae3000.com/controlreports>

<sup>155</sup> Ibid. p. 61

Moreover, many organizations are 'locked' into their ICT systems because detailed knowledge about how the system works is available only to the provider, so that when they need to buy new components or licenses only that provider can deliver. **This lack of competition leads to higher prices and some € 1.1 billion per year is lost unnecessarily in the public sector alone<sup>156</sup>.**

As mentioned in the SWD "A Single Market Strategy for Europe - Analysis and Evidence"<sup>157</sup> a large body of economic studies that show the impact that standard have on economic growth and GDP<sup>158</sup>. **For France the impact on growth is estimated at 0.8 %, for United Kingdom at 0.3 % and for Germany at 0.9 % of GDP.** To put this in monetary terms, DIN (the German Institute for Standardization) estimates that in Germany alone, standards generate up to EUR 17 billion a year. A more recent study from the UK 'The Economic Contribution of Standards to the UK Economy' also confirms that the use of standards benefits the national economy: standards contributed to around EUR 11 billion of the EUR 40 billion GDP growth in 2013 (2014 prices) and to around EUR 8.5 billion to UK exports<sup>159</sup>. The same study shows that standards help to enhance quality, with 70 % of respondents stating that standards had contributed improving the quality of supplier products and services. In the econometric models supporting such estimates standards are considered, together with R&D expenditure and patents, as fuelling the knowledge input in the classical production functions. One key hypothesis is that standards can, to some extent, counterbalance some well-known market failures and the possibility that investments in knowledge by private players are sub-optimal and not sufficient to produce social surplus (externalities).

**Benefits for the Cloud Computing Industry of an EU wide Certification Framework:** In a world that is increasingly interconnected, it does not make much sense for a State to tackle digital security issues on its own. The new French digital security strategy states France's will to engage a dialogue both within multilateral organizations and with long-term trustworthy partners following two objectives: contributing to the global stability of cyberspace as well as reinforcing the States' own cybersecurity.

The longstanding and close bilateral cooperation between ANSSI and BSI is based on trust and has been greatly facilitated by a shared vision on many strategic and political issues, a common positioning at the national level fulfilling only defensive missions and a comparable high level of technical expertise.

ANSSI and BSI have been working together in many fields, such as cloud-computing with the creation of a common label for secure cloud service providers, security certification through a very strong support of the international recognition schemes (CCRA and SOG-IS) and industrial synergies. An EU wide certification framework could guide these initiatives in order to avoid the fragmentation of standards and certification schemes across Europe and the further development of national approaches. The benefits of standardization through an EU wide certification scheme include, among others:

---

<sup>156</sup> <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0455&from=EN>

<sup>157</sup> Brussels, 8.10.2015 SWD (2015) 202 final, accompanying the document Upgrading the Single Market: more opportunities for people and business (COM (2015) 550 final) {SWD(2015) 203 final}.

<sup>158</sup> Among peer-reviewed journal articles see: Acemoglu, D., G. Gancia and F. Zilibotti (2012), 'Competing Engines of Growth: Innovation and Standardization,' *Journal of Economic Theory*, 147, 570–601; Blind, K. and A. Jungmittag (2008), 'The Impact of Patents and Standards on Macroeconomic Growth: A Panel Approach Covering Four Countries and 12 Sectors,' *Journal of Productivity Analysis*, 29, 51–60; Jungmittag, A., K. Blind and H. Grupp (1999), 'Innovation, Standardisation and the Long-term Production Function,' *Zeitschrift für Wirtschafts- und Sozialwissenschaften*, 119, 205–222; Wakke, P., Blind, K.; Ramel, F. (2016): The impact of participation within formal standardization on firm performance, *Journal of Productivity Analysis* 45 (Issue 3), 317–330; Wijen, F.H. (2014). Means versus ends in opaque institutional fields: Trading off compliance and achievement in sustainability standard adoption. *Academy of Management Review*, 39 (3), 302–323. Swann, P. (2010), *International Standards and Trade: A Review of the Empirical Literature*. Report for the UK Department of Business, Innovation and Skills (BIS). OECD Trade Policy Working Papers. Among reports commissioned by standardization bodies see: SCC (2007). *Economic Value of standardisation*; AFNOR (2009). *The Economic Impact of standardisation*; DIN (2011). *The Economic Benefits of standardisation*; Standards Australia (2012). *The Economic Benefits of standardisation*; Cebr (2015). *The Economic Contribution of standards to the UK Economy*; Cebr (2016). *Economic Contribution of Standards in Ireland – A report for the National Standards Authority of Ireland*.

<sup>159</sup> British Standards Institution (BSI), 'The Economic Contribution of Standards to the UK Economy', 2015

- **Competitive Advantage.** Companies are motivated to participate in standardization because they gain an edge over non-participating companies in terms of insider knowledge. Early access to information is valuable;
- **Cost Reduction.** Standardization lead to lower transaction costs in the economy as a whole, as well as to savings for individual businesses. transaction costs drop considerably as a result of standards, since they make information available and they are accessible to all interested parties;
- **Supplier/Client Relationship.** Standards can help businesses avoid dependence on a single supplier because the availability of standards opens up the market. The result is a broader choice for businesses and increased competition among suppliers;
- **Standards and R&D.** Businesses not only reduce the economic risk of their R&D activities by participating in standardization, but can also lower their R&D costs. When a company can influence the content of standards to its advantage, the economic risk is lower. The expense of R&D is potentially reduced when the participants in standards work make their results generally available, and research need not be duplicated
- **Raising Trust.** An annual report featured on eWeek<sup>160</sup> shows that 73% of survey respondents are worried about cloud computing security. An EU wide Certification Scheme could raise the trust level of companies in the Cloud Computing services, reducing insecurity due to the various jurisdictions of different Countries.

**Conclusion:** Even if States are primarily responsible for their national digital security, it is France and Germany's shared vision that many challenges can best be addressed **through a common and coordinated effort at European level.** This could be guaranteed introducing an EU wide certification framework, which avoids multiplication of national approaches, duplication of efforts and waste of resources. Beyond the development of EU Member States' capacities and cooperation, the EU must as well recognize that European digital security is challenged on other fronts, requiring a collective ambition to guarantee Europe's digital sovereignty. Three challenges in particular are ahead of us<sup>161</sup>:

- The EU and the Member States' ability to protect and defend the EU institutions, the administrations, the critical infrastructures, the companies and the general public in cyberspace must be ensured;
- The EU must actively support the development of sustainable European industries in the field of digital security and guarantee Member States' ability to evaluate and approve the security of digital products and services;
- The EU must preserve its capacity to choose autonomously how data and related services should be protected in Europe.

Along with like-minded Member States, France and Germany will closely work together to promote the European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of European values.

<sup>160</sup> <http://www.eweek.com/cloud/companies-worry-about-security-implications-of-cloud-services>

<sup>161</sup> Federal Office of Information Security, BSI, Security in focus, Europe and International Cooperation, BSI Magazine 2016/02