Council of the European Union

Brussels, 22 January 2026
(OR. en)

**Interinstitutional Files:**
**2026/0011 (COD)**
**2026/0012 (COD)**

**5611/26**
**ADD 4**

**CYBER 29**
**JAI 85**
**DATAPROTECT 22**
**TELECOM 29**
**MI 58**
**IND 48**
**CADREFIN 26**
**FIN 100**
**BUDGET 3**
**CODEC 90**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director |
| date of receipt: | 21 January 2026 |
| To: | Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union |
| No. Cion doc.: | SWD(2026) 11 final |
| Subject: | COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the documents Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) And Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2] |

Delegations will find attached document SWD(2026) 11 final.

Encl.: SWD(2026) 11 final

EUROPEAN
COMMISSION

Strasbourg, 20.1.2026
SWD(2026) 11 final

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT REPORT**

***Accompanying the documents***

**Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)**

**And**

**Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]**

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 12 final}

## Table of contents

## LIST OF TABLES AND ANNEXES

### LIST OF TABLES



### LIST OF ANNEXES

**LIST OF TABLES (ANNEXES)**

**LIST OF FIGURES (ANNEXES)**

## GLOSSARY

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

| *Term or acronym* | *Meaning or definition* |
|---|---|
| 2024 Evaluation report | Report from the Commission to the European Parliament and the Council on the Evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework |
| 5G Cybersecurity Toolbox | European Commission, Commission Recommendation (EU) 2019/534 of 26 March 2019, Cybersecurity of 5G networks. |
| AHWG | Ad hoc working group |
| CER Directive | Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC |
| CERT-EU | The Cybersecurity Service for Union institutions, bodies, offices and agencies |
| 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. |
| CRA | Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). |
| CSA | Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013. |
| CSIRTs network | The CSIRTs network was established under the NIS Directive and its legal basis continued under the NIS 2 Directive. The mandate of the CSIRTs network is to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States. |
| CSoA | Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 |

| *Term or acronym* | *Meaning or definition* |
|---|---|
| CVD | Coordinated vulnerability disclosure |
| Cyber Blueprint | Council Recommendation on an EU blueprint for cyber crisis management - Council Recommendation approved by the Council at its meeting on 6 June 2025. The Cyber Blueprint describes clearly and simply who does what in an EU cyber crisis. |
| Data Act | Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) |
| Data Governance Act | Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). |
| DEP | Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. |
| DORA | Regulation EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 |
| ECCC | European Cybersecurity Competence Centre |
| ECCF | European Cybersecurity Certification Framework |
| ECCG | European Cybersecurity Certification Group |
| ECSF | European Cybersecurity Skills Framework |
| EDBP | European Data Protection Board |
| eIDAS 2 | Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework |
| ENISA or the Agency | European Union Agency for Cybersecurity |
| EU | European Union |
| EU5G | EU 5G Cybersecurity Certification |

| *Term or acronym* | *Meaning or definition* |
|---|---|
| EUCC | Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) |
| EUCS | EU Cloud Certification Scheme |
| 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) |
| EU-CyCLONe | The European cyber crisis liaison organisation network (EU-CyCLONe) was established by the NIS 2 Directive to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies. |
| FTE | Full time equivalent |
| GDPR | 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) |
| Horizon Europe | Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013. |
| ICT | Information and communication technology |
| IICB | Interinstitutional Cybersecurity Board |
| 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 | 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 |

| *Term or acronym* | *Meaning or definition* |
|---|---|
| | assessment is carried out. 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. |
| International Digital Strategy | International Digital Strategy for the European Union, JOIN(2025) 140 final |
| MFF | Multiannual financial framework of the EU |
| MSSP | Managed security service provider |
| NCCAs | National Cybersecurity Certification Authorities |
| NCCS | Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows |
| NIS | Network and Information Systems |
| NIS 2 Directive | Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 |
| OECD | Organisation for Economic Co-operation and Development |
| PART-IS | Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645 on requirements for the management of information security risks with a potential impact on aviation safety for organisations and competent authorities |
| PC | Public consultation |
| Preparedness Union Strategy | Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy, JOIN(2025) 130 final |
| ProtectEU Strategy | Communication from the Commission to the European Parliament, the Council, the European Economic and Social |

| *Term or acronym* | *Meaning or definition* |
|---|---|
| | Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM(2025) 148 final |
| REFIT | The European Commission's regulatory fitness and performance programme (REFIT) aims to ensure that EU laws deliver on their objectives at a minimum cost for the benefit of citizens and businesses. |
| SCCG | Stakeholder Cybersecurity Certification Group |
| SMEs | Small and medium-sized enterprises |
| TFEU | Treaty on the Functioning of the European Union |
| TS | Technical specifications |
| URWP | Union Rolling Work Programme for Cybersecurity Certification |

## 1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

In today's interconnected world, technology is the backbone of Europe's economy, society, and sovereignty. From energy grids and hospitals to financial systems and transport networks, digital infrastructure powers every critical sector. With this transformation comes a reality which by now is widely acknowledged: cybersecurity is no longer optional. It is a political, economic, and strategic imperative. The EU's Preparedness Union[1] and ProtectEU[2] strategies have placed cybersecurity at the heart of Europe's resilience agenda. These strategies recognise that persistent cybersecurity threats are not just technical challenges, but strategic risks to our democracy, economy, and way of life. The **revision of the Cybersecurity Act (CSA)** is an important contribution to reinforce EU preparedness and make the EU cybersecurity framework more effective and efficient.

The 2019 **CSA** empowered the EU Agency for cybersecurity (ENISA) and established the European Cybersecurity Certification Framework (ECCF) to ensure trust and consistency across the internal market. At the time, the EU cybersecurity regulatory and policy framework was rather limited. However, **since 2019,** the cybersecurity threat landscape has significantly evolved[3] in an increasingly complex geopolitical reality and subsequently triggered a more comprehensive European regulatory and policy approach.

Cyberattacks have surged and became more sophisticated, targeting critical infrastructure, businesses, and citizens. Emerging technologies like AI and quantum computing are reshaping the tools of defence and the tactics of adversaries. The overall cost of cybercrime in the global economy was estimated at amounting to EUR 5.5 trillion in 2020[4]. Projections show that by 2031, ransomware will strike every 2 seconds down from 11 seconds today[5]. **Supply chain incidents**, either caused by criminals for financial gain or State actors for disruption, espionage, disinformation or warfare have intensified. Nowadays, the impacts of a cyber incidents do not just stop at stolen data or financial losses. As part of a wider hybrid strategy, they ripple outward, disrupting essential services, undermining trust in institutions, and affecting our defence readiness. The avalanche effects of cybersecurity incidents onto the real world can have impacts from disruption of services and economic activity, financial instability to existential consequences, with a risk on citizens' lives. Incidents, such as the 2020 SolarWinds attack, which impacted more than 18,000 organisations worldwide including EU defence actors, or the recent attack on Collins aerospace which disrupted air traffic in several EU airports, show the magnitude of impacts from single incidents [6] *(see Annex 7, Parts 2, 3 and 4).*

---

[1] JOIN/2025/130 final.
[2] COM/2025/148 final.
[3] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
[4] JOIN(2020) 18 final.
[5] Who's who in Ransomware Report, q2 2023 Whos Who in Ransomware Report | PDF | Ransomware | Security
[6] BBC, *EU cyber agency says airport software held to ransom by criminals*, https://www.bbc.com/news/articles/cqjeej85452o.

The **EU has expanded its legal and policy tools** with the adoption of the NIS2 Directive to strengthen cybersecurity for critical infrastructure, complemented for physical security by its 'sister directive' CER, the Cyber Resilience Act (CRA) to enhance the cybersecurity of products, the Cyber Solidarity Act (CSoA) to build EU-wide response capabilities, the EU Cyber Blueprint[7] to support EU-level crisis management cooperation, the 5G Cybersecurity Toolbox[8] (5G Toolbox) and the Cybersecurity Skills Academy[9] to address the growing challenge of the cybersecurity talent gap. This cybersecurity framework was complemented by sector-specific legislation, i.e. the DORA Regulation for the financial sector, NCCS for the electricity sub-sector, PART-IS for the air transport sector, and policy such as the EU action plan on the cybersecurity of hospitals and healthcare providers[10] *(see Annex 9).*

With such an extensive regulatory and policy framework in place, the **CSA revision** comes to provide the necessary tools to **make such framework more effective and efficient** in delivering the expected results, provide for a **stronger European dimension** and leverage and **fill in the remaining regulatory gaps**. Given the coverage of horizontal and sector-specific legislation, and the fact that numerous businesses provide multiple services across the internal market, it is necessary to explore further ways to **facilitate compliance** with cybersecurity risk-management requirements arising from different regulatory instruments. **Simplification** measures should unlock resources to strengthen the operational cybersecurity preparedness of entities in Europe's critical sectors. These needs were also confirmed by the responses to the public consultation *(see Annex 2).*

This impact assessment therefore analyses the needs for an updated and stronger legislative framework, which would entail: (1) the *revision of the mandate of ENISA* to adapt it to the evolving cybersecurity threat landscape and the main stakeholders' needs; (2) *the revision of the ECCF*, to expand and clarify its scope and improve its governance and procedures and (3) *targeted amendments to the NIS2 Directive* to facilitate and align compliance across the internal market and (4) *filling in regulatory gaps by setting up a framework at EU level to enhance ICT supply chain* security against the non-technical risks.

For what concerns ENISA, the **European Parliament** underlined that with increasing cyber threats, ENISA's budget should be accordingly increased[11] and the motion for a resolution on European technological sovereignty and digital infrastructure[12] highlights the need to close the digital skills gap. The **Council** has stressed the need for focused and clearly defined mandate, "with concrete strategic objectives" and invited the Commission

---

[7] COM/2025/66 final.
[8] Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures, NIS Cooperation Group, 1/2020, available at: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
[9] COM(2023) 207 final.
[10] COM(2025) 10 final.
[11] European Parliament resolution of 11 April 2024 on discharge in respect of the implementation of the budget of the European Union agencies for the financial year 2022: performance, financial management and control (2023/2182(DEC), point 61
[12] 2025/2007(INI), points 104-109. At the time of writing, the REPORT on European technological sovereignty and digital infrastructure | A10-0107/2025 | European Parliament has been voted by the Industry (ITRE) committee of the European Parliament, awaiting vote in Plenary session.

to examine and strengthen ENISA's role in supporting operational cooperation. The Council acknowledged ENISA's role in the ECCF, underpinning trust in ICT products, services and processes"[13].

In the **ProtectEU Strategy**, the Commission further stated that a harmonised approach to the security of the **Information and Communication Technology (ICT) supply chain** can address the current fragmentation of the internal market caused by different approaches at national level, avoid critical dependencies and de-risk ICT supply chains from high-risk suppliers, in this way securing critical infrastructure. The **Economic Security Strategy** also highlighted the need to make the EU's economy and supply chain more resilient in order to promote its own competitiveness.[14] The need to address disruptions of supply chains and cyberattacks was also highlighted in the Preparedness Union Strategy and the White Paper for European Defence[15]. The co-legislators further share the sense of urgency to take enhanced actions to ensure the security of ICT supply chains. The **European Parliament** called on the Commission to develop binding ICT supply chain security legislation that addresses non-technical risk and to "exclude the use of equipment and software from manufacturers based in high-risk countries, particularly China and Russia"[16]. Members of the European Parliament also called for urgent action to secure telecommunications infrastructure against undue foreign influence and security risks[17]. Digital supply chain risks are further raised in the resolution on European technological sovereignty and digital infrastructure[18]. The **Council** in its conclusions on the Future of Cybersecurity[19], reiterated its commitment towards ensuring the security of the ICT supply chains and noting the relevance of non-technical risk factors[20].

In his 2024 **report on 'The Future of European Competitiveness'**, Mario Draghi highlighted the need to increase security and reduce dependencies as one main areas of action needed in Europe[21]. EU companies should maintain a foothold in areas where technological sovereignty is required, such as security, referring to e.g. supply chain security needs. In particular, the report stresses the need to enforce compliance with the EU Toolbox for 5G security within a set timeframe to ensure that sensitive elements are from trusted suppliers, and preferably from EU providers. The report further underscores the need to fill in the skills gap in Europe.

---

[13] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.
[14] JOIN/2023/20 final.
[15] JOIN/2025/120 final.
[16] European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI), points 62 and 63.
[17] Euronews, *Lawmakers call for binding 5G security measures in wake of Huawei scandal*, https://www.euronews.com/next/2025/03/19/lawmakers-call-for-binding-5g-security-measures-in-wake-of-huawei-scandal.
[18] 2025/2007(INI)
[19] Council of the European Union, Council conclusions on the future of cybersecurity, 21 May 2024, no. 10133/24.
[20] Council of the European Union, Council conclusions on ICT supply chain security, 17 October 2022, no. 13664/22.
[21] European Commission, The future of European Competitiveness, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

Finally, the CSA revision would come to complement the Critical Entities Resilience (CER Directive) Directive which provides supply chain aspects as part of resilience measures of critical entities. Moreover, it would complement upcoming initiatives under preparation, such as the Cloud and AI Development Act (CAIDA) which aims, among others, to tackle the lack of a competitive EU-based offer of cloud computing services at sufficient scale to serve highly critical use cases or sectors; the upcoming Digital Networks Act (DNA); and the public procurement framework[22] which is currently under evaluation.[23]

## 2. PROBLEM DEFINITION

### 2.1. What is/are the problems?

There are four main problems identified in relation to the current CSA, as well as more widely in relation to the effectiveness of the current EU cybersecurity regulatory framework. The problems identified were broadly confirmed by the public consultation, the main stakeholders concerned by the respective frameworks, as well as by calls of European Parliament and Council.

#### 2.1.1. *Problem 1: Misalignment between the Union's cybersecurity policy framework and stakeholders' needs in an increasingly hostile threat landscape*

The CSA gives since 2019 a permanent mandate to ENISA. However, the fast-evolving cybersecurity landscape and its consequences on real-world economy *(see Annex 7)* and growing geopolitical instability[24] led over the past 5 years to a gradual extension of ENISA's tasks through various legislative instruments *(see Annex 9).* Furthermore, other new needs emerged, such as an increasing demand for more effective standardisation and certification processes to facilitate cybersecurity measures and level the playing field or an increasing need to address the cybersecurity skills gap and take more effective actions in this regard. With the recent legislative instruments, only some of the emerging needs where ENISA can play an important role, were tackled, but these were rather addressed disparately, and **could not achieve a reboot of the overall focus of ENISA on most pressing needs where such a European agency can play a decisive role**.

Overall, whilst Member States and industry, value ENISA and its advisory role in policy implementation, they also indicate that the agency is not able to implement its mandate efficiently and effectively[25].

*First*, ENISA does not meet stakeholders' needs in **supporting efficiently cooperation among Member States and bringing a consolidated European perspective to Member States and industry on situational awareness at the EU level**[26] **or in**

---

[22] In particular Directives 2014/23/EU, 2014/24/EU and 2014/25/EU.
[23] European Commission, Commission launches call for evidence and public consultation on the evaluation of the Public Procurement Directives, https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_en.
[24] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[25] 2024 Evaluation report.
[26] ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf.

**reaching its full potential to support implementation of cybersecurity measures and raise the bar for cybersecurity standards**. The NIS2 Directive and the CRA brought ENISA more responsibilities for holding an overview of vulnerabilities exploited across the internal market. With the expanded regulatory framework, ENISA is expected to support more effectively Member States in their overseeing of compliance with cybersecurity requirements. The recently adopted Cyber Blueprint intends to improve coordination in cyber crisis management and to provide for clear roles and responsibilities. The CSoA further introduces measures such as the EU Cybersecurity Reserve[27], explicitly recognising the need for additional support to address significant or large-scale cybersecurity incidents[28]. ENISA's role as a secretariat to the CSIRTs network and EU-CyCLONe is limited to providing coordination, requiring reflection on additional tasks and responsibilities for contributing to developing a cooperative response to large scale cross-border cyber incidents and[29]. In 2024, the Agency further did not meet its targets to *"provide regular risk monitoring (...) and provide specific risk assessments and threat landscapes as requested by Member States"* (target set on 50%, result for 2024 was 30%)[30]. The capabilities for developing standards and technical specifications to support implementation of CRA or ECCF are insufficient and the existing processes lack agility and adaptability to the pace and extent of market needs.

*Second*, the de-prioritisation of the Agency towards cybersecurity skills-related activities[31] marks a discrepancy **with stakeholders' expectation to see ENISA leading skills-related activities,** such as the development of an attestation scheme for cybersecurity skills supported by 69.43% of respondents to the public consultation *(see Annex 2)*. This disengagement is further in contradiction with the ever-growing **gap in the cybersecurity workforce, which continued to increase** from an estimated 274,000 missing professionals in 2023 to 299,000 in 2024[32] (+9%), leaving public administrations and companies, in particular **SMEs vulnerable** due to lack of in-house cybersecurity expertise[33].

The cybersecurity training offer is well developed by market actors such as higher education institutions, vocational education and training providers and companies[34], and

---

27 Specifically, the CSoA requires the Commission to entrust ENISA with the operation and administration of the EU Cybersecurity Reserve (in full or in part), Art. 14(5) CSoA.

28 ENISA, *2024 Report on the State of Cybersecurity in the Union*, https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

29 ST 16527/24, point 16

30 ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf.

31 ENISA, *ENISA Single Programming Document 2025-2027*, https://enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA%20Single%20Programming%20Document%202025-2027.pdf.

32 ISC2, *First Look at the 2024 Cybersecurity Workforce Survey*, https://digital-skills-jobs.europa.eu/system/files/2024-12/ISC2_Workfoce-Study-Findings-EU.pdf.

33 Eurochambres, *Twin transition survey*, https://www.eurochambres.eu/wp-content/uploads/2022/09/Eurochambres-Twin-Transition-Survey.pdf; ENISA, Cybersecurity Policy Assessment.

34 ENISA, *ENISA's Cybersecurity Higher Education Database (CyberHEAD)*, https://www.enisa.europa.eu/tools/cyberhead-cybersecurity-higher-education-database. And See for illustration the non-exhaustive list of cybersecurity trainings offered across the EU on the Digital Skills and Jobs Platform, https://digital-skills-jobs.europa.eu/en/opportunities/training?f%5B0%5D=digital_technology%3Ahttp%3A//data.europa.eu/uxp/c_04ae3ba8.

regulators and other non-market actors are adopting strategies and recommendations to address the skills and talent shortages[35]. However, the absorption of cybersecurity-specific roles into existing non-cybersecurity related roles[36] shows the need for lifelong learning and established ways to prove competences to ensure career evolution[37]. In this regard, the **cybersecurity labour market increasingly relies on individual cybersecurity certifications**: non-formal cybersecurity education through certification allows for recognition of skills associated to cybersecurity professionals[38], which is outpacing formal education in cybersecurity[39].

However, European individual certifications market suffers from **market failures**. In particular, reputation-based individual certifications are leading to **market control**, where job advertisements for cybersecurity positions display an **oligopoly** of private actors. This market also suffers from **negative externalities**: whereas the labour market can, to the extent that they ease hiring processes and career evolutions, benefit from market-recognised individual certifications, they impede the growth for other, less known certifications, harming the emergence of new providers.

To address this, ENISA has been entrusted in the communication on the Cybersecurity Skills Academy with the development of a pilot project exploring the set-up of a European attestation scheme for cybersecurity skills. Despite having launched the pilots in 2024 and Member States support, materialised by ENISA's Management Board's call to further enhance the concept of attestation of skills[40], the Council call to build on the Cybersecurity Skills Academy[41], and eight Member States are taking part in the ENISA-run pilots[42], the project is moving forward at slow pace.

*Third*, ENISA operates alongside a range of **complementary cybersecurity EU-level actors,** including CERT-EU, Europol (for cybercrime) and the European Cybersecurity Competence Centre (ECCC). While their mandates are clearly delineated, synergies to avoid fragmentation and enhance collective resilience, especially in operational response, strategic coordination and innovation programming, have not sufficiently materialised. This problem has the potential of impacting the EU's security at a time where EU agencies and bodies in justice, home affairs, and cybersecurity play a key role, in line

---

[35] Council Recommendation of 16 June 2022 on a European approach to micro-credentials for lifelong learning and employability 2022/C 243/02, ST/9790/2022/INIT. And STEM education strategic plan, https://education.ec.europa.eu/focus-topics/stem.

[36] Eurobarometer (2024) on Cyberskills, https://europa.eu/eurobarometer/surveys/detail/3176.

[37] ANSSI, *Observatoire des métiers 2025*, https://cyber.gouv.fr/publications/observatoire-des-metiers-2025.

[38] In this way, and whereas certifications rely on a similar rationale of having skills quickly and easily recognised by employers, training providers and other actors, they strongly differ from the concept of a European Digital Skills Certificate (Action 9 of the Digital Education Action Plan (2021-2027), COM/2020/624 final) which aimed at supporting digital skills recognition across Europe. The target audience also differs insofar as certifications target cybersecurity professionals, actual or potential, whereas the EDSC ambitions was to address the population at large (jobseekers and the labour force, but also students, citizens and teachers). CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., HÜSING, T., CUARTAS-ACOSTA, A. and TROIA, S., European Digital Skills Certificate (EDSC) Feasibility Study, Publications Office of the European Union, Luxembourg, 2024, doi:10.2760/958195, JRC138344, JRC Publications Repository - European Digital Skills Certificate (EDSC) Feasibility Study.

[39] Ibid. See for example in France where 37% of the cybersecurity workforce holds a certification in cybersecurity whereas 33% holds a cybersecurity diploma.

[40] Ibid.

[41] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.

[42] CY, DE, IT, NL, ES, SE, PT and SK.

with the ProtectEU Strategy[43]. Additionally, **structured cooperation between ENISA and the ECCC** is not delineated in a way as to ensure synergies between their activities and plans. Further, while a representative of ENISA is a permanent observer in meetings of the ECCC's Governing Board under the ECCC Regulation[44], there is no equivalent provision in the Management Board of ENISA. This renders the collaboration fragmented and inefficient.

#### 2.1.2. *Problem 2: Stalled implementation of the ECCF*

The CSA (2019) set up **the ECCF** for the development of voluntary EU cybersecurity certification schemes for specific ICT products, services, processes, and, through a later amendment, for managed security services, to ensure an adequate level of cybersecurity and avoid fragmentation. However, despite broad support and acknowledged value of the ECCF and the efforts harmonise cybersecurity certification across the EU, significant challenges remain.

**Member States and industry have voiced their concerns over the lengthy process of selection**, elaboration and adoption of cybersecurity certification schemes, with Member States recurringly noting their *"slow and challenging development"*[45]. The reply to public consultation further shows dissatisfaction of over 70% of the respondents with the time required to develop and adopt the schemes. Companies are particularly critical in this regard, showing alignment between large companies (80%) and small companies (78%).

Indeed, nearly five years after the CSA's entry into force, **only one of five requested certification** schemes (the European Common Criteria-based cybersecurity certification scheme (EUCC)), was adopted, while the EU Cloud Certification Scheme (EUCS) and the EU 5G Cybersecurity Certification (EU5G) have faced repeated delays of four to five years or even blockage. Meanwhile the expectation and market standard for scheme development is estimated to be 2-2,5 years[45]. This stalled implementation of ECCF triggers real-world strategic, security and business problems:

*First*, it has **hindered its capacity to support the implementation of a robust cybersecurity framework across the EU**. In the current setting, it cannot effectively deliver the needed support for the compliance with the security requirements laid down by multiple Union legislative acts (eIDAS2, CRA, NIS2, CSoA).

*Second*, the **businesses could not consider certification a viable business opportuni**ty. The first Union Rolling Work Programme for Cybersecurity Certification (URWP)[49], intended to define priorities and identify suitable ICT products, services and processes for certification, was only adopted in 2024, nearly 4 years after the date set out in the CSA[50]. Unclarity of coverage of risks and mixing of aspects that go beyond technical risks also affected the predictability of upcoming certification schemes.

*Third*, while there is an expectation from both businesses and authorities for certification schemes to support compliance processes, the absence of EU-wide certification schemes forces Member States and industry to **rely on national-level schemes** (e.g. for cloud

---

[43] COM(2025) 148.

[44] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

[45] According to the targeted consultation conducted between July and August 2025 with the Member States experts in the ECCG and interviews of the relevant ENISA personnel.

services; the German C5 attestation[51] or the French SecNumCloud[52]), **placing additional burden on companies, in particular SMEs, and hindering competitiveness**. This lack of harmonisation, where providers of cloud services need to comply with four different sets of security requirements to provide their services in Germany, France, Spain and Netherlands, complicates cross-border procurement, limits the scalability of cybersecurity solutions, forcing providers to develop software solution per national market. It also burdens SMEs with navigating multiple non-aligned or non-standardized schemes lacking mutual recognition and limit their possibility to scale-up.

*Annex 10* provides a general overview of **ENISA's key stakeholders, their expectations and unmet needs, including with regards to certification**.

#### 2.1.3. *Problem 3: Complexity and diversity of the cybersecurity-related policies impacting the Union's cyber posture*

The EU has horizontal and sectorial cybersecurity-relevant acts or policies, as mentioned in *Section 1*. These require entities to take cybersecurity risk-management measures and demonstrate compliance with requirements as set out in Union or national transposition law.

*First*, while these requirements are designed to achieve the **specific objectives of the respective acts**, the public consultation evidenced that the **similar cybersecurity risk-management measures required under different legal acts, and various required ways to demonstrate compliance, therewith creates high administrative burden on businesses**[46]. Many respondents indicated that multiple frameworks apply to their entities, including NIS2, GDPR, DORA, CER and the AI Act. For instance, diverging compliance requirements for security measures from various legal acts are evidenced in their deviating rules and terminology as can be seen in Guidance Materials developed by an Aviation Cybersecurity Subgroup under the NIS Cooperation Group.[47] In the Implementation Dialogue on Cybersecurity Policy held by EVP Virkkunen on 15 September 2025, stakeholders raised concerns about the cumulative burden of demonstrating compliance with multiple cybersecurity obligations set out by various Union acts. For instance, in the aviation sector reportedly it took two to three months to map the NIS2 Directive and PART-IS for an entity's systems, raising doubts whether this is manageable for smaller companies. The stakeholders also raised that SMEs are struggling to interpret which regulations apply to them and in what manner and to ensure compliance without exhausting their resources. This fragmentation increases administrative overhead, undermining a unified EU market approach.

*Second*, undertakings and groups of undertakings which have entities falling under the **jurisdiction of several Member States**, are often **subject to different approaches to supervision of cybersecurity requirements across Member States, which can result in** an administrative burden when demonstrating compliance, as the entities have to invest time and resources required to map in particular national frameworks internally for

---

[46] According to Frontier Economics, *Assessing the Economic Impact of EU Initiatives on Cybersecurity*, direct costs of implementing the NIS 2 Directive across the EU are EUR 31.2 billion per year. The report also mentions the risk that businesses *"face unnecessary compliance costs as a result of following multiple different notification and vulnerability assessment processes"*; source: https://www.frontier-economics.com/media/izyk5rgz/assessing-the-economic-cost-of-eu-initiatives-on-cybersecurity.pdf.

[47] These legal acts relate to aviation security (EC Regulation 300/2008 and its implementing acts), aviation safety (Part-IS and within the framework of EC Regulation 2018/1139) and the NIS 2 Directive.

compliance purposes.[48] Entities which are subject to different national cybersecurity frameworks may have to obtain several certifications, increasing costs for compliance.

*Third,* regarding the **scope of application of the NIS 2 Directive**, certain challenges to the interpretation of provisions for both the entities and the Member States were systematically brought to the attention of the Commission services, notably during meetings of the NIS Cooperation Group, demonstrating the need for clarification. For example, the definitions of healthcare providers, electricity producers and entities from the chemical sector have been criticised as providing for a wider scope than envisaged during the preparation of the NIS2 Directive[49]. Likewise, stakeholder feedback has highlighted disproportionate requirements arising from the application with regard to certain entities that would be subject to the Directive irrespective of their size, such as domain name system (DNS) service providers[50].

#### 2.1.4. *Problem 4: Increasing ICT supply chains security risks*

##### 2.1.4.1. Key concepts around ICT supply chain and interplay between technical and non-technical risks

*First,* understanding information and communication technology (ICT) supply chains security risks requires defining supply chains and ICT supply chains, and clarifying the notions and distinction between technical risks and non-technical risks.

**Supply chains** can be defined as the entire sequence of activities, organisations, resources, and technologies involved in the production and distribution of goods or services from raw material extraction to final delivery to consumers, including disposal or reuse. Within supply chains, **ICT supply chains** can be identified as a network of entities, processes, and technologies involved in the development, delivery, and maintenance of ICT products and services, including provision of support during ICT products and services' life cycle[51]. This includes hardware, software, and digital services that are critical to the functioning of modern digital infrastructure. They underpin critical infrastructures and ensure the flow and provision of essential goods and services – from transport, digital infrastructure and semiconductors to energy, food, medical supplies, banking. In a time of heightened geopolitical tension, control over ICT supply chains can be used as a tool of influence and coercion.

ICT supply chains are vulnerable to two types of risks:

- **technical risks** can be defined as dangers arising from failures in the components, configurations or human error within the supply chain or from disruption of the

[48] ECSO, *Streamlining Regulatory Obligations (2025)*, Streamlining-Regulatory-Obligations_Action-Plan_v2.pdf.

[49] The Impact Assessment accompanying the proposal for the NIS2 Directive (SWD(2020)345 final, part 1/3) estimated that 110,000 entities would be scope (see p. 70). However, based on experience from the implementation of the Directive, as of November 2025, the number of entities in scope is estimated as at least 160,000 (see pp. 62 – 63 of the Staff Working Document accompanying the proposal for a Digital Omnibus, SWD(2025)836 final)).

[50] Regardless of their size, DNS service providers are also in scope of the Commission Implementing Regulation (EU) 2024/2690, which sets out more detailed provisions regarding cybersecurity incident reporting and risk-management measures by further specifying Article 21(2) and Article 23(3) of the NIS 2 Directive vis-à-vis the relevant types of entities.

[51] Council of the European Union, Council conclusions on ICT supply chain security, 17 October 2022, no. 13664/22.

supply chain as such. Technical risks may occur accidentally or result from malicious cyber activity[52], such as a cyber threat actor exploiting a vulnerability to compromise a network/system. Technical cybersecurity risks such as phishing or a malicious software update, can affect both software or hardware, or arise from potential deficiencies in the security processes of any stakeholder along the supply chain. Existing regulatory framework such as the current CSA, the NIS2 Directive and the CRA address such technical cybersecurity risks.

- **non-technical risks** could be defined as the likelihood of the supplier being subject to undue influence by a third country with the potential to cause loss or disruption of the service provided or to compromise the product manufactured by an entity or to lead to exfiltration of data, including for the purposes of espionage or revenue generation. This could be the case when the suppliers of services or products are established or controlled by entities from certain third countries, subject to laws which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited.

*Second*, regarding the **interplay between technical and non-technical risks**, these should not be regarded as being mutually exclusive. For instance, a software vulnerability (technical risk) can be weaponised where the law and governance in place in a given country leads to mandatory reporting to a public authority before a patch is available (non-technical risk).

Additionally, in practice, non-technical risks alone – i.e. with no interplay with technical risks – can result in arbitrary and possibly extraterritorial governmental access to any kind of company operations or data, including sensitive data. Non-technical risks can enable a third country to engage into economic espionage, carry out malicious cyber activities or campaigns against the Union and its Member States, or engage in irresponsible state behaviour in cyberspace, leading to potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. Non-technical risks can also be linked to concealed vulnerabilities or backdoors.

#### 2.1.4.2. Destabilisation and disruption using ICT supply chains security risks

Concerns over the security of ICT supply chain are apparent from the public consultation, as well as calls from European Parliament and Council against a background where the current EU regulatory framework does not contain dedicated instruments to address non-technical risks.

Respondents elaborated on the types of threats contributing to ICT supply chain-related cybersecurity incidents, commonly citing compromise of third-party software components, insertion of malicious code during software development or updates, and poor security practices among suppliers *(see Annex 2)*. These replies echo the findings of ENISA. According to the Agency's Threat Landscape 2024, supply chain attacks remain

[52] Drawing on the United States' National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/malicious_cyber_activity, malicious cyber activity can, in the European Union context, be defined as activities that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

one of the seven prime threats to cybersecurity[53] . It was already in 2021 identified as the second most prevalent initial vector for infection[54] and was estimated that between 39% and 62% of organisations were affected by a third-party cyber incident[55].

*First*, ICT supply chain attacks entail strong financial, economic and societal impacts. A supply chain breach, even if seemingly small, can expand through the supply chain through lateral movement, affecting interconnected suppliers, partners, and customers, triggering a chain reaction often referred to as the domino effect[56]. Supply chain compromises take the longest time to detect and contain (267 days)[57] *(see Annex 7, part 1)*. Their aftermath includes direct and indirect costs ranging from costs of IT support to reputational and financial damage, severely impacting end users and, in some cases, leading to business closures due to customers losing confidence in the company's ability to protect their data[58]. In this regard, the average global direct cost of supply chain compromise as initial attack vector is estimated at USD 4.91 million[59] *(see Annex 7, part 1)*. The breach may further lead to rise of cybercrime against end users through ransomware attacks or data theft.[60]

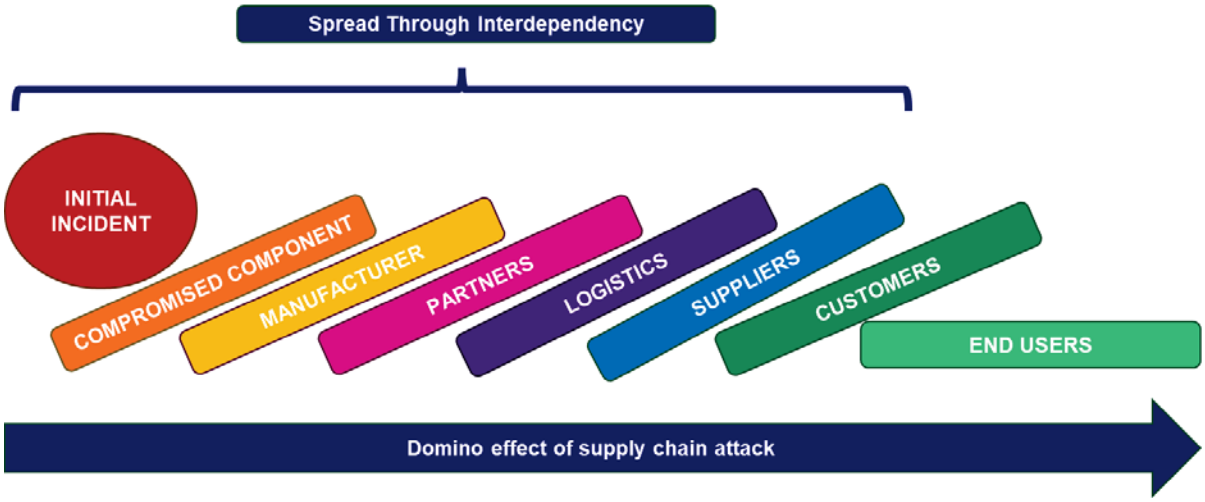



*Figure 1: Illustration of supply chain dependency*

[53] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[54] ENISA, *Good practices for supply chain security*, https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Supply%20Chain%20Cybersecurity.pdf.
[55] WEF, *Global Cybersecurity Outlook 2022*, https://www.weforum.org/publications/global-cybersecurity-outlook-2022/ or Anchore, *2022 security trends: Software supply chain survey*, https://anchore.com/blog/2022-security-trends-software-supply-chain-survey/.
[56] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[57] IBM, Cost of a data breach report 2025, https://www.ibm.com/reports/data-breach.
[58] Black Kite, The True Impact of Cascading and Concentration Risk, https://www.fbcinc.com/source/virtualhall_images/2023_Virtual_Events/DISA_JSP_(July)/Black_Kite/Black_Kite_Concentration_and_Cascading_Risk_EBook.pdf.
[59] IBM, Cost of a data breach report 2025, https://www.ibm.com/reports/data-breach.
[60] Cybersecurity Insiders, *The Domino Effect of Cyber Incidents: Understanding the Ripple Impact of Cybersecurity Breaches*, https://www.cybersecurity-insiders.com/the-domino-effect-of-cyber-incidents-understanding-the-ripple-impact-of-cybersecurity-breaches/.

**Example of an impactful supply chain attack: The SolarWinds case**

In December 2020, malicious activity that led to the compromise of the software of a major provider was exploited to access data of more than 18,000 of the providers' customers. According to CERT-EU, the attack was a very sophisticated supply chain attack[61]. According to a survey[62], 85% of SolarWinds cyberattack victims said the attack had an impact ranging from 'small' to 'significant'. One of the most notable impacts was its financial fallout. On average globally, the attack cost companies 11% of their annual revenue. These financial costs include incident response and remediation, system upgrades, legal and regulatory fines, customer notification and support, operational disruption and downtime, in addition to a wide range of indirect and long-term costs such as reputational damage and loss of trust, loss of intellectual property and sensitive data, insurance premium increases, litigation and legal fees, or loss of competitive advantage.

Beyond impacts for supply chain actors and possible direct impacts on public entities, ICT supply chains attacks can lead to indirect impact for governments, with a need to step in to protect national supply chains *(see further in Annex 7, parts 2 and 3).*

**An example of state-level impact of ICT supply chain attacks: the Jaguar Land Rover case**

In September 2025, a major cyberattack forced Jaguar Land Rover (JLR) to halt production across its factories in the UK, China, Slovakia, and India, after its IT systems were effectively disabled by the attack. As a consequence, the manufacturer is forced to suspend production for weeks, crippling the automotive manufacturing sector, disrupting global supply chains, and threatening SMEs and thousands of jobs[63], 30,000 people being directly employed at the company's UK plants and 100,000 working for firms in the supply chain[64]. The incident triggered a 1.5 billion pounds loan guarantee from the British government to protect affected jobs.

*Second*, weakening of the ICT supply chain entails risks to European economic security[65]. The exposure to non-technical risks of the supply chain for ICT products has been internationally recognised in the context of efforts to ensure economic resilience and security, with a commitment to ensuring that *"sensitive technologies that are crucial for national security or could threaten international peace and security are appropriately controlled (...)"*[66]. Further, the Cybersecurity Working Group of the G7 agreed that in order to address Internet of things (IoT) cybersecurity in its entirety, both technical and non-technical risks , including the overall risk of influence of an IoT product vendor by a

---

[61] CERT-EU, *Multiple Vulnerabilities in SolarWinds Orion*, https://cert.europa.eu/publications/security-advisories/2020-060/.

[62] IronNet, 2021 *Cybersecurity Impact Report*, https://www.ironnet.com/hubfs/IronNet-2021-Cybersecurity-Impact-Report-June2021.pdf?hsLang=en&submissionGuid=39c8446a-6789-41e5-8652-a7dd61b8af94.

[63] The Guardian, *Jaguar Land Rover extends production shutdown after cyber-attack*, https://www.theguardian.com/business/2025/sep/16/jaguar-land-rover-production-shutdown-cyber-attack.

[64] BBC, *Government to guarantee £1.5bn JLR loan after cyber shutdown*, https://www.bbc.com/news/articles/cgl15ykerlro.

[65] See in this regard the European Economic Security Strategy, JOIN/2023/20 final.

[66] G7 Leaders' Statement on Economic Resilience and Economic Security, 20 May 2023, https://www.consilium.europa.eu/media/64501/g7-statement-on-economic-resilience-and-economic-security.pdf.

third country, should be taken into account.[67] At the **global level**, several international partners have taken or are planning action in this fieldto strengthen supply chain security, with the UK and Canada providing for legal safeguards to security of the telecommunication infrastructure, including from high-risk suppliers, the US and Australia having even broader approach.

The **EU's 2023 Economic Security Strategy** also recognised as a priority the promotion of our own competitiveness by making our economy and supply chains more resilient bolstering innovation and industrial capacity.[68]

*Third*, ICT supply chain is a vector for disruption in a geopolitically instable world. Among non-technical risks, state-backed cyber campaigns targeting critical infrastructure have reached unprecedented levels of scale and sophistication. Hostile foreign states and state-sponsored actors seek to infiltrate and disrupt the EU's critical infrastructure and supply chains, not merely for intelligence gathering, but to establish latent control and disruption capabilities. At the same time, state-nexus threat actors have always been increasingly adept at understanding the environments they infiltrate[69]. They strategically deploy tools to conduct thorough reconnaissance and prevent the detection and analysis of their implants by employing robust anti-forensic measures[70]. Predominantly, actors associated with Russia, Iran and North Korea continue to deploy disruptive malware[71]. These activities oftentimes have the aim of espionage, i.e. to gather political, military and economic intelligence; or strategic disruption, i.e. to position oneself in critical infrastructure for a possible disruption of essential service in the future, for instance in the case of a conflict.

**Example of a state using ICT supply chains as a means of disruption**

The Chinese state-sponsored '**Salt Typhoon'** campaign[72] , whereby the threat actor gained access to targets through a partner or a vendor or, targeted telecommunications entities around the world with the potential for major cascading effects including on public safety and Union security. Chinese state-sponsored actor '**UNC5221**' compromised dozens of organisations worldwide by targeting vulnerabilities in Ivanti IT security products. These activities should be placed in the context of Chinese companies owning or having stakes in a wide range of European critical infrastructure, including

[67] Chairs' statement on G7 Cybersecurity Working Group meeting (2025), https://www.cyber.gc.ca/en/news-events/chairs-statement-g7-cybersecurity-working-group-meeting.

[68] Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy, 20 June 2023, JOIN/2023/20 final.

[69] Crowdstrike, *Global threat report*, https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf.

[70] Mandiant, *Active North Korean campaign targeting security researchers*, https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/ or Cisco, *ArcaneDoor - New espionage-focused campaign*, https://blog.talosintelligence.com/arcanedoor-new-espionage focused-campaign-found-targeting-perimeter-network-devices/.

[71] Palo Alto, *Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors*, https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/, Mandiant, *The GRU's Disruptive Playbook*, https://www.mandiant.com/resources/blog/gru-disruptive-playbook or Reuters, *North Korea hacking teams hack South Korea defence contractors - police* https://www.reuters.com/technology/cybersecurity/north-korea-hacking-teams-hack-south-korea-defence-contractors-police-2024-04-23/.

[72] Cybersecurity and Infrastructure Security Agency, *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

ports, airports, customs, electricity companies, wind and solar farms and telecommunication, as well as the strategic aim of China to secure its access to EU markets and technologies.[73]

## 2.2. What are the problem drivers?

Whereas three drivers are common to all problems ("horizontal drivers"), other drivers relate to one or several problems. These are presented hereafter. Following a different categorisation of the drivers, some elements of the drivers are linked to the scope whereas other elements are linked to implementation and management. This classification is presented in the table below.

Table 1: Elements of the drivers linked to the scope and linked to implementation and management

| | **Elements of the drivers linked to the scope** | **Elements of the driver linked to implementation and management** |
|---|---|---|
| **Driver 1** | Evolution of threat and technological landscapes insufficiently catered for (horizontal)<br>Geopolitical factors insufficiently catered for (ECCF) | |
| **Driver 2** | Prioritisation of tasks across legislations, new tasks (ENISA mandate)<br>CRA and NLF coherence (ECCF)<br>Certification of cyber posture not covered (simplification)<br>No maintenance mechanisms (ECCF)<br>ICT supply chain security not covered (ICT supply chain<br>No support for supervision (simplification)<br>Interplay with NIS2 not sufficiently anticipated (simplification, ENISA mandate) | Ineffective synergies with other bodies (ECCF)<br>Procedural deficiencies, lack of transparency (ECCF) |
| **Driver 3** | High dependency on non-European suppliers not covered (all)<br>Dependency on high-risk suppliers not covered (all)<br>Non-technical risks not covered (all) | |
| **Driver 4** | Lack of clear focus of ENISA's role in providing support in consistent implementation throughout the EU (ENISA mandate, ECCF)<br>Weak and undefined mandate on cybersecurity skills (ENISA mandate)<br>Mandate unfit for active and operational role (ENISA mandate) | Overstretching of ENISA resources (ENISA mandate) |
| **Driver 5** | Lack of sufficient synergies between the mandates of ENISA and the ECCC as regards research and innovation.<br>Lack of structured frameworks on how the Agency supports capacity building efforts in third countries | |

[73] Council on Foreign Relations, *China's approach to global governance*, https://www.cfr.org/china-global-governance/.

| | | |
|---|---|---|
| | Overlapping roles and responsibilities and lack of clear framework on cooperation between ENISA and other EU Agencies (ECCF) | |
| **Driver 6** | Absence of maintenance structure in the CSA<br>Lack of clarity regarding the harmonisation effect of the schemes (ECCF) | Lengthy adoption processes (ECCF)<br>Unpredictable timings and lack of transparency in the development process of schemes; difficulty to translate draft schemes into implementing acts (ECCF)<br>Unclear and rigid governance (ECCF) |
| **Driver 7** | Bottlenecks created by the interplay CRA/ECCF | Increasing demand for schemes (ECCF) |
| **Driver 8** | Definitions missing, not clear enough or inconsistent with other acts (ENISA mandate, simplification)<br>Diverging requirements for notification and reporting (ENISA mandate, simplification) | Empowerments or supporting guidance for NIS2 implementation not used to their full potential (ENISA mandate, simplification) |
| **Driver 9** | No obligation for entities to comply with supply chain security measures based on non-technical risks (ICT supply chains)<br>Limited scope of specific supply chain security risks in specific areas not covering the whole spectrum of non-technical risks (ICT supply chains) | Diverging implementation of security measures (ICT supply chains) |

#### 2.2.1. *Driver 1 – Increasingly hostile and unpredictable threat landscape in a rapidly evolving technological environment (horizontal driver).*

The threat landscape, as well as the security and defence prerequisites for Europe, have changed significantly since 2019[74]. These realities triggered a renewed need for a **stronger and more strategic role of ENISA as well as for a stronger leveraging position of the EU globally,** while building own capabilities in a more sustainable manner in a number of areas, such as vulnerability disclosure, where there are current dependencies of common vulnerabilities and exposure services on one third country government steer and funding, as well as management or standardisation. Russia is waging a hybrid campaign against the EU and its Member States, using cyberattacks as one tool; China is seeking to advance its geopolitical agenda through control of **supply chains**, exploitation of software vulnerabilities and economic dependencies: these trends demand **increased operational cooperation**, at the forefront of which enhanced **shared situational awareness** among Member States, EU entities *(see Annex 10)*. In addition, after Brexit, the EU is not part of the main intelligence network (the Five Eyes alliance between the US, CAN, UK, NZ and AU).

Furthermore, technical evolutions such as AI are giving both cyber criminals and non-state and state actors a whole new set of capabilities, reducing the time for mass exploitation of vulnerabilities from weeks or months to a matter of days. Emerging technologies are further considered by cybersecurity professionals to be the biggest

[74] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

challenge to come in the EU in the next two years[75]. The World Economic Forum (WEF) acknowledges that skills in operating AI and defending against it are becoming increasingly important, and companies must commit to equipping their workforce and educational curricula should *"mirror the dynamic of cyberthreat landscape and emerging technologies"*[76]. While ENISA is uniquely placed to facilitate this shared awareness, the Agency is currently not appropriately equipped to enhance its support in this area.

The evolution of **geopolitical landscape** considerably affected the **ECCF**. According to the 2024 Evaluation Report, 49% of stakeholders considered that geopolitical factors impacted the ECCF negatively or highly negatively. In particular, the politicisation of the discussion related to the structure of the cloud computing market in Europe (heavily dominated by non-EU players) impacted the development of EUCS. Triggering factors included international developments such as the adoption of the US Cloud Act and the related privacy concerns. Several other EU initiatives, such as the European strategy for data[77], and the subsequently adopted the Data Act and the Data Governance Act, reflected the increasing concern about the protection against unlawful access to data stemming from third-country legislations that have extra-territorial effects in conflict with EU laws.

In this context, the uncertainty related to the scope of the ECCF as to the types of risks covered *(see Driver 8)* became prominent. It created political bottlenecks in the preparation of candidate schemes due to disagreements between Member States. It has also triggered criticism regarding the lack of transparency of the framework and insufficient stakeholder involvement[78] and that the certification would go against the security interests of the EU by certifying hyperscalers, and creating overdependency on non-EU provider.

#### 2.2.2. *Driver 2 – Regulatory gaps (horizontal driver)*

Since the adoption of the CSA in 2019, the EU cybersecurity regulatory landscape evolved considerably *(see Section 1).*

Each of the instruments is either filling regulatory gaps or resetting focus of policy objectives and compliance facilitation. Main regulatory gaps were identified and are **further detailed in Annex 9**.

---

[75] ISC2, *First Look at the 2024 Cybersecurity Workforce Survey*, https://digital-skills-jobs.europa.eu/system/files/2024-12/ISC2_Workfoce-Study-Findings-EU.pdf.
[76] WEF, *Global Cybersecurity Outlook 2025*, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.
[77] COM(2020)66 final.
[78] 2024 Evaluation report.

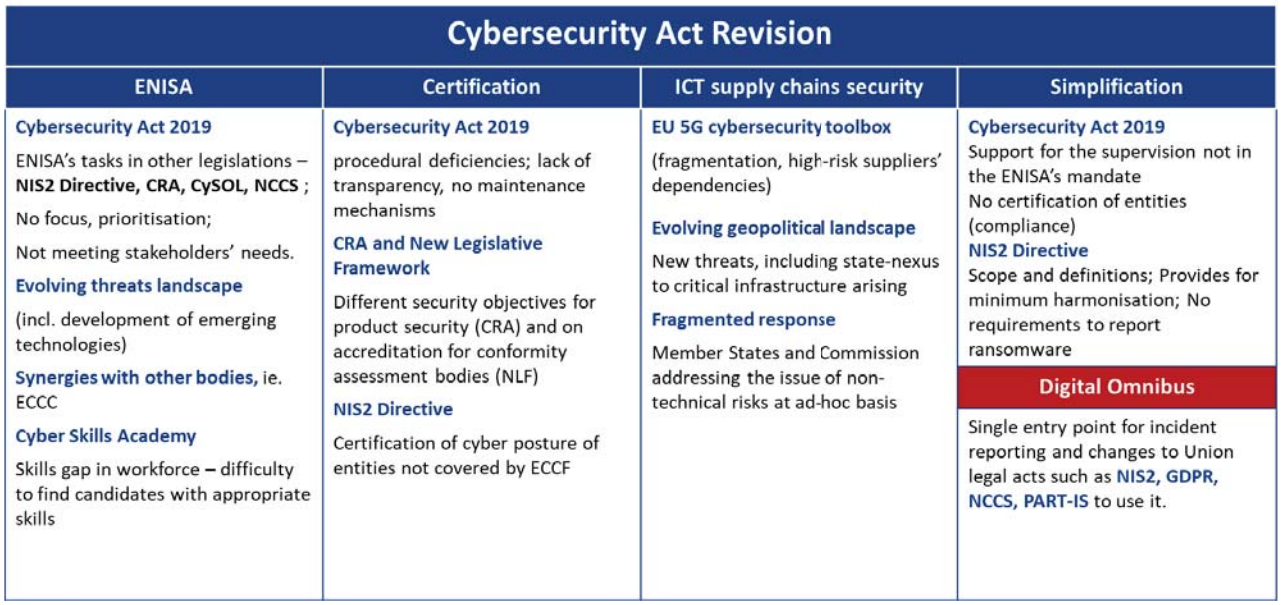



*Figure 2: Overview of regulatory gaps*

### 2.2.3. *Driver 3 – Vulnerabilities linked to non-technical risks (horizontal driver)*

As a general rule, in cybersecurity any dependency creates a vulnerability. A root cause for ICT supply chain risks, in particular non-technical risks, are the vulnerabilities induced by high dependency on non-European suppliers, on high-risk suppliers and single suppliers (lack of diversification of the supply chains). Additionally, non-anticipation of such non-technical risks can be identified as a source of stalled implementation of ECCF.

*First*, **high dependency on non-European suppliers leads to increased ICT supply chains security risks**. This covers the situation where the suppliers are established in or controlled by entities from a third countryposing cybersecurity concerns, factoring in legal obligations of suppliers subject to the third countries' laws or other obligations or requirements imposed on the supplier. In 2022, it was estimated that European countries were strongly digitally dependent for over 80% of their digital products, services, infrastructures and intellectual property[79]. For example, submarine data cables, which carry 99 % of inter-continental Internet traffic, where certain components are not manufactured by any single European supplier (e.g. submarine optical fibre), creating a strong reliance on non-EU suppliers[80].

*Second*, the risks are further increased in situations where such dependency exists on high-risk suppliers, as the possibility of foreign interference is substantially higher. This is the case especially if such dependency manifests itself in sectors and services which are of vital importance to key societal and economic activities, the sectors of high criticality and other critical sectors covered by the NIS2 Directive[81], such as banking, digital infrastructures, health, energy, transport, which have reportedly been affected by

[79] Centre on Regulation in Europe (CERRE), *Digital Industrial Policy for Europe*, https://cerre.eu/publications/digital-industrial-policy-for-europe.
[80] Report from the European Submarine Cables Expert Group to be published in September 2025.
[81] COM/2025/148 final.

supply chain security incidents as highlighted in reply to the public consultation *(see Annex 2).*

The presence of high-risk suppliers in the EU's 4G, 5G and fixed telecommunications networks[82] illustrates the extent of the Union's vulnerability, at the forefront of which strategic dependency and exposition of the EU to risks of third country interference[83]. Indeed, eleven Member States have reportedly an over 40% share of high-risk suppliers in their 5G radio access network (RAN) and 41% of the mobile subscribers in Europe have access to 5G RAN from high-risk suppliers[84]. This vulnerability becomes particularly exacerbated considering the role of 5G in modern defence systems, military logistics and counter drone initiatives, where it should be seen against a backdrop of the no limit partnership announced by Russia and China in February 2022.

***Illustrative case of vulnerability: the EU's high dependency on high-risk supplier for photovoltaic systems***

Solar inverters are highly critical components for delivering the core functions of a photovoltaic system, significantly contributing to grid stability and holding information about electricity demand[85]. Nine of the top ten inverter shipment leaders from 2023 were headquartered in China[86]. From a total of 350 Gigawatt (GW) photovoltaic inverter shipments to Europe over 2015-2023, 225 GW or 64% were coming from Chinese companies, with 114 GW from Huawei alone[87]. In 2023, 70% of inverters installed in Europe originated from Chinese vendors, with two Chinese vendors having control of remote access to 168 GW of photovoltaic capacity in Europe[88].

Technical risks arise from the fact that inverters are connected to the Internet, allowing remote access for software and firmware. Those technical risks could also be a vehicle for non-technical risks if connected with the inverters; supplier could be subject to an interference from a third country. Switching off inverters remotely, changing their settings and behaviour can destabilise power grids, damage energy infrastructure, trigger widespread blackouts and prevent grid recovery. In addition to this risk of sabotage, insight into operational data of solar inverters can provide real-time grid intelligence and reveal the location and behaviour of sensitive assets that can be exploited for strategic,

---

[82] Strand Consult, *The Market for 5G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 31 European Countries*, https://strandconsult.dk/the-market-for-5g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-31-european-countries/.

[83] NIS Cooperation Group, *EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors*, https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors.

[84] Strand Consult, *The Market for 5G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 31 European Countries*, https://strandconsult.dk/the-market-for-5g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-31-european-countries/.

[85] SolarPower Europe, *Inverters Explained*, https://www.solarpowereurope.org/advocacy/position-papers/inverters-explained.

[86] Wood Mackenzie, *Global PV inverter shipments grew by 56% in 2023 to 536 GW*, https://www.woodmac.com/press-releases/2024-press-releases/global-pv-inverter-shipments-grew-by-56-in-2023-to-536-gwac.

[87] SolarPower Europe, *Solutions for PV Cyber Risks to Grid Stability*, https://api.solarpowereurope.org/uploads/SPE_2025_Solutions_for_PV_Cyber_Risks_to_Grid_Stability_032dc2ae5a.pdf?updated_at=2025-04-29T07:11:32.315Z.

[88] European Solar Manufacturing Council, *Restrict Remote Access of PV Inverters from High-Risk Vendors*, https://esmc.solar/restrict-remote-access-of-pv-inverters-from-high-risk-vendors/.

economic, or military advantage.

Rogue communication devices not listed in product documents are reported to been found in Chinese solar power inverters[89]. The rogue components provide additional, undocumented communication channels that could allow firewalls used by utility companies to prevent direct communication back to China to be circumvented remotely[90], with potentially catastrophic consequences as described above. Furthermore, a recent bibliometric study of open-source Chinese academic literature[91] has revealed a systematic and sustained research effort focused on identifying vulnerabilities in Western power grids, including those in Europe (with over 150 Chinese-authored publications simulating disruptions targeting EU.

*Third,* **the non-anticipation of non-technical risks** can be considered a root cause for the stalled implementation of ECCF. Drawing on the experience of the preparation of several schemes, major issues related to how to cater for non-technical risks have stalled the adoption of the schemes (blockage of the EUCS and the EU5G). The ECCF was not designed to cover these risks in an efficient manner as it only addresses technical risks.

#### 2.2.4. *Driver 4 – Unsuitable ENISA mandate and resources to evolve with EU cyber ecosystem's and regulatory needs.*

The current CSA does not reflect properly the nature of the tasks that has been given to ENISA through different Union legal acts nor the needs of the cybersecurity ecosystem or the focused European added value that such agency is needed to be in support of the EU cybersecurity objectives *(see Driver 2 and Annex 9).* What is more, the current resourcing model is not appropriately matching its new responsibilities. The **current CSA does not ensure a clear focus of ENISA's role in providing support in consistent implementation throughout the EU**, with certain new tasks carrying an important weight, for instance managing and enriching vulnerability records or standardisation support for the CRA and for ECCF. Certain other tasks in the CSA also give a very broad mandate to ENISA, without providing a focus or direction, i.e. in the area of international cooperation[92].

In contrast, regarding the growth and strengthening of the **cybersecurity workforce, ENISA's current mandate is further weak and undefined[93]**, with no clarification on how ENISA can achieve the objective of supporting its stakeholders in addressing the skills and talent gap. As a result, ENISA's support in this field lacks necessary focus, visibility and scaling, as shown by strong disparity in the level of awareness and uptake

[89] Reuters, *Rogue communication devices found in Chinese solar power inverters*, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.
[90] Ibid.
[91] Homeland Security Today, *China Is Studying How to Hack and Crash Our Power Grids*, https://www.hstoday.us/subject-matter-areas/cybersecurity/china-is-studying-how-to-hack-and-crash-our-power-grids.
[92] 2024 Evaluation report.
[93] The current CSA provides that one of the objectives of ENISA is "*to assist stakeholders to develop skills and competencies in the field of cybersecurity*" and refers to trainings that can be delivered to public entities.

of the 2022-born European Cybersecurity Skills Framework (ECSF) across Member States[94].

Additionally, whereas ENISA has been entrusted in the **communication on the Cybersecurity Skills Academy with the development of a pilot project** exploring the set-up of a European attestation scheme for cybersecurity skills, it lacks the means and prioritisation of this task to implement the project in a timely and thorough manner[95].

Also, ENISA's mandate is not constructed for the agency to take a more active and operational role. This is particularly the case of sharing sensitive information based on enhanced EU situational awareness or handling sensitive reported incidents.

In parallel, ENISA's budget has increased from almost EUR 17 million in 2019[96] to more than EUR 26 million in 2024[97]. While the increase may be seen as noticeable, it does not address the actual needs. The increasing use of contribution agreements to deliver some tasks, such as the Cybersecurity Support Action, also demonstrates the lack of sufficient resources.

As concluded by the 2024 Evaluation report, the **proliferation of tasks is overstretching ENISA's resources** and its ability to focus actions on alignment with the Union's priorities and stakeholders' expectation. Insufficient resources limit ENISA's ability to respond with the necessary agility to the dynamic cybersecurity and technological landscape. There is a relatively small and not steady increase of FTEs between 2017 (83.25 FTEs) and 2024 (110.74 FTEs) *(see Annex 11)*. The number of main activities carried out by ENISA grew from 5 Activities in 2017 to 13 in 2024 *(see Annex 11).*

#### 2.2.5. *Driver 5 – Complex and fragmented collaboration on cybersecurity among EU agencies, governance bodies and stakeholders.*

In the area of research and innovation, ENISA advises on priorities, participates in implementation, and contributes to the EU strategic innovation and research agenda. However, with the creation of the ECCC, which now manages relevant parts of the Digital Europe Programme (DEP) and Horizon Europe, strengthening cybersecurity technology and industrial capacities in the EU, there is a risk of inefficiencies and lack of sufficient synergies between the mandates of ENISA and the ECCC as regards research and innovation.

On the international level, while the international cybersecurity policies have significantly evolved since 2019, ENISA responds to requests of third countries and organisations on an ad hoc basis. For instance, ENISA signed a contribution agreement with the Commission to support Western Balkans. This shows a lack of structured

---

[94] Eurobarometer (2023) Flash Eurobarometer 547 on Cyberskills, https://europa.eu/eurobarometer/surveys/detail/3176.

[95] See ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf, which identifies "leading the process for the attestation of skills" as one of the eleven tasks associated to "Support the implementation and uptake of EU cybersecurity skills framework" while considering it "a high priority task".

[96] See point 3, *Statement of Revenue 2019 in ENISA's annual budget 2019*, https://www.enisa.europa.eu/sites/default/files/all_files/ENISA%202019%20Annual%20Budget.pdf.

[97] ENISA, *ENISA Annual Report on Budgetary and Financial Management*, https://www.europarl.europa.eu/cmsdata/294501/ENISA%20RBFM%202024.pdf.

frameworks on how the Agency will be supporting the Union capacity building efforts in third countries.

The wider EU cybersecurity ecosystem involves numerous overlapping roles and responsibilities. For example, with regard to the ECCF, ENISA co-chairs the Stakeholder Cybersecurity Certification Group (SCCG), establishes and steers ad hoc working groups, and consults private entities on the development of the certification candidate schemes, often involving the same stakeholders, multiple times. This brings a risk of inconsistency of the stakeholders' input, which would lead to inefficient use of resources. The ECCF also does not provide for a clear framework for the cooperation between ENISA and other EU Agencies and bodies in certification. This has contributed to the lack of meaningful collaboration with the European Data Protection Board (EDPB) to establish synergies with the GDPR's certification schemes.

#### 2.2.6. *Driver 6 – Implementation failure: The practical experience of the development and adoption process of first schemes*

Aside the lengthy adoption process for the first and only existing European cybersecurity certification schemes, the blockage in the development of EUCS and EU5G has evidenced technical complexities and general shortcomings of the framework, which were not estimated with the adoption of the CSA and hence negatively impacted the design and development of the schemes. This included in particular[98] (i) the unpredictable timings and lack of transparency in the development process of schemes; (ii) the difficulty to translate draft schemes into legal text (i.e. implementing acts) and (iii) the absence of maintenance structure in the CSA both evidenced by the implementation of the EUCC; and (iv) the lack of clarity regarding the harmonisation effect of the schemes, which was challenged mainly in the context of EUCS. For instance, the current requesting, development and decision-making processes do not envisage any clear development plan or even a timeline for a requested scheme, which leads to lack of predictability for stakeholders and accountability of the actors involved in the process (Commission, ENISA, ECCG).

**Unclear and rigid governance** has also resulted in coordination challenges across various stakeholder groups contributing to the scheme development. The 2024 Evaluation report also recognised these challenges and the private stakeholder groups have asked the Commission to clarify the scope of ECCF *(see Driver 2 and Annex 9)*, including whether the schemes should address non-technical risks or, to provide more legal clarity by including more elements (e.g. extended security requirements or continuity of certification activities during crisis scenarios).

Against this backdrop, the only adopted scheme, EUCC, demonstrates the potential of the ECCF as it has already gained solid uptake with over 20 accredited conformity assessment bodies[99] and multiple certificates issued since it entered into application in February 2025. It is expected to be immensely useful in the upcoming years due to its broad scope (any ICT products), and its harmonisation effect unlocking the single market benefits. Furthermore, Europe has a unique standing in the world of common criteria for

---

[98] Ibid.

[99] See Single Market Compliance Space, https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies/free-search?filter=notificationStatusId:1,notificationLegislationId:164702.

ICT products with 44% of the total assessment bodies, a number which we expect to grow in the coming years[100].

#### 2.2.7. *Driver 7 – Legislative developments not factored in the current ECCF*

The legislative developments in the area of cybersecurity since 2019 have been driving an **increasing demand for schemes,** as apart from providing a harmonised way of demonstrating security assurance, there is an increasing expectation they can facilitate compliance. At the same time, it revealed shortcomings in the scope of the framework and design of schemes (i.e. NIS 2 Directive demonstrated the absence of certification of entities). Furthermore, a growing number of legislations referred the ECCF as a mean to demonstrate compliance (CRA; AIA; NCCS).

The **interplay between the ECCF and the CRA** has also created following bottlenecks:

*First*, **the preparation and adoption of the CRA have significantly impacted the delay in the publication of the Union Rolling Work Programme** on strategic priorities for European cybersecurity certification schemes (URWP)[101]. The broad scope of the CRA impacting all products with digital elements and introducing a conformity assessment regime of such products, changed considerably the legislative context of the ECCF, as all potential ICT products for which a scheme could be developed are also covered by the CRA. While the CRA foresees that the schemes that can provide presumption of conformity, any scheme related to products shall be designed with the CRA in mind. The contrary would mean additional burden through duplications of requirements for manufacturers.

*Second*, **in the context of the EUCC (scheme for product certification), some general misalignment between the CRA and the ECCF has been evidenced**. This misalignment occurred while the EUCC was already well underway. Security requirements stemming from the CRA such as those related to vulnerability handling could not be considered from the design of the EUCC. Furthermore, the governance frameworks of the CRA based on the New Legislative Framework and the ECCF apply different regime for the governance (competence requirements, obligations and supervision) of conformity assessment bodies, which does not appear justified. For instance, a CAB does not have the same obligations towards the supervisory authority under the ECCF and the CRA. Those inconsistencies will lead to **administrative burden** for product manufacturers, public authorities and CABs.

#### 2.2.8. *Driver 8 – Fragmented compliance landscape and complexity of horizontal and sectoral frameworks*

Companies, notably those providing multiple different types of services, face various cybersecurity-related obligations under horizontal instruments, such as the NIS 2 Directive, the GDPR, as well as sector-specific instruments. As a result, compliance with cybersecurity risk-management measures involves navigating various legal requirements and, where relevant, different national transpositions and implementation approaches,

---

[100] ENISA, Evaluations & Certifications - State of Play 2018-2022, https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity%20Certification%20Statistics%20Report.pdf.

[101] SWD(2024) 38 final.

aggravated in cases where Member States adopt additional measures beyond the minimum harmonisation requirements of legal acts, such as the NIS 2 Directive[102]. Furthermore, national supervisory approaches for enforcing the same rules differ in Member States. They affect more strongly the undertakings and groups of undertakings which have entities falling under the jurisdiction of several Member States or are subject to obligations arising from multiple instruments.

In addition, several further clarifications and adjustments are needed, as revealed by the implementation process thus far and the interaction with stakeholders:

*First*, **certain scope-related clarifications to ensure legal certainty**, e.g. on the definitions of healthcare providers, electricity producers or with respect to entities from the chemical sector. For example, the Impact Assessment Report for the proposal for the NIS 2 Directive estimated the number of electricity producers as about 3,944 companies and the number of companies in scope as 82 main electricity generating companies. However, with the current definitions of NIS2, any entity that operates solar panels to consume the self-generated electricity could qualify as essential or important entity if they meet size-cap criterion of the NIS 2 Directive, which would be a far higher number given the increasing use of renewable sources. This broad interpretation leads to compliance burden for both entities, and for national authorities which have to supervise a larger number of entities than originally estimated. On the other hand, certain providers whose cybersecurity is necessary for critical services, such as providers of European Digital Identity Wallets and operators of submarine cable infrastructure, are not specifically outlined as a type of entity to be covered, which requires national authorities to use alternative legal options[103] to ensure that NIS2 obligations apply to those entities.

*Second*, the **EU level overview of entities under NIS2 scope and incidents to be reported**, is insufficient, affecting the overall EU situational awareness and the potential for an effective cybersecurity compliance across internal market. Furthermore, divergent requirements related to notifying specific types of cybersecurity incidents, in particular **ransomware incidents**[104], cause authorities to have a disjointed overview of the landscape of incidents, whereas the entities notifying incidents may face diverging requirements among Member States.

*Finally*, **empowerments or supporting guidance for NIS2 implementation were not used to their full potential** to level more the playing field in the implementation approaches across Member States. For example, suppliers to entities in scope of the NIS 2 Directive are confronted with diverse implementation and interpretation of the supply chain security requirements set out by the NIS 2 Directive. The absence of streamlined

---

[102] For examples of diverging national transpositions of the NIS2 Directive, see European Cybersecurity Organisation (January 2025) NIS2 Implementation: Challenges and Priorities. Available at https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf.

[103] Assessing whether the entity falls in scope of the NIS2 Directive on account of another type of service that it provides, or using Article 2(2), points (b)–(e), to identify the entity as falling under NIS2 scope.

[104] As an example of a specific national approach to ransomware, see draft legislation considered in Italy which would prohibit ransom payments and would also provide for a 6-hour deadline for reporting ransomware incidents, which is shorter than the 24-hour deadline set out in the NIS 2 Directive. Privacy Matters, *Italy: Ransomware and Crime – A proposal to tackle cyber extortion in Italy*, https://privacymatters.dlapiper.com/2025/06/italy-ransomware-and-crime-a-proposal-to-tackle-cyber-extortion-in-italy/.

approaches, inconsistent and overlapping security assessment practices like questionnaires, create additional administrative burden.

#### 2.2.9. *Driver 9 - Inadequate measures to address ICT supply chain cybersecurity risks*

Taking into account the growing threat to the cybersecurity of ICT supply chains, the EU has already put in place certain measures in recent years. Regarding technical risks, the CRA contributes to the supply chain security objectives by introducing cybersecurity requirements for hardware and software accessing the internal market. The ECCF, while addressing technical risks, it does not cover non-technical risks *(see Driver 4)*.The NIS2 Directive mandates Member States to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of network and information systems, including risks related to supply chain security and provides for a framework for Union coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains. It should be conducted at the EU level, taking into account technical and, where relevant, non-technical risk factors. These risk assessments conducted jointly by Member States, Commission and ENISA analyse specific critical supply chains, where critical dependencies and urgent risks may materialise in relation to specific assets, and high-risk suppliers. However, due to the nature of the NIS2 Directive and the fact that there is no obligation for entities to comply with supply chain security measures based on non-technical risks, their implementation varies at national level leading to fragmentation. This poses challenges to the internal market, as identification and restrictions of high-risk suppliers may vary among Member States.

For instance, in the area of 5G networks, five years after the adoption of the 5G Toolbox, there are still significant shortcomings and gaps[105]. Only thirteen Member States have implemented restrictions on high-risk suppliers. In addition, the scope of potential restrictions on high-risk suppliers is fragmented across Member States.[106] Differences exist also as regards, assets covered by those restrictions, with some Member States not following the recommendations of the 5G Toolbox. What is more, it is likely that a majority of Member States' authorities have no clear picture of which suppliers are present in the deployed networks. These divergencies were emphasised in the European Court of Auditors' audit on the 5G roll-out in the EU[107] stating that *"the absence of a concerted approach across the EU, may impact the effective functioning of the single market"*[108].

Beyond 5G, in the absence of comprehensive and effective measures at EU level, some Member States have also put in place national frameworks and measures to address non-technical risks related to ICT supply chain security risks (the Czech Republic[109],

---

[105] NIS Cooperation Group, *Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity*, https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.
[106] Ibid.
[107] European Court of Auditors, *5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved*, https://www.eca.europa.eu/en/publications?did=60614.
[108] Ibid.
[109] CZ Cybersecurity act (ZÁKON ze dne 11. června 2025 o kybernetické bezpečnosti), https://www.e-sbirka.cz/sb/2025/264/2025-11-01?zalozka=text.

Belgium[110] and Lithuania). However, the effectiveness of such measures may be limited where they are applicable only in one Member State.

Further, the Commission took action to reduce supply chain cybersecurity risks in the context of deploying energy from renewable sources[111] and hydrogen[112]. These recent initiatives also aimed to address non-technical cybersecurity risk factors. However, their scope remains limited to specific auctions and the measures set out in these initiatives are not apt to address in a comprehensive manner the whole spectrum of non-technical risk.

Although a number of measures have been taken at EU level and in Member States the Union lacks a comprehensive framework for addressing ICT supply chain risks.

### 2.3. How likely is the problem to persist?

All the aforementioned problems can only be expected to become increasingly acute.

The 2024 ENISA Threat Landscape Report[113] together with the 2025 EU-SOCTA Report[114] warn of increasingly complex, AI enhanced and state sponsored threats targeting critical infrastructure across Member States. ENISA's Foresight on Cybersecurity Threats for 2030[115] highlights that the skills shortage in the cybersecurity field and the vulnerabilities in legacy systems are amongst the top threats, especially for SMEs and the public administration. It highlights that emerging technologies and the rise of targeted attacks will result in higher and new classes of risks.

Furthermore, as highlighted in the Evaluation report[116] rapid technological change, overlapping funding initiatives and geopolitical instability are threats that could strain ENISA's resources and reshape policy priorities, requiring increased funding and access to resources.

The stakeholder feedback collected during the 2024 Evaluation report indicates that 46% of private bodies and 46% of national authorities perceive *"somewhat"*, *"to a small extent"* or *"not at all"* that ENISA provides added value to the activities of their organisation. As more responsibilities are added to ENISA under various legislative acts, its ability to prioritise and act in a focused effective manner is likely to continue to diminish without institutional adjustment.

Furthermore, without further simplifying and facilitating compliance with cybersecurity risk-management requirements, entities may disproportionately dedicate resources to compliance documentations. This may compromise their ability to invest and focus on substantive actions needed for preparedness and response. Given that multiple Member

---

[110] BE Raad van State - Arrest nr. 256.645, https://www.stradalex.com/nl/sl_src_publ_jur_be/document/rvst_256.645.

[111] Commission Implementing Regulation (EU) 2025/1176 of 23 May 2025 specifying the pre-qualification and award criteria for auctions for the deployment of energy from renewable sources.

[112] Terms and Conditions (T&Cs) for the second auction for the production of renewable hydrogen (IF24 Auction), via the Innovation Fund.

[113] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[114] Europol, European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg.

[115] ENISA. *Foresight Cybersecurity Threats For 2030 - Update 2024*, https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20For%202030%20Update%202024_0.pdf.

[116] 2024 Evaluation report.

States are still transposing some of the relevant legislation (in particular the NIS 2 Directive), without dedicated action, the issue of complexity in cybersecurity compliance and legal unclarity is likely to persist.

Meanwhile, without a clarified scope, streamlined procedures, lifecycle management mechanism and clear governance, new certification schemes are unlikely to emerge in a timely or coherent manner. However, there is a demand for schemes across the internal market. The 2024 Evaluation report notes that national certification schemes are increasing, despite the ECCF, which could lead to further fragmentation. Member States and the industry, especially those organisations operating across borders, confirmed the value of replacing national certification schemes with EU ones to ease administrative burden. It is expected that European cybersecurity certification schemes will remain highly relevant and complementary to the existing regulatory framework.

ENISA's Foresight on Cybersecurity Threats for 2030 further lists supply chain compromises as the number one threat. ENISA indicates that if not effectively addressed, this problem will persist and most probably will be aggravated, as it is foreseen that by 2030, there will be more integration of components and services combined into new products. The responses in the public consultation show that there is a strong perception of increasing cybersecurity risks in ICT supply chains, in a wide range of critical and highly critical sectors *(see Annex 2)*.

In conclusion, the available evidence indicates that the identified problems are well established in the current cybersecurity landscape and are not likely to be resolved through incremental change or Member States' initiatives alone.

## 3. WHY SHOULD THE EU ACT?

### 3.1. Legal basis

The legal basis for a revision of the CSA is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which empowers the European Union to adopt measures aimed at establishing and ensuring the functioning of the internal market. Regulation (EU) 2019/881, commonly known as the CSA, was originally adopted under this provision. The CSA established a permanent mandate for ENISA, and laid down the structure of the ECCF, intended to facilitate trust in ICT products and services across the EU.

The changes introduced in this proposal are based on the framework already established in the CSA and follow its regulatory logic. They are intended to strengthen ENISA's role in contributing to reducing the fragmentation of the internal market and further harmonise the approach at Union level to the cybersecurity certification.

In the area of the cybersecurity of ICT supply chain security, the fragmentation of national frameworks addressing non-technical risk factors brings negative effects to the functioning of the internal market in terms of data flows but also resilience and trustworthiness.

Amending the CSA under Article 114 TFEU is justified given the evolving nature of cybersecurity challenges, limited impact of the current act and the increasing interdependence of Member States' digital systems. Adjustments to the legal framework must reflect the most recent developments in the cybersecurity legislative landscape, especially in light of ENISA's growing responsibilities and the expanding scope of certifications and risk management.

The legal basis for the proposal for a Directive amending the NIS 2 Directive as regards simplification measures and alignment with the proposal for the CSA2 is Article 114 of the TFEU. This proposal amends the NIS 2 Directive which was adopted under Article 114 TFEU.

### 3.2. Subsidiarity: Necessity of EU action

ENISA's mandate has expanded through subsequent legislation, without a comprehensive revision of its core responsibilities and resourcing. This has created overlaps, inefficiencies, and insufficient prioritisation of core support tasks for Member States.

Several Member States have implemented their own national cybersecurity certification schemes, which significantly differ in scope and conformity assessment procedures. This creates market fragmentation and duplicative burdens for operators and SMEs, seeking to be certified once and operate across the EU. The ECCF was established in the CSA to address market fragmentation, but implementation has been slow and inconsistent.

Similarly, several horizontal and sectoral legal acts set out cybersecurity measures with different purposes and objectives, leading also to differences in compliance check and supervisory approaches set by Member States. As a consequence, entities, especially SMEs or businesses operating across several Member States face additional compliance burden, negatively impacting their competitiveness.

Concerning ICT supply chain security, dependencies on high-risk suppliers affect entities across the Union, while significant supply chain cybersecurity incidents often spread across national borders. Addressing the issue at national level alone is not likely to be efficient.

As is explained under Driver 9, diverse approaches to ICT supply chain security and different measures taken by the Member States lead to market fragmentation, and different compliance requirements for entities. In particular, given the cross-border nature of ICT supply chains, fragmentation of compliance requirements within the internal market would undermine legal certainty for entities. Differing national frameworks for the restriction of high-risk suppliers risks creating barriers for the movement of goods and services across borders within the internal market. Finally, as ICT supply chains may involve critical entities and infrastructure, regardless of where those suppliers are established, fragmentation and gaps in cybersecurity measures creates additional security risks to those entities.

Furthermore, the proposals for Multiannual Financial Framework (MFF) programmes include a horizontal provision which mandates the exclusion of high-risk suppliers identified under EU law, in order to protect the integrity of the EU budget and ensure that Union expenditure does not contradict essential Union security interest. The CSA supply chain framework would be the mechanism which allows for this identification in the area of ICT supply chains and can thus only be carried out at the EU level.

EU intervention is crucial as cybersecurity threats and related challenges extend beyond individual Member States. Fragmented national solutions have proven insufficient to achieve market-wide trust and coordination. A revised EU legal framework is required to remove barriers, ensure consistent implementation, and support Member States in an increasingly complex regulatory and threat environment.

### 3.3. Subsidiarity: Added value of EU action

Action at the European level can deliver substantial added value by ensuring coherence, effectiveness, and operational efficiency across Member States. A revision of the CSA would enhance the ability to address cybersecurity threats through harmonised cybersecurity certification schemes by making the framework more effective and efficient, simplifying compliance for entities, and clarifying role of the relevant actors in the process. Addressing the fragmentation on the internal market would also contribute to reduction of administrative burden for businesses. Finally, the newly introduce maintenance mechanism will ensure that schemes will remain future- and cyber- proof.

A revision of the CSA would further streamline compliance with various horizontal and sectoral cybersecurity-relevant legislation. This simplification would aim to reduce compliance costs and legal uncertainty for affected entities, facilitating and improving the rate of compliance with cybersecurity requirements, and help to level the playing field on approaches to supervision and compliance checks across Member States.

In relation to ICT supply chain security, only intervention at the EU level will ensure the same level of security in the Union and necessary harmonisation of approaches. EU action would benefit from interplay with the future MFF programmes, as they were proposed, by enabling an EU-wide restrictions of high-risk suppliers identified under EU law as well as with synergy with economic security framework. On a sectorial level, the intervention will be in synergy with the upcoming CAIDA, which will complement the CSA, by introducing a framework that will ensure that the EU cloud industry remains competitive and can serve the needs stemming from highly critical use cases. Moreover, the intervention will also be leveraged by the upcoming DNA, aiming to improve access to secure, fast, and reliable connectivity for the transition towards cloud-based infrastructure and Artificial Intelligence. They will together address cybersecurity and competitiveness failures in the cloud market.

Reinforcing ENISA's mandate would enable it to act as a single point of expertise for cybersecurity at Union level. This would strengthen its contributions to policy implementation and support to Member States, by providing an overview of the uptake and impact of cybersecurity measures, as well as identifying existing challenges across the whole internal market. It would also enhance capacity building, operational coordination, and the development and implementation of certification schemes.

In conclusion, action at the EU level would offer clear added value by supporting harmonisation, legal clarity and coordinated responses to cybersecurity challenges. A comprehensive analysis is needed to determine the most appropriate level and form of intervention, including whether EU action would lead to better outcomes than Member State solutions alone.

## 4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

### 4.1. General objectives

Based on the main problems identified in section 2.1, and in line with the EU's cybersecurity strategy, the main objectives of the intervention should be to **increase cybersecurity capabilities and resilience and prevent fragmentation across the single market by:**

- contributing to strengthening the Union's cybersecurity governance and helping to ensure that relevant institutions, authorities and other stakeholders are better prepared to prevent, detect, and respond to cybersecurity threats in a coordinated and effective manner.
- supporting the development, implementation and uptake of common Union cybersecurity instruments, such as certification schemes and providing harmonised frameworks that build trust and interoperability across Member States.

These general objectives respond to the key challenges identified in the problem definition. They reflect the overarching policy aim of strengthening cybersecurity governance in the Union and supporting the development of a secure, resilient and competitive sdgital single market.

### 4.2. Specific objectives

To help achieve the general objectives listed above and based on the problem drivers identified in section 2.2, this intervention pursues the following specific objectives:

*To address the misalignment between the Union cybersecurity policy framework and stakeholders' needs:*

- ***Specific Objective (SPO) 1: Create the capacity to effectively implement Union cybersecurity policies and continuous operational cooperation enabling more structured cooperation between Member States.***
- ***SPO2: Develop and implement means and mechanisms to effectively support and address the needs of Member States, industry and other stakeholders.***

*To address the limited uptake and effectiveness of the ECCF:*

- ***SPO3: Create the prerequisites for faster delivery of cybersecurity certification schemes driven by market needs by broadening the scope of the ECCF, ensuring effective maintenance and agile procedures and increasing transparency.***

*To address the fragmented compliance landscape and complexity of horizontal and sectoral frameworks:*

- ***SPO4: Create mechanisms and conditions to facilitate compliance with cybersecurity requirements, thereby making their implementation more coherent and effective.***

*To address cybersecurity risks in the supply chain:*

- ***SPO5: De-risk critical ICT supply chains from entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers) and reduce critical dependencies by developing a coherent and effective framework at EU level to address ICT supply chain security risks.***

## 5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

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

Under the baseline scenario, no new policy intervention would be introduced, as regard the CSA and in the area of ICT supply chain security. The existing legal and policy framework established by the CSA and other EU instruments would continue to apply in its current form.

Regarding **ENISA**, the fragmentation of responsibilities across EU legislation will probably continue to impact ENISA's ability to prioritise and allocate resources effectively generating inefficiencies and limited strategic focus for the Agency.

The cyber threat landscape, as described in *Section 2.5*, is likely to evolve and get more complex and attacks more sophisticated. Under the baseline scenario, the current mandate of ENISA remains unchanged, constrained in its ability to scale up its activities to match the speed of these developments. In particular, in accordance with the NIS2 Directive, ENISA will be supporting Member States to share information in the CSIRTs network and EU-CyCLONe, as a secretariat of the networks but a clear task, adequate tools or a stable resourcing to effectively support and bring significant added value to the operational cooperation, including situational awareness will most probably stay **fragmented along national lines**. In addition, after Brexit, the EU is not part of the main intelligence network (the 5 eyes agreement between the US, CAN, UK, NZ and AU). Without strong cooperation for Union situational awareness, EU may be further sideways at the global level, as considered not to be interesting partner. This could further deepen fragmentation and inequalities among Member States, with the most cybersecurity matured ones to deepen cooperation with the global partners rather than sharing with other Member States. Similarly, for the **vulnerability records and management system,** without changes to ENISA's mandate (currently not a task of the agency), the EU would continue relying on the Common Vulnerabilities and Exposure (CVE) services, which is currently run by a US association – MITRE – dependent on the US government funding. In the baseline scenario, this dependency would persist and would not allow sufficient grounds to increase ENISA' capabilities and added value in this regard.

In the area of skills, without intervention, the ECSF would not fulfil its potential as a reference framework to the skills and competencies recognition, as ENISA has no task to develop skills attestation schemes based on the ECSF. Individual certifications recognised on the market would remain with a few non-European private players and prove expensive for individuals to obtain. Alternatively, it could also lead to Member States developing their own schemes limiting skills portability in the Single Market.

Finally, in the baseline scenario, the Commission will continue to lack substantial technical support and expertise in European and international standards development activities to facilitate the implementation of the CRA, the ECCF as well as international efforts to promote the technical alignment with main international partners, such as the US. Current ENISA's mandate does not foresee the agency role in the standards development. Standardisation development activities would continue to be supported by Member States and industry, but it could also lead to the EU needing to rely on work done by third countries weakening its technological leadership and values.

For the **ECCF**'s under the baseline scenario, the slow development and adoption of schemes under the ECCF, including the average time of developing schemes (4 to 4.5 years – *see Annex 12*) is likely to persist, coupled with inefficient procedures as noted in *Section 2.1.2*. The lack of a robust scheme maintenance mechanism (not part of the current ECCF) will persist, leading to the risk of adopted schemes to become quickly outdated. These shortcomings of the ECCF will likely undermine the request for and adoption of new schemes Draft schemes such as EUCS and EU5G will continue being blocked due to lack of measures to address non-technical risks. Regarding the schemes on Managed Security Services (MSS) European ID Wallet (EUID), while their development is driven by existing legislative frameworks, implementation issues could arise especially for the assurance level high in the absence of measures to tackle non-

technical risks. While it is likely that the EUCC will enable businesses to benefit from a presumption of conformity with the CRA, conformity assessment bodies (CABs) will continue to be subject to different governance regimes. This inaction is likely to increase **regulatory fragmentation**, as at **national level,** Member States will continue to develop their own national certification schemes leading to substantial compliance costs on cross-border operations, particularly affecting SMEs that have less resources to deal with market fragmentation. Currently at least four Member States have schemes in place on cloud security[117]. The persistence of non-harmonised approaches will likely further erode trust in certification as reliable assurance mechanism and limit the potential of the Digital Single Market.

In the baseline scenario, the divergence of national approaches to cybersecurity risk-management frameworks in transposition of the **NIS2 Directive** would persist. The NIS2 Directive will continue providing for minimum harmonisation in relation to empowerments for further specifying cybersecurity risks management measures, allowing for national gold-plating. Furthermore, certain unclarities surrounding the scope and definitions in the NIS2 Directive will remain (*Section 2.2.7*). Moreover, other than for the digital service providers where ENISA holds a registry, there would still be no EU level overview of all the other entities in the scope of NIS2. It would therefore be more difficult to detect potential compliance issues when Member States would not have a cross-border visibility of issues encountered across the internal market.

In relation to **ICT supply chain security**, the baseline scenario would likely entail a continuation of the growing dependency on third-country suppliers, including high-risk suppliers in sectors and for services such as telecommunications and digital infrastructure. Under the baseline scenario, the EU and Member States could carry out one or several coordinated security risk assessments of specific critical supply chains under the NIS2 Directive and develop a non-binding set of recommending measures to mitigate those risks. The non-binding nature of those recommendations would likely result in fragmented implementation among Member States.

In addition, there are only limited possibilities to exclude high-risk suppliers from the funding programmes (such as those under the current framework of Horizon Europe[118] and DEP[119]) The proposed provision under the new Multiannual Financial Framework on high risk suppliers, even if adopted as proposed, cannot effectively restrict the participation of high risk suppliers in EU fundings if there would be is no EU mechanism to identify those high risks suppliers.

At **the global level**, international partners are working towards strengthening supply chain security, with the UK and Canada providing for legal safeguards to security of the telecommunication infrastructure, including from high-risk suppliers, the US and Australia having eve broader approach and G7 discussing the IoT supply chain security. In baseline scenario, the EU will not be able to meaningfully influence those discussions.

---

[117] ENISA, *Cybersecurity assessments*, 2024, available at: https://www.enisa.europa.eu/publications/cybersecurity-market-assessments
[118] Article 22(5).
[119] Article 12(5).

### 5.2. Description of the policy options

This report analyses **four areas of intervention, each with a set of policy options** considered in view of the specific objectives to be achieved as set out in Section 4.2 above: (1) ENISA mandate *(also part of the current CSA);* (2) ECCF *(also part of the current CSA);* (3) targeted amendments notably concerning the NIS2 Directive and aiming at simplification, but also interlinked with ENISA mandate and ECCF; (4) ICT supply chain security, which is also relevant both for NIS2 ecosystem and for ECCF. Each of these sets of options are intervention areas on their own, while at the same time interlinked and relevant to each other. Within each set, the options considered range from those involving the least intervention at the EU level and therefore closer to the baseline scenario (a soft law and non-legislative instruments approach) through a lighter option that could involve minimum legislative interventions, up to the most interventionist action proposing comprehensive regulatory intervention. Each intervention area on its own could have certain expected impact, yet various combinations with various policy options from other intervention areas are in fact determinant to impacts to be assessed as per the problems and problem drivers identified. The possible combinations of options that reinforce the effects or are complementary are presented in section 5.5 below. For better illustration of measures included in all option presented below, see *Annex 13*.

#### 5.2.1 Options to address the misalignment of the Union cybersecurity policy framework and stakeholders' needs in an increasingly hostile environment

***Option A.1: Clarifying ENISA's mandate and providing for prioritisation***

This option would ensure a clear and **stable framework for the tasks of ENISA by incorporating the tasks set out by other pieces of legislation**, such as the NIS 2 Directive, the CRA, the CSoA, DORA and NCCS. It would not change the structure of the mandate. The intervention would also ensure for synergies with the ECCC by providing the Centre with the necessary information about the cybersecurity trends, especially in relation to emerging technologies and providing for an observer status for the ECCC in the Management Board of ENISA. ENISA's tasks in the area of research and innovation would be removed.

To ensure higher efficiency in terms of the use of resources, this option proposes setting a clear **prioritisation** of the Agency's tasks, with a greater focus on support for policy implementation, including increasing the issuance of sector specific guidelines. Under this option, ENISA would receive further tasks to support operational cooperation, making ENISA not only a secretariat of two operational networks (CSIRTs network and EU CyCLONe), but also strengthening its role in facilitating **operational cooperation between Member States within those networks**, in cases of cross-border incidents., for example by providing coordination in relation to a joint incident response. The Agency's resourcing mechanisms would be changed by adjusting the current budget to reflect the additional tasks from other legislative acts and include the cost of human resources needed within ENISA's establishment plan. It would limit ad hoc contribution agreements, limiting administrative costs related to them.

***Option A.2: Reforming of ENISA's mandate***

This option would repeal and replace the CSA, providing an overhaul of the Agency mandate.

The mandate would organise ENISA's tasks along three main pillars bringing the possibility to create synergies between those tasks and clarifying the priorities for the Agency: **(i)** supporting **implementation of general and sector-specific cybersecurity policies and legislation,** such as NIS 2, DORA, Action Plan for the cybersecurity of hospitals and healthcare providers, NCCS etc.; **(ii) operational support,** including in activities such as the EU Cybersecurity Reserve under the CSoA and enhancing support for Member States to contribute to better situational awareness, and **(iii) cybersecurity certification, standardisation** (including on CRA implementation) **and attestation for cybersecurity skills**.

On **resourcing,** in this option, ENISA will not only rely on the Administrative Heading of the MFF to ensure the sustainable growth of the Agency. ENISA's activities could be supported by national liaison officers delegated by each Member State, in particular to reinforce operation cooperation activities ENISA would be able toc collect fees from activities related to cybersecurity certification and skills authorisation. In particular, the fees could cover the development and maintenance of attestation schemes and the process of verification of providers that apply to be authorised to issue EU skills attestations or to additionally support maintenance work related to European certification schemes (additionally to ENISA FTEs provided).

This option, as option A.1, would also provide for an observer status for the ECCC in the Management Board of ENISA.

**Under the first pillar**, this option would strengthen ENISA's role and added value in actively supporting the implementation of cybersecurity legislation and policy. More specifically, ENISA would become a European equivalent to MITRE, allowing it to act as Union's root authority within international vulnerability identification systems, handle more effectively methodologies in this respect, enrich disclosed vulnerability records and create more synergies with related responsibilities of ENISA such as the managing of the CRA single reporting platform. The new mandate, in combination with related targeted NIS2 amendments (*link to options C2*), would also allow for more support of ENISA to Member States' supervision of compliance and mutual assistance, notably when cross-border aspects and 'multi-country entities'[120] are concerned, and a better overview of cybersecurity maturity of the key sectors of the Union's economy and society. It would also further specify the role of ENISA in capacity building efforts, especially concerning sectorial support (such as the Health Action Plan). ENISA's international activities would be linked to the Union's priorities to bring a clear added value to the Union's cyber posture.

**Under the second pillar**, ENISA would develop the necessary capabilities to establish shared EU situational awareness in cooperation with Member States within the Union level networks (i.e. EU CyCLONe and CSIRT network) as well as with relevant Union entities such as EUROPOL. ENISA would develop a single repository of verified reliable cyber threat intelligence that would enhance ENISA's operational capabilities for supporting Member States in handling cyber threats and incidents. Furthermore, ENISA's supporting role in the operation of EU networks (EU-CyCLONe and CSIRTs network)

[120] These are in particular entities which provide services in more than one Member State, or provide services in one or more Member States and their network and information systems are located in one or more other Member States.

would be strengthened by allowing ENISA to analyse relevant information on threats and cybersecurity events gathered from Member States and from other sources and producing Union wide early warnings regarding actual or potential incidents or cyber threats of potential cross-border natures to be shared through these networks ENISA would also become a member of the CSIRTs network. In addition, ENISA would also support incident response activities, i.e. the EU Cybersecurity Reserve under the CSoA.

**Under the third pillar,** this option would entrust ENISA, as a scheme manager *(see options B1, B2 and B3)* with the development and implementation of the certification schemes, upon request from the Commission. ENISA would develop the necessary capacity to support the development of cybersecurity standards for the industry (e.g. for the implementation of CRA or NIS 2 Directive) and the adoption procedure of technical specifications supporting the development of the ECCF schemes. This would enable ENISA to leverage its expertise to support Member States in building certification capacity.

Finally, under this option ENISA would develop and maintain European individual cybersecurity skills attestations schemes, hereby supporting the recognition and portability of skills across Member States.

***Option A.3: Reforming of ENISA's mandate with a strong operational support focus***

This option would build upon option A.2. IIn addition, ENISA would develop capabilities to support NIS 2 Directive entities directly in responding to and recovering from the cybersecurity incident upon Member State's request. The Agency would be equipped with an operational team, available 24/7, consisting of ENISA's staff and reinforced by national liaison officers and service providers. In addition, ENISA would also act as an EU-level cybersecurity umbrella, providing technical advice to entities implementing NIS 2 Directive and serving as a centre for information. These would entail a notable shift of ENISA's priorities and tasks, with a clear focus on the support for operational cooperation which would require more operational-driven skills and profiles. The approach to the resourcing of the Agency would be the same as defined in option A.2, adding the possibility of additional seconded national experts to be sent by Member States.

### 5.2.2 Options for the European Cybersecurity Certification Framework

***Option B.1: Clarifying the ECCF's scope, elements and objectives and introducinga maintenance mechanism***

This option will provide **for a new maintenance mechanism of the schemes**, after their adoption, to be done by ENISA. It would leverage the new tasks of ENISA in standardisation under options A.2 and A.3. To this aim, it would:

- formalise and detail the procedure for the preparation, update and endorsement of technical specifications (new for ENISA under options A.2 and A.3) and guidelines, to support the harmonised operation of the schemes;
- provide for the mechanism to consult and liaise with relevant stakeholders, including for the purpose of receiving technical contributions, and exchange of information related to identify where updates to the schemes are needed.

This option would also provide clarification of the scope of the ECCF in terms of risks covered, clarifying covering **only technical risks factors** (*this option could be complemented by option D.3, establishing the framework to cover non-technical risk factors and would be inefficient if not combined. The combination of those options does not mean that an entity would need to be certified, not be considered high-risk, see further*).

Finally, targeted changes to the ECCF would be introduced to improve its synergy with the CRA and NLF, and in particular as regards security objectives for product security and the requirements on conformity assessment bodies. This would allow that the schemes such as the EUCC and the future EUCS can better facilitate the implementation of the CRA through presumption of conformity.

Under this option, certification as such remains voluntary as is in the current CSA [121].

***Option B.2: Reforming the ECCF by revising its procedures and extending the scope to facilitate simplification of regulatory compliance***

In this option, the CSA would be repealed and replaced by a new regulation. In addition to option B.1, a complete **revision of the procedure** related to request, development and adoption of schemes would be introduced to improve accountability and efficiency through:

- New **Strategic planning** with streamlined procedure, to be regularly updated and published on a new Commission website together with overview of the ongoing work and allowing interactions with stakeholders;
- **Detailed Commission requests for schemes**, which will be informed by market studies to be performed by ENISA, setting out clear scope of the future scheme, **development plan and strict timeline** (expected between 2-2.5 years) for delivery of the candidate scheme and its preparation for adoption by the Commission;
- The development of the candidate scheme will be fully in hands of ENISA (i.e. **role as a scheme manager** - *links to options A.2 and A.3*), advised by the ECCG and ad hoc working group (AHWG), with a support of the Commission guarding the integrity of the process and deciding on the adoption of the scheme within a clearly defined timeframe;
- **Strengthened stakeholder engagement** across various stages (planning, request, adoption) of the development, streamlined through **public consultation**; and
- **Clarification of the roles of relevant stakeholders** (EC, ECCG, AHWG and ENISA) in the process resulting in more accountability and ownership in the procedure.

[121] The current procedure for their possible mandating from the current version of the CSA (Article 56(3)) is retained. Such a possibility is currently reflected in the CRA (Article 8) and NIS 2 Directive (Article 24), and could be further reflected in other Union legal acts in the future.

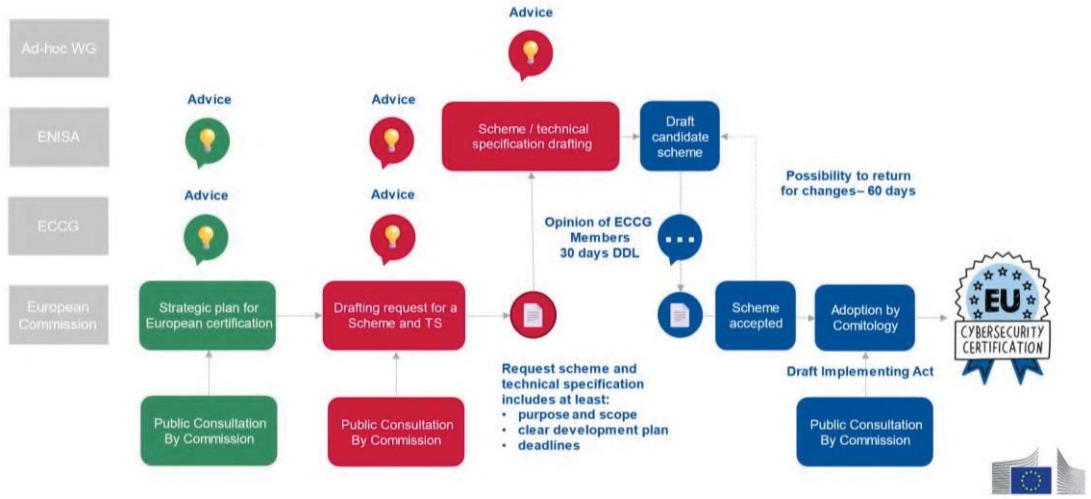



*Figure 3: ECCF revised procedure*

This option would build on the maintenance procedure envisaged in option B.1, by introducing a limited possibility to develop minor updates[122] for certification schemes in the maintenance phase without requiring comitology.

The revision would seek to solidify a **synergy between the certification framework and other recent cybersecurity legislation**, by adding, in addition to the alignment with CRA under B1, alignment with requirements related to organisational security (NIS 2 Directive), and support compliance with the relevant legislation. To this end, this option would extend the scope of the ECCF to cater for the **certification of organisation-wide security posture** (i.e. certification of entities) allowing for demonstrating compliance with the cybersecurity requirements laid down by the NIS 2 Directive – links with option C2 and C3).

As in option B1, also under this option certification remains voluntary, unless explicitly provided otherwise in other acts for specific use cases.

***Option B.3: Reforming the ECCF as envisaged under option B.2 and introduce mandatory certification for cyber posture***

This option would build on option B.2, but aims at further strengthening the impact of the framework by introducing **mandatory certification of essential entities considering specific risk scenarios**, instead of relying solely on voluntary certification of entities.

Specifically, the revision of the CSA would provide legal basis for the Commission to **mandate the future certification of organisation-wide cyber posture for the targeted scope of all or certain essential entities** listed in Annex I of the NIS2 Directive. Such designated essential entities, due to their critical role for cyber resilience of the economy and society would be mandated to demonstrate that they meet adequate organisational

[122] Updates of technical specifications developed by ENISA to deliver security requirements of the cybersecurity certification schemes and corresponding references in the text of implementing acts establishing the schemes.

cybersecurity measures (i.e. requirements of the NIS2 Directive) through cybersecurity certification (*links to option C2 and C3 enhancing efficiency of the options*). This possibility would complement existing empowerments that allow mandating certification in the context of NIS 2 Directive, CRA or the European Digital Identity Regulation (mandating certification of European ID Wallets).

To facilitate this process, next to the actual establishment of the scheme foreseen under B2, this option would include an empowerment (implementing act) for the Commission to identify and adjust the list of sectors (amongst those listed in Annex I) where the scheme would be mandated following an **impact assessment considering technical risk factors as well as the market impact** (proportionality and necessity of the intervention). The assessment of the potential market impacts and of the cybersecurity risks (impact assessment) would be conducted by the Commission in consultation with ENISA and all relevant stakeholders, including the ECCG and the NIS2 Cooperation Group.

What is more, as in options B1 and B2, certification under this option would cover only **technical risk factors (**non-technical aspects outside of the scope of the framework – links with option D.3, without which this option could be inefficient).

### 5.2.3 Options for simplification

***Option C.1: Taking a soft law and non-legislative instruments approach, including the use of existing empowerments (adoption of implementing acts under Article 21(5) and Article 23(11) of the NIS 2 Directive)***

This option foresees the adoption of implementing acts under the existing empowerments of the NIS2 Directive to ensure a higher degree of harmonisation of the cybersecurity risk-management measures, incident reporting thresholds, as well as information, formats and procedures of notifications. The implementing acts regarding the cybersecurity risk-management measures and incident reporting thresholds would be horizontal and could be supplemented by sectoral specifications (also by virtue of an implementing act under existing empowerments) where necessary, such as for providers of public electronic communications networks or of publicly available electronic communications services. While the empowerment exists under the baseline scenario, there is no obligation for the Commission to propose such implementing acts.

Moreover, the Commission would adopt guidelines:

- on the application of supply chain security requirements that entities in scope of the NIS2 Directive pass on to their suppliers, in order to ensure legal certainty and prevent the undue passing on of obligations on entities not in scope of the NIS2 Directive […];
- clarifying the scope of the NIS2 Directive, including definitions;
- to streamline ransomware reporting to inform policies and assess the effectiveness of measures taken against ransomware attacks.

***Option C.2: Targeted intervention – further simplification of compliance with relevant Union cybersecurity legislative framework***

Option C.2 involves limited intervention through changes in the CSA and the NIS2 Directive aiming at simplifying specific aspects of the cybersecurity framework and

adoption of the set of guidelines to enhance legal certainty and harmonised implementation.

This option would introduce the possibility of using organisational cybersecurity certification schemes developed within the ECCF[123] (*cannot materialise without options B.2 and B.*3), which would enable entities and suppliers to demonstrate compliance with the NIS2 Directive and other Union legal acts where a scheme covers the respective legal requirements. This could improve the coherent implementation of cybersecurity requirements of Union legal acts to level the playing field across Member States.[124] Moreover, targeted amendments to the NIS2 Directive and other relevant Union legal acts would ensure that holding valid certificates enable to demonstrate conformity and to confer presumption of conformity with the respective legal acts. It would open the possibility for mutual recognition of compliance audits amongst Member States.

To further facilitate compliance with cybersecurity risk-management measures for multi-country entities subject to supervision by competent authorities from several Member States, ENISA would have a new role supporting Member States in the supervision of these entities and facilitate mutual assistance and would also have for this purpose a better overview of entities under NIS2 scope and incidents reported across the internal market (*see option A.2*).

This option would also provide for a series of targeted amendments to the NIS 2 Directive:

- clarify the scope and definitions (e.g. a targeted amendment to clarify that the scope covers only entities for which generation of electricity is an essential part of their general activity);
- reduce the scope as regards micro- and small-sized DNS service providers;
- introduce maximum harmonisation for implementing acts under Articles 21(5) – *specifying the cybersecurity risk-management measures* – and 23(11) – *specifying the significant incidents* – to facilitate compliance for entities and supervision for authorities.
- introduce a new category of small mid-caps, in line with the 2025 Commission Recommendation on the definition of small mid-cap enterprises.[125] Entities qualifying as small mid-caps would be designated as important entities, reducing their burden of compliance and the burden of supervision for competent authorities;
- ensure a harmonised collection of data on ransomware attacks by amending Article 23 of the NIS2 Directive on reporting obligations;

As in Option C.1, this option would further foresee the adoption of guidelines on the application of supply chain security requirements.

***Option C.3: Harmonising cybersecurity-related measures set out in Union legislation***

[123] Possibility for certifying the level of cybersecurity risk-management measures taken by an entity.
[124] The avenues for achieving presumption of compliance have been extensively researched in relation to the CRA, in force since December 2024, establishing product-level security baseline. The CSoA mandates certification of managed security services to become part of the EU Cybersecurity Reserve.
[125] C(2025) 3500 final.

This option would build on the solutions encompassed by option C.2. This option would remove all cybersecurity risk-management measures or empowerments in relation to the cybersecurity risk-management measures from sectorial legislation, DORA, NCCS, PART-IS. Instead, the NIS2 Directive ecosystem would be amended to provide for streamlined requirements for all types of entities, ensuring in that way deeper harmonisation. More specifically, the NIS2 ecosystem would ensure direct application of the cybersecurity requirements, which could be achieved either through turning NIS2 in a regulation, or, while still remaining a directive, allowing for maximum harmonisation of empowerments for implementing acts, which can also be sector-specific, complemented by the needed supportive standards or technical specifications. The NIS2 ecosystem can also be adapted to adjust to a wider circle of cooperation among authorities and information sharing, while ensuring secure and automatised channels of communication and reporting. As necessary, the NIS2 scope can also be adjusted to cater for specific sectorial coverage.

### 5.2.4 Options for ICT supply chain security

***Option D.1: Taking a soft law approach to address cybersecurity risks for ICT supply chains***

This option would not provide for regulatory intervention at EU level. Instead, the Commission would increase the number of coordinated risk assessments and voluntary toolboxes, It would provide for the priority list of areas where the risk assessments and recommendations to apply measures will be proposed with the immediate follow-up.

Based on this priority list, the Commission would identify the supply chains to be assessed by the NIS Cooperation Group and to develop non-binding set of recommending measures to mitigate them, as in the baseline scenario. The difference with the baseline scenario, is that the Commission will commit itself to proceed with announced risk assessments and measures. The Commission would further support the implementation of these toolboxes in relation to specific critical supply chains, by raising awareness of the non-technical risk factors and promoting use of trusted suppliers.

Finally, the Commission, as possible in the baseline scenario, would continue introducing security requirements on an ad hoc basis to address rising concerns related to ICT supply chains in public procurement tenders or auctions.

***Option D.2: Ad hoc regulatory intervention codifying the 5G Toolbox***

This option would codify the 5G Toolbox measures. It would introduce an obligation for Member States to ensure that components from high-risk suppliers are not used in key assets of the network as identified by the EU coordinated risk assessment on 5G security[126]. Rather than specifying specific deadlines at EU level, this option would oblige Member States to conduct risk assessments of suppliers, design mitigation strategies, and implement measures to restrict use of equipment as identified in the EU coordinated risk assessment (i.e. core network, network function virtualisation

[126] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

management and orchestration (MANO), and RAN) from high-risk suppliers in 5G networks.

In addition, Member States would require operators to provide detailed and up-to-date information about their plans for the sourcing of 5G equipment and for the involvement of third-party suppliers.

***Option D.3: Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks***

This option would establish a **horizontal, technology and sector-neutral regulatory framework** to address in particular **non-technical cybersecurity risks, in ICT supply chains.** It would not include directly applicable measures on any ICT supply chains.

Instead, the framework would include empowerments allowing measures to be applied only in specific contexts, and only after several preparatory steps have been completed. This to ensure that any measure triggered is necessary and proportionate to address the security risks. Each application of the framework to a particular ICT supply chain would be based on a dedicated risk and accompanied by an assessment of economic impacts of the measures proposed — including analysis of factors such as the availability of alternative suppliers and the potential impact on industry. The work would involve the participation of relevant stakeholders, including Member States, as described below. The framework would contain the following steps:

- **A dedicated EU coordinated security risk assessment** for each identified ICT supply chain, based on the existing framework set out in the NIS2 Directive. The risk assessment will be carried out using the common methodology that was elaborated with Member States in the NIS Cooperation Group assessing risks related to countries posing cybersecurity concerns and high-risk suppliers as well as dependencies. This step also includes a comprehensive **economic analysis** addressing among others, economic feasibility, available alternatives in the market, impact on economic operators including SMEs, and the lifecycle of the specific products, which would be factored in when determining appropriate mitigating measures such as phase-out periods for assets coming from high-risk suppliers or transition periods to remove security risk dependencies;
- **Development of mitigation measures** will be based on the results of the EU coordinated security risk assessments and the economic analysis, and a **list of key assets will be established. In addition, targeted and proportionate mitigation measures to be applied for the identified key assets, will be agreed with Member States**. Such mitigation measures could range from restrictions such as imposition of data localisation requirements or requirements for diversification of providers to reduce over-reliance, restrictions in terms of ownership and control, bans in public procurement or prohibition to use products from certain suppliers or from suppliers from certain countries posing cybersecurity concerns, where transition periods for phasing out hardware and software from such suppliers in these key assets would also be established;
- The Commission would then prepare implementing acts establishing the necessary **mitigation measures,** which would be adopted following comitology procedure (i.e. examination procedure). The implementing acts will be **accompanied by a thorough assessment of the potential economic impact of the envisaged measures in accordance with the Better Regulation Toolbox.**

The chart below illustrates how the roll-out of option D.3 would work in practice.

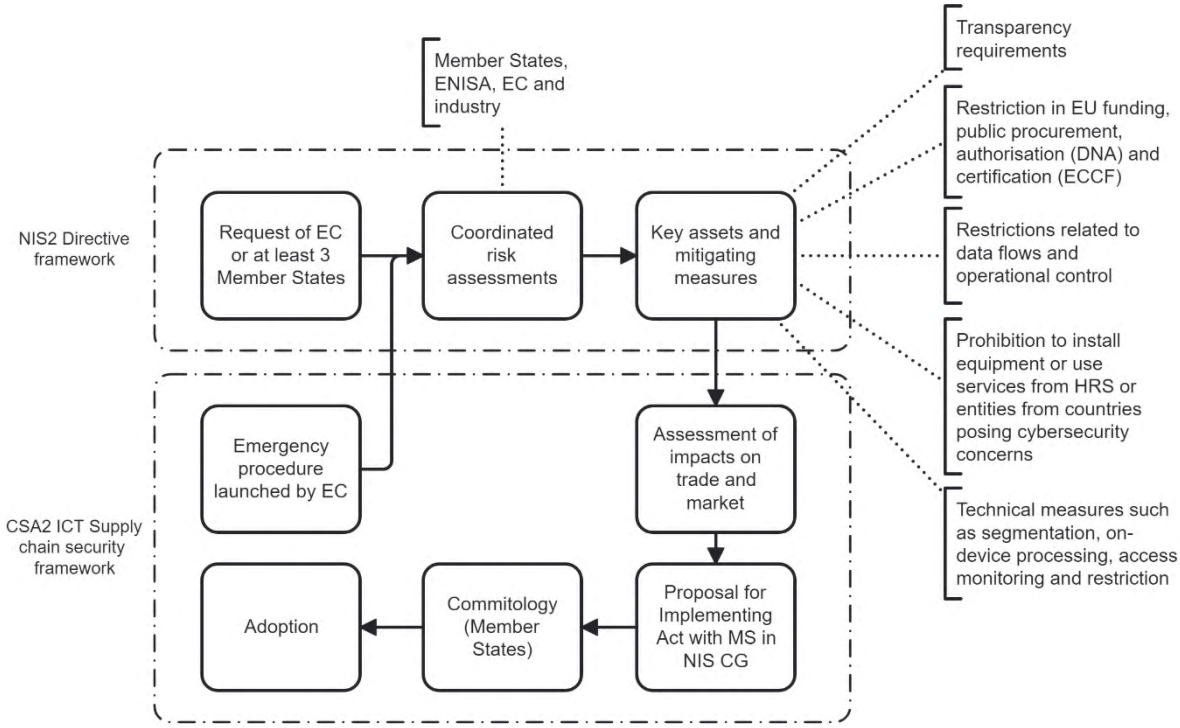



*Figure 4: Roll-out of option D.3*

Under this option, the first concrete application of the framework would be in relation to telecommunications, including 5G networks. The EU coordinated risk assessment of the cybersecurity of 5G networks has already been carried out in 2019[127] and the next steps would therefore be to establish by law which assets of 5G networks are considered as key assets, as well as designate of countries posing cybersecurity concerns, high-risk suppliers (through empowerment).

The potential ICT supply chains to be assessed – after 5G networks – could be the following: scanning equipment, submarine cables, and electricity supply chain. For each of these ICT supply chains, dedicated EU coordinated security risk assessments have started or are about to start. Additional EU coordinated security risk assessments could be initiated by the Commission and the Member States. Before proposing an implementing act to identify key assets and appropriate mitigation measures, the impacts of the proposed measures, including economic impacts will be assessed.

In addition, the framework would provide a basis for other relevant EU legislation to address non-technical cybersecurity risks, in relation to ICT supply chains in the internal market, including for example in relation to:

- the ECCF to exclude from certification ICT products, services or processes provided by entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk-suppliers) in relation to key ICT assets or limit the eligibility for certification under specific assurance levels;

[127] NIS Cooperation Group, EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

- the European individual cybersecurity skills attestations to exclude entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk-suppliers) from becoming authorised providers of cybersecurity skills attestations;
- the revised public procurement directives to restrict participation in public procurement procedures of entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk-suppliers);
- the proposed MFF framework[128] and the Financial Regulation[129], by providing for the legal basis to restrict participation of entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk-suppliers) in EU funding programmes and instruments.

Under this option, in order to ensure a coherent enforcement by the Member States of the restrictions on high-risk suppliers or entities originating or controlled from countries posing cybersecurity concerns adopted at EU-level, the Commission will assist Member States with unravelling corporate ownership structures and subsidiaries of those entities building on existing registries and mechanisms**.**

### 5.3. Options discarded at an early stage

In addition to the policy options presented in section 5.2, in the analysis of potential policy options that could address the problems described in section 2 and reach the general and specific objectives set out in section 4, the following alternative options entailing regulatory intervention were discarded at an early stage and therefore not assessed in further detail:

- **Repealing the ECCF without equivalent substitute** was discarded as an option at an early stage. While certifications could be, in part, replaced by technical specifications (TS) developed by ENISA to address technical risk factors, such approach would not provide the necessary assurance or include various relevant security stakeholders. To illustrate the difference, TS lack a process that confirms and provides evidence, verified by a third-party conformity assessment body, that security requirements listed in TS or standard are met by a certification object. Moreover, there is a clear market demand for certification. Public consultation showed that certification is widely perceived as a tool for enhancing product and service security, with micro businesses being the most supportive (66.67% strongly agree that certification improves security).
- A **soft law and non-legislative instruments approach as regards ECCF** was initially considered due to minimal financial burdens for stakeholders. Under this option, the Commission would issue **guidance on good practices and procedures**

[128] See for example a proposal for the European Competitiveness Fund regulation, COM(2025) 555 final.
[129] European Commission, Financial Regulation applicable to the general budget of the Union (recast), September 2024, https://op.europa.eu/en/publication-detail/-/publication/990fe2a6-8f52-11ef-a130-01aa75ed71a1/language-en. Article 136 allows, for the protection of security or public order, the authorising officer responsible to set up specific conditions applicable to the award procedures and the legal commitments.

with the aim of improving efficiency of the development and implementation of the cybersecurity certification schemes. This guidance could suggest ways of better organising the procedures, but would not be able to change the ones in place, or introduce new ones. It could also provide limited clarifications on interpretation of the scoping and harmonisation effect of the ECCF. What is important, this option would not resolve an issue of the maintenance mechanism of the schemes, as no formal procedure could be introduced. This option was discarded at an early stage because of its negligible impact on identified problem drivers.

- An option to adopt a **Commission Recommendation** on security of 5G networks was discarded at an early stage. This option would entail recommending Member States to implement the 5G Toolbox with regard to the restriction or exclusion of the high-risk suppliers from providing **critical and highly sensitive assets as identified in the EU coordinated risk assessment of the cybersecurity of 5G networks**[130], namely the core network, network function virtualisation management and orchestration, and the RAN. This option was discarded at an early stage as it was considered that it would not have a significant impact beyond the baseline scenario and would not lead to significant limitation to the fragmented implementation.
- An option to propose **an intervention based on a comprehensive ICT supply chain security framework that would apply directly to key assets**, was discarded at the early stage. This option would have built upon option D.3 but would expand the list of key assets/technologies in highly critical and other critical sectors, as provided in Annexes I and II of the NIS2 Directive, directly in the act (without further empowerments). Consequently, in this option, an obligation not to use assets provided by entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers), would be imposed to specified entities. This option was discarded at the early stage as the absence of a relevant data to identify the key assets and proportional and necessary measures to address them, could lead to disproportionate restrictions with unknown impact on the relevant market.
- Another option that was discarded at an early stage was to **introduce a comprehensive and horizontal framework to address ICT supply chains cybersecurity risks in the NIS2 Directive**. This is in fact a variation of the discarded option above, using a different legislative vehicle (a Directive instead of a Regulation). In addition to the reasoning for discarding the option above, in this option, introducing the framework in a directive would likely result in fragmented implementation across Member States.

### 5.4. Complementary initiatives

The options analysed in this Impact Assessment Report should be considered to be complementarity to the measures foreseen in the Digital Omnibus, part of the Digital package announced in the Commission Work Programme 2025. The Digital Omnibus will not include substantive amendments to NIS 2 Directive scope or other provisions. In the Digital Omnibus, a Union-level single-entry point for cybersecurity relevant incident and data breach reporting obligations under multiple Union legal acts (e.g., NIS 2, GDPR, the Network Code on Cybersecurity, Part-IS) would be proposed. Once entities

[130] Ibid.

report the information required by the respective legal acts via the single-entry point, the reports would reach the relevant recipients as required by the respective Union legal acts and their national transpositions (such as CSIRTs or national authorities). The single-entry point would be established and maintained by ENISA. The Digital Omnibus would mandate the use of the Union-level single-entry point by all entities covered by the incident reporting obligations in those legal acts.

The measures under the Digital Omnibus would also aim to reduce the compliance burden on entities regarding incident reporting obligations stemming from various legal acts and their national implementations. The impacts, costs (with the exception of the costs of ENISA's staff and costs needed to develop and maintain the single-entry point that is part of this Report) and benefits related to the single-entry point are assessed within the proposed Digital Omnibus and are not taken into account in the assessment of impacts for the CSA.

### 5.5. Possible combinations of options

There are several links between options as described above. Combination of certain options will reinforce effectiveness of the options in question or ensure that options can materialise at all, namely:

- combination of B2/ B3 that propose extending the scope of the ECCF and introduce the certification of organisations with C2/C3, which would then use such certification to demonstrate compliance could generate more benefits for economic entities and national authorities as it would facilitate supervision. B3 that introduces the mandatory use of such certification for essential entities under NIS2 would not make sense without C2/C3 as it would mean to make those entities subject to two supervisory regime;
- combination of C1/C2/C3 that provide for the guidelines on the application of supply chain security requirements in the NIS 2 Directive with D1/D3 where further recommendations or obligations, respectively, regarding supply chain security are foreseen would reinforce and complement their effect;
- options B1/B2/B3 could not materialise without A2/A3 that empower ENISA to be a cybersecurity certification scheme manager and is tasked to do the maintenance of the schemes;
- options C2/C3 that provide for further facilitation of compliance with cybersecurity risk-management measures for multi-country entities subject to supervision by competent authorities from several Member States would not be possible if ENISA would not receive a new role supporting Member States in the supervision of these entities and facilitate mutual assistance under A2 and A3;
- options B1/B2/B3 that clarify that the ECCF would only tackle technical risk factors would be inefficient and would not provide added value to the baseline scenario if they are not combined with option D.3 that provides for the horizontal framework on the ICT supply chain security, addressing the issue of non-technical risk factors. As this was an important reason for blockage of the EUCS and EU5G certification schemes. Lack of solutions of option D3 could also put at risk the managed security services certification, in particular for the assurance level high. The combination with option D2, would address the issue of non-technical risk factors for the EU5G certification scheme. Option D.3 would provide that entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk

suppliers) would not be eligible to apply for the ECCF certification. The combination of options B with option D.3 does not entail that an entity would need to be certified not be considered high-risk.

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

This section outlines main impacts of the policy options. Given that different markets will be affected, economic impacts are addressed in detail (*see section 6.1)*, including impacts on compliance costs, on SMEs and impacts on trade, innovation and competitiveness. Furthermore, given the relevance to the policy options, next to economic impacts, also impacts on cyber resilience and technological sovereignty are analysed in detail (*see section 6.2*).

The following stakeholders are expected to be impacted by the different policy options:

- **Businesses** (both large and SMEs): essential and important entities covered by NIS2; suppliers of ICT products, services, processes, managed security services; businesses using ICT solutions and relying on critical infrastructure; providers of individual skills attestations.
- **Public authorities:** National cybersecurity authorities; national cybersecurity certification authorities; national accreditation authorities; ICT users.
- **Consumers and citizens** as actual and potential cybersecurity professionals, ICT users and users of public services.
- EU institutions and agencies, in particular **ENISA.**

To ensure readability of this document and provide for a concise overview, methodological background, including details of calculations for the estimates, is provided in *Annex 4*. Below, an overview of key methodological considerations is provided.

**Key methodological considerations**

To the extent possible, **specific and aggregated quantitative** estimates have been elaborated for the different sources of costs and benefits with relevant assumptions. Different methodologies have been used depending on the options and are further explained in *Annex 4*.

To complement quantitative estimates, **qualitative assessments** of impacts (costs and benefits) have been included. To compare the policy options, a scale from neutral "0" to +++ / --- has been used (with "+++" indicating the highest impact for the benefits, including cost savings, and "---" indicating the highest impact for the costs).

The cost aggregation has been done **over five years** (2028 – 2032) to have a representative assessment of impacts (e.g. some cost impacts would only intervene after couple of years) ), with the exception of the measures related to supply chain security where a **three years** transition period is foreseen for the phasing out of high-risk equipment in the area of 5G.

The costs are indicated compared to the **business-as-usual scenario** (BaU) (*see baseline in section 5.1*). Where relevant those costs are specified under each specific section.

The cost estimation per FTE across this impact assessment is based on previous evaluations, estimates from similar activities conducted in comparable EU agencies, and the CSA impact assessment, where the average cost of one FTE, adjusted for inflation, is

calculated at **EUR 128 277**[131] *(see more explanations in Annex 4).*

A more detailed overview of the **possible direct and indirect costs and benefits** for all categories of stakeholders is provided in *Annex 4*.

In terms of **benefits**, regarding the **main cost savings** (*see section 6.1.1*), they focus mainly on i) procedural efficiencies, ii) administrative cost savings, and iii) cost savings related to reducing the probability or impacts of cybersecurity incidents. Broader benefits are analysed related to SMEs (*section 6.1.2*), internal market (*section 6.1.3*), trade, innovation and competitiveness (*section 6.1.4*), and cybersecurity resilience (*section 6.2 and see hereafter*).

In terms of **costs,** the **main costs drivers** (*see section 6.1.1)* stem from i) adjustment and administrative costs; ii) substitution and transaction costs; iii) enforcement costs, iv) potential price increase. Broader costs might stem from impact on market access (*section 6.1.4*).

Given the geopolitical context and the avalanche effects cyber incidents can have on the real world (*see sub-section 1, 2.1.4.2, 2.2.1 and Annex 7*), **impacts on security, including hybrid threats, and on resilience, technological sovereignty, open strategic autonomy and security of supply** are an important benefit considered for public authorities, businesses and citizens across policy options. Given its broader implications, this aspect is also analysed in more details in *section 6.2*. Limited availability of reliable market data did not allow for granular and accurate quantitative assessments of cost savings related to the specific policy measures being assessed. The limitations are further explained in *Annex 7*. To the extent available, estimates to illustrate the costs related to cybersecurity incidents have been included in the impact assessment and summarised in this Annex. To the extent possible, aggregated quantitative estimates have been elaborated with necessary disclaimers and assumptions to evidence the impact of relevant policy options. Due to the lack of available data, it is difficult to quantify the direct causality between the measures included in the different policy options and related cost savings in terms of probability and impact of cybersecurity incidents. All measures contribute to different degrees to the general objective of mitigating risks (and related costs) of cyber incidents occurring (e.g. through faster detection) and safeguard against potential adverse cybersecurity events (e.g. faster response) of unpredictable nature.

### 6.1. Economic Impacts

This section outlines the expected economic impacts of the policy options described in *section 5.2.* Next to direct and indirect costs and cost savings, broader impacts on the internal market, on SMEs, and on trade, competitiveness and innovation are analysed.

[131] European Commission (2017). *Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA),* https://digital-strategy.ec.europa.eu/en/library/final-report-evaluation-european-union-agency-network-and-information-security-enisa.

6.1.1. *Cost impacts for businesses, public authorities, citizens*

6.1.1.1. Policy options related to ENISA (A.1 to A.3)

(a) Enforcement and compliance costs for public authorities, citizens, businesses

At the end of 2024 ENISA had 132 employees and reported a total budget of EUR 26 218 721[132] (business as usual). A detailed overview of ENISA's FTEs by activity (for the operational and corporate activities) is available in *Annex 11*.

**Option A.1** entails a targeted intervention through limited amendments to the CSA, with the objective of enhancing the role of ENISA within the evolving cybersecurity landscape. By supporting and issuing sector-specific guidelines, this option aims to enhance resource efficiency without incurring additional costs, as these tasks are already part of ENISA's existing mandate. This option also seeks to establish clear processes and mechanisms for cooperation between ENISA and the ECCC.

Overall, the estimated **costs** for **EU institutions and agencies, in particular ENISA,** in human resources and logistical support for this option are marginal, considering that ENISA already engages in coordination efforts as part of its mandate and regular work. The prioritisation and streamlining of resources would incur rather reorganisation of existing resources and would entail only marginal increase of FTEs, which would be offset by the marginal cost savings mentioned under benefits.

As for **costs for national authorities,** given that CSIRTs network and EU-CyCLONe are already institutionalised, this measure primarily involves reorganisation, with minimal impact on costs for Member States[133]. As for costs for businesses and citizens, there are none under this option.

For implementing ***Option A.2,*** ENISA requires a total of **EUR 148 118 870 additional cost over 5 years,** which is an incremental cost compared to the baseline (i.e. it does not include current ongoing activities).

This additional budget of EUR 148.12 million (M) includes **one-off costs of EUR 10.1M** and **recurring cost of 138M over 5 years (EUR 26.7M in 2028 and EUR 27.8M yearly from 2029 to 2032)**, which represent mainly adjustment costs to comply with the new regulation, broken down as follows: ca. EUR 12.2 M per year, (i.e. **EUR 61.06M** over five years) related to CVD, CTI, CRA single reporting platform maintenance, single entry point, CRA implementation, skills attestation schemes, and cyber maturity, see details below; the yearly maintenance of secure communications of EUR 1 083 250 from 2029 to 2032 (EUR 4.3M over 4 years); the annual costs of EUR 13.08 million (i.e. **EUR 65.42M over 5 years**) for additional **102 FTEs** at ENISA to deliver the additional tasks; the costs of 40 NLOs seconded to ENISA in amount of 1.44 M yearly (i.e. **EUR 7.2M over 5 years**).

---

[132] ENISA, *FINAL accounts 2024*, https://www.enisa.europa.eu/sites/default/files/2025-07/ENISA%20Final%20Annual%20Accounts%202024%20%28V1%20-%20e-signed%20%29.pdf

[133] As outlined in the NIS 2 Directive impact assessment report, Brussels, 16.12.2020 SWD(2020) 345 final

As a reminder, the cost estimation per FTE for ENISA is based on previous evaluations[134] and amounts to EUR 128 277 per year (this relates to salaries, social contributions and allowances, excludes overhead (*see Annex 4, section 2*)). A detailed breakdown of the allocation of FTEs by task and related costs on a yearly basis is provided below. The salary estimation of an NLO seconded to ENISA (paid by the Member State) is of 56 500 EUR (*see Annex 4, section 4.2*)[135].

To be noted that ENISA's FTEs and operational costs related to the certification are listed under Option B.2 and amount to between **8 (in 2028) and 14 FTEs** (from 2030 onwards). These costs are not counted under Option A.2., only under Option B.2., thus the costs under the two options are mutually exclusive. This means that **ENISA's total number of employees** would be increased from the **132 in 2024 to 288 by 2030** (considering the 40 NLOs and the 14 FTEs under Option B.2. as well as 102 FTEs under option A.2, i.e. **156 additional employees**) – **an increase of 118% compared to the baseline.** The total additional budget for ENISA under Option A.2 and Option B.2 amounts to EUR 161.3 M.

The detailed breakdown of this additional budget of EUR 148.12 million for Option A.2 is provided below.

- Firstly, the administration and operation of the **EU Cybersecurity Reserve** require around **10 FTEs**[136], resulting in a total recurring cost of **EUR 1 282 770** per year (i.e. EUR 6.4M over 5 years); to be complemented by procured services from trusted managed security service providers[137].
- Secondly, the work on the **European vulnerability database** and relating actions stemming for this including involvement and representation at global level, enrichment of the database, etc. For this action (further details *section 5.2*), ENISA would require 15 **additional FTEs**, which results in a total recurring cost of approximately EUR 1 924 155 **per year (i.e. 9.62M over 5 years)** and **EUR 1M** recurring costs for setting up and operating the database (totalling **EUR 5M** over 5 years).
- Thirdly, ENISA's support to Member States in the **mutual assistance and supervision NIS 2 Directive entities**, subject to the jurisdiction of several Member States (link with option C) would result in recurring costs for human resources with minimum **4 additional FTEs**, equal to **EUR 513 108** per year (i.e. EUR 2.57M over 5 years).

---

[134] European Commission (2017). *Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA)*, https://digital-strategy.ec.europa.eu/en/library/final-report-evaluation-european-union-agency-network-and-information-security-enisa; European Railway Agency, *ERA Consolidated Annual Activity Report 2023*, https://www.era.europa.eu/library/documents-regulations/era-work-programmes-activity-reports; and Cybersecurity Act, *Impact Assessment accompanying the document*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52017SC0500.

[135] Based on Eurostat data and OECD, the European average salary for ICT roles is approximately EUR 56 500, derived from data adjustments factoring in regional wage disparities and purchasing power variances.

[136] The estimate of a number of human resources is based on ENISA's current resources implementing the Cybersecurity Support Action and the EU Cybersecurity Reserve, currently financed via contribution agreements.

[137] The cost of the procurement of services from trusted MSSP are to be financed from the EU funding programme (currently Digital Europe Programme) via contribution agreement, as provided by the Cyber Solidarity Act.

- Fourthly, for the support of critical sectors resilience (including implementation of the European action plan on healthcare cybersecurity) 5 FTEs are needed, which amounts to a yearly recurring cost of EUR 641 385, i.e. EUR 3.2M over 5 years.
- Fifthly, the development of the first **European individual cybersecurity skills attestation scheme** action would require **2 additional FTEs**, amounting to recurring costs of **EUR 256 554** per year (i.e. EUR 1.28M over 5 years). In addition, **6 FTEs** would be required for maintenance and auditing tasks of the providers that would be granted the role of entities issuing attestations, costing **EUR 769 662 recurring costs per yea**r *(i.e.* EUR 3.85M over 5 years, see Annex 4, section 4.1.2.2(a)). These FTEs would be **needed for the first five years,** covering the preparation and roll-out of the first European individual attestation scheme and starting the second scheme[138]. To meet the market demand most effectively and ensure budgetary efficiency, **fees collected from providers** would gradually complement and fully replace the EU budget after five years. In addition, there would be a **one-off operational adjustment cost of EUR 1M to** design, develop, and penetration-test a secure website for running the mechanism[139] (*see Annex 4, section 4.1.2.2(b)*). Additional **operational adjustment costs** borne by EU budget during the first three years and shared between EU budget and fees during the two-year transition period (see explanations below) would cover **scheme development and maintenance activities**, such as expert involvement and audits of providers. It can be estimated that the recurring costs would amount to EUR 212 920 per year, **i.e. EUR 1 064 600 in total over the first 5 years**, after which these operational costs would no longer be borne by the EU budget (*see Annex 4, section 4.1.2.2(b)*).

  In more details, based on ENISA's experience in running pilot projects, the first scheme would take five years to set up, test and roll-out[140]. During the first five years, EU budget would allow to cover the development, testing and rolling out of the first European individual attestation scheme. This period would be divided into two phases: (1) after an initial three-year period, during which EU budget would be necessary to nurture and test the model, (2) the activity would gradually become self-financed while still being supported by EU budget over the two following years. During this two-year transition period, both fee-based revenues and EU budget would support the model until it reaches sufficient maturity. In parallel, during the years four and five, ENISA would start developing a second scheme justifying to keep the same level of financing from EU budget for all five years, before the model would become fully independent financially.

  It is taken into account that as the schemes and the demand for authorisation from providers grows, this could lead to numerous applications of candidate attestation providers to be assessed by ENISA and ultimately, a growing number of providers for ENISA to supervise to ensure consistency in implementing the schemes. Consequently, ENISA would likely need additional resources to deliver on its tasks

[138] There are 12 ECSF cybersecurity profiles in total which can be divided into subsets. Therefore, there could be 12 European individual cybersecurity skills attestation schemes and potentially new ones in the future.
[139] Estimation provided by ENISA.
[140] Estimations are provided by analogy based on ENISA's experience in running pilots on a European individual attestation scheme, implementing the communication on the Cybersecurity Skills Academy.

(authorisation and supervision). After year five, these additional **costs would no longer be funded by the EU budget but by the fees collected from providers.**

The fees could also be used by ENISA to cover the cost of training a pool of auditors in each Member State to perform the supervision tasks and to set up an internal governance ensuring uniform implementation of the schemes.

Regarding cost-offsetting for ENISA after the five-year period, provided that operational costs for the Agency are estimated at EUR 1 064 600 in total over the first 5 years, i.e. recurring EUR 212 920 per year on average, and admitting that the the approximated average cost of an authorisation would amount to EUR 8 540 (see below, compliance costs for businesses and national authorities) and that renewing yearly the authorisation would cost on average EUR 800 per year, **25 new attestation providers would need to be authorised every year or 266 authorisation renewals granted to offset the operational costs** incurred by ENISA. On the medium run, it can be anticipated that cost-offsetting should be a hybrid model of authorisations for new providers and renewals.

- Sixthly, in relation to the **CRA single reporting platform (SRP) and the single entry point (SEP)**, **23 FTEs** are needed: 10 FTEs for the **management of the SRP,** 5 FTEs for related platform services (vulnerability analysis) and to cater for future needs driven by legislative developments, 8 additional FTEs should be foreseen for **managing the single-entry point** where the CRA platform will also be integrated (in connection with the Digital Omnibus *see Section 5.4*). This amounts to a total of **EUR 2 950 371 per year, as** a recurring cost (i.e. EUR 14.75M over 5 years).

  In addition, other costs amounting to **EUR 18 million over five years** will occur related to the operation and on-going maintenance (e.g. renting out for server space, paying for software licences), as follows. For the CRA single reporting platform and depending on the final architecture of the CRA platform (including possible extensions with the single-entry point), those costs could amount yearly for up to EUR 2M recurring costs, i.e. a **total of EUR 10M** over 5 years. The estimate is based on preliminary experience in setting up the platform (*see Annex 4, section 4.1.2.2(b)*).

  Furthermore, the extension of the CRA single reporting platform to the single-entry point is expected to amount to initial one-off adjustment costs of EUR 6 million for various activities ranging from design to equipment (*see Annex 4, section 4.1.2.2(b)*). In addition, operational expenses are estimated to be around EUR 500 000 per newly added legislation (one-off adjustment costs) for the extension. The assumption is that at least four legislations would be added in the next five years, amounting to EUR 2M. These one-off costs of EUR 2M and the one-off costs of 6M add up to a total of **EUR 8M one-off adjustment costs**. The estimate is based per analogy with the single reporting platform and experience with the implementation of other platforms supporting EU legislation in which ENISA is involved.

- Seventhly, for supporting the **implementation of the CRA**, 22 FTEs are needed (8 FTEs for the work on technical guidance, product security expertise and market analysis, 5 FTEs on standardisation related to CRA implementation and certification, 5 FTEs for supporting the market surveillance activities and 4 FTEs for conformity/testing and security evaluations. This amounts to a recurring cost of **EUR 2 822 094 per year (i.e. EUR 14.11M over 5 years)** (*see Annex 4, section 4.1.2.2(b)*). Additionally, there is a yearly **EUR 2M operational costs** related to the implementation of the CRA, i.e. EUR 10M over 5 years.

- Eighthly, for **operational cooperation, including situational awareness,** additional recurring adjustment costs of approximately EUR 4 641 385 are needed per year, which amounts to EUR **23.21M** over 5 years. This amount would cover 5 FTEs, i.e. **EUR 641 385 yearly**, and the costs related to procuring cyber threat intelligence (CTI), which would amount to approximately **EUR 4M per year (i.e. EUR 20M over 5 years)** (*see Annex 4, section 4.1.2.2(a) and (b)*). The estimate is based per analogy with similar CTI platforms (*see Annex 4, section 4.1.2.2(b)*).
- Ninthly, for setting up secure communications a one-off cost of EUR 1.1M was calculated in the first year and then a recurring yearly maintenance cost of EUR 1 083 250 is needed over 4 years (i.e. a total of EUR 4.33 M over 4 years).
- Tenthly, for the reaching the required cyber maturity level, a yearly EUR 3 million is needed, i.e. EUR 15 million over 5 years. This is based on consultations with ENISA and among other things includes the migration to a secure European Data Centre. It is of paramount importance that the EU Cybersecurity Agency has the highest levels of cybersecurity and is recognised as a trust partner and lead by example in Europe.
- Additionally, in the context of operational cooperation, an additional cost stems from the daily allowance of **National Liaison Officers (NLOs) seconded by each Member State** to ENISA, (*see below under 'costs for national authorities'*), which amounts to a recurring adjustment cost of EUR **1 440 000 yearly** for **40 NLOs (i.e. EUR 7.2M over 5 years)**.
- Finally, given the overall increased headcount of ENISA an additional 10 FTEs are needed for admin/support functions (such as accounting, HR, IT etc.) amounting to a recurring adjustment cost **EUR 1 282 770 yearly (i.e. EUR 6.41 M over 5 years).**

Regarding **national authorities**, a recurring adjustment cost emerges by seconding to ENISA at least one national liaison officer per Member State (i.e. in total at least 40 additional NLOs) for tasks related to operational cooperation, which amounts to an annual recurring cost of EUR 56 500 per NLO, i.e. EUR **2.26M** for 40 NLOs (**i.e. EUR 11.3M over 5 years**) *(see Annex 4, section 4.1.2.3).*

Related to the **European individual attestation scheme**, next to the costs for ENISA, it is not possible to provide aggregated costs as participation would remain voluntary in nature. The following costs would nevertheless occur for the stakeholders (public and private) who voluntarily decide to apply to becoming authorised attestation providers:

- For **businesses and national authorities**: compliance costs would cover:
  Administrative costs: providers of European individual cybersecurity skills attestations would bear **both one-off and recurrent fees**. Providers would pay a fee to ENISA to apply to become an authorised provider for a particular cybersecurity role profile as laid down in the European Cybersecurity Skills Framework, or for a subset thereof (e.g. emergency incident responder). ENISA would carry out regular audit to ensure that those providers can be authorised and maintain their authorisation (recurrent costs). The costs of an application or a renewal would vary depending on the cybersecurity role profile for which the provider applies. For instance, an application to become authorised provider for a role that entails a practical assessment (e.g. use of a cyber range or labs) would likely be higher than the cost of an application that entails theoretical assessment only. In order to evaluate the range of

costs, national authorities who have developed such mechanisms for specific role profiles and are known to the Commission have been explored (*see Annex 4, section 4.1.2.3).* Based on one Member State's publicly available information[141], it can be estimated that the cost for providers of an **initial authorisation, including surveillance** for the profiles of Cybersecurity Manager and Cybersecurity Auditor would amount to an estimated **EUR 8 540.** Using the same country's publicly available information, it can be estimated that the provider would additionally pay **a yearly fee of around EUR 800** for maintaining the authorisation (recurring cost of EUR 800, every year for a duration set in the scheme) *(see Annex 4, section 4.1.2.3).* It should be noted that this estimation represents an order of magnitude of the fees related to authorising providers for two specific role profiles in one Member State, based on publicly available data. It does not reflect an average fee across Member States nor caters for the variation of costs from one country to another. It does not cover the variations in the costs across all ECSF role profiles. In this regard, it can be noted that the fees to take an exam with a private cybersecurity certification provider vary depending on the role profile, e.g. the certification exams associated to the ECSF profile Cybersecurity Architect are more expensive than the certification exams associated to the ECSF role profile Cybersecurity Implementer[142]. The fact that an exam, notably the assessment method, costs more for some role profiles could in turn entail higher fees to become authorised. Similarly, the different levels of proficiency could have an impact on the fees to become authorised[143]. Therefore, the estimation provided in this report should be understood as illustrative and does not pre-empt nor impact the future implementing acts that will determine the fees associated each European individual cybersecurity skills attestation schemes.

Adjustment costs: providers will need in practice to adjust to meet the European individual cybersecurity skills attestation scheme requirements. These costs will **vary from one provider to another, depending on the level of maturity of the provider and its already ongoing activities**. For instance, adjustment costs may cover: to have or to hire individuals to conduct and supervise the assessments, to have the necessary personnel to ensure that the scheme requirements continue to be met, to submit the application to ENISA and maintain their authorisation, to comply with scheme elements such as the storage method of the attestation in the European Union Digital Identity wallet. These adjustment costs will be **one-off costs**, to be in a capacity to be authorised and to implement the scheme. It can further be anticipated that these adjustment costs will be higher for the first authorisation. **Recurring costs** to maintain the authorisation or to adapt to the other schemes should be marginal. Additionally, the **costs will vary from one scheme to another**, in particular with relation to the assessment method to be used by the provider according to the applicable scheme. For example, an assessment method based on testing knowledge

---

[141] Slovakia, see Decision RR-02: Price list of SNAS services

142 See in this regard the mapping of certifications by vendor-neutral providers against the ECSF, e.g. ISC2 and CompTIA and associated costs of certification exams (How Much Do ISC2 Certification Exams Cost? and IT, AI, and Data Certifications | CompTIA Europe)

143 Experience of private providers of cybersecurity certifications shows that the cost of a certification can vary based on the proficiency level, e.g. a certification for experienced incident handler proves more expensive than a certification for incident handler, see for example GIAC certifications (Certification Pricing | GIAC Certifications. This could influence the fees for becoming an authorised provider.

only would entail less costs than an assessment method that could induce practical testing on a virtual machine. Without the scheme in place and the assessment methods defined, it is not possible to anticipate the extent of the variation in costs. Such costs will likely be linked to the IT equipment a provider will need to invest in to conduct the assessments and can therefore be anticipated to be **one-off** cost.

- The fees applying to providers would be partly offset by the prices of individual attestations paid by **individuals**. Those fees would be likely one-off and recurring in case the professional wishes to maintain the skills attestation. However, considering that the foreseen cost of the European individual cybersecurity skills attestation would be potentially closer to those delivered by public organisations, and lower than the current average cost of cybersecurity certifications delivered by private certification bodies, this could in fact lead to costs savings (see further below).
- No further compliance costs are foreseen **for national authorities**. They may cooperate with ENISA to shape the individual attestation schemes on a voluntary basis, deciding on the resources to invest.

***Option A.3*** extensively reforms of ENISA's mandate, giving ENISA possibility to directly support operationally individual entities. This approach builds upon the reforms proposed in option A.2. The financial implications of implementing option A.3 are considerable, with an estimated **total recurring adjustment cost** of approximately EUR 14.04M yearly for ENISA (see *Annex 4*)**.** This amounts to EUR 70.22M over 5 years. It reflects the investment required to extend ENISA's mandate and transform its operational capabilities.

The first key component is establishing an operational team for direct intervention to support to entities under the NIS 2 Directive. This team would be composed of ENISA staff and national liaison officers. Based on previous estimates[144], the initial setup would cost around EUR 1.92M and require 15 FTEs (in the 1st year). Once fully operational, management and maintenance costs would reach around EUR 3.21M, assuming that the team would progressively grow to reach 25 FTEs in the 2nd year. The total cost for this component is estimated at EUR 14.75M over 5 years (with 25 FTEs from the 2nd year), which gives when divided in 5 an average recurring cost of EUR 2.9M per year.

The second key component focuses on building operational support, akin to an EU-level cybersecurity umbrella, includes technical advice to NIS2 entities, serving as a centre for information. Based on past cost estimates for creating such an umbrella[145], 2.5 FTEs would have to be added to the reforms of Option A.2, with the recurring cost of EUR 320 693 per year, i.e. EUR 1.6M over 5 years. The two key components will generate a yearly recurring cost of EUR 3 271 064.

In addition, ENISA will pay the daily allowances of 5 SNEs seconded to ENISA (additionally to the 40 NLOs seconded to ENISA under Option A.2), which amount to a recurring cost of EUR 180 000 yearly. i.e. EUR0.9M over 5 years (see further details on NLOs and SNEs below). Moreover, additional organisational burdens would derive from the need to integrate NLOs and SNEs.

---

[144] Ibid.

[145] Actualised costs estimates based on *Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA)*, https://digital-strategy.ec.europa.eu/en/library/final-report-evaluation-european-union-agency-network-and-information-security-enisa.

**National authorities would incur recurring adjustment costs of** EUR 282 500 (i.e. EUR 1.41M over 5 years) for delegating additional approximately 5 SNEs to ENISA.

Table 2: Allocation of FTEs and costs for Options A.1, A.2 and A.3

| Option/ Stakeholder/ Purpose | Details | 2028 FTEs | 2029 FTEs | 2030 FTEs | 2031 FTEs | 2032 FTEs | Costs per year (EUR) | Total costs over 5 years (EUR) |
|---|---|---|---|---|---|---|---|---|
| **Option A.1/ ENISA, MS, businesses, citizens** | | - | - | - | - | - | - | - |
| **Option A.2** | | | | | | | | |
| **ENISA** | | | | | | | | |
| Reserve | | 10 | 10 | 10 | 10 | 10 | 1 282 770 | 6 413 850 |
| CVD | | 15 | 15 | 15 | 15 | 15 | 1 924 155 | 9 620 775 |
| Mutual Assistance on NIS2 | | 4 | 4 | 4 | 4 | 4 | 513 108 | 2 565 540 |
| Support for critical sectors resilience | | 5 | 5 | 5 | 5 | 5 | 641 385 | 3 206 925 |
| Skills scheme development | | 2 | 2 | 2 | 2 | 2 | 256 554 | 1 282 770 |
| Skills scheme maintenance | | 6 | 6 | 6 | 6 | 6 | 769 662 | 3 848 310 |
| CRA platform & single-entry point | | 23 | 23 | 23 | 23 | 23 | 2 950 371 | 14 751 855 |
| CRA implementation | | 22 | 22 | 22 | 22 | 22 | 2 822 094 | 14 110 470 |
| Operational cooperation | | 5 | 5 | 5 | 5 | 5 | 641 385 | 3 206 925 |
| Admin | | 10 | 10 | 10 | 10 | 10 | 1 252 770 | 6 413 850 |
| **TOTAL FTEs for ENISA[146]** | | **102** | **102** | **102** | **102** | **102** | **13 084 254** | **65 421 270** |
| NLOs seconded to ENISA (budget split between. ENISA &MS) | Daily allowances (EU budget) | 40 | 40 | 40 | 40 | 40 | 1 440 000 | 7 200 000 |
| **TOTAL costs for FTEs + NLOs for ENISA** | | **142** | **142** | **142** | **142** | **142** | **14 524 254** | **72 621 270** |
| Setting up and operating the CVD database | | | | | | | 1 000 000 | 5 000 000 |
| Skills scheme development and maintenance | | | | | | | 212 920 | 1 064 600 |
| Skills website (one-off cost) | | | | | | | | 1 000 000 |
| CRA platform maintenance | | | | | | | 2 000 000 | 10 000 000 |
| CRA implementation | | | | | | | 2 000 000 | 10 000 000 |
| CTI services | | | | | | | 4 000 000 | 20 000 000 |
| Single entry point – one-off costs | Design, equipment, legislations | | | | | | | 8 000 000 |
| Secure communications set-up (one-off costs) | | | | | | | | 1 100 000 |
| Secure communications maintenance | | | | | | | 1 083 250 | 4 333 000 |
| Cyber maturity | | | | | | | 3 000 000 | 15 000 000 |
| **Total costs for ENISA** | | | | | | | | **148 118 870** |
| **Member States** | | | | | | | | |
| NLOs seconded to ENISA (budget split between. ENISA and MS) | MS budget | *(40)* | *(40)* | *(40)* | *(40)* | *(40)* | 2 260 000 | 11 300 000 |
| **TOTAL for Member States** | | *(40)* | *(40)* | *(40)* | *(40)* | *(40)* | **2 260 000** | **11 300 000** |
| **Businesses - Potential cost of paying a fee to ENISA to get authorised to deliver European individual attestations** | | | | | | | | |

[146] ENISA's FTEs and costs related to the certification are listed under Option B.2 and amount to between **8 (in 2028) and 14 FTEs** (from 2030 onwards). The total number of FTEs could reach between 83 and 89 FTEs by 2030 depending on the combination of policy options (B2/B3 + D2/D3).

| Option/ Stakeholder/ Purpose | Details | 2028 FTEs | 2029 FTEs | 2030 FTEs | 2031 FTEs | 2032 FTEs | Costs per year (EUR) | Total costs over 5 years (EUR) |
|---|---|---|---|---|---|---|---|---|
| **Citizens - Potential cost of acquiring the individual skills attestation** | | | | | | | | |
| **Option A.3** (building on option A2) | | | | | | | | |
| **ENISA** | | | | | | | | |
| FTEs covering areas under Option A.2 (FTEs + NLOs) | | **142** | **142** | **142** | **142** | **142** | **14 524 254** | **72 621 270** |
| Other costs for ENISA under Option A.2 | | | | | | | | **75 497 600** |
| Operational team - direct support under the NIS 2 Directive | | 15 | 25 | 25 | 25 | 25 | 2 950 371 | 14 751 855 |
| EU Cybersecurity Umbrella | | 2.5 | 2.5 | 2.5 | 2.5 | 2.5 | 320 693 | 1 603 463 |
| Additional SNEs Option A.3 (budget split between. ENISA & MS) | Daily allowances (EU budget) | *5* | *5* | *5* | *5* | *5* | 180 000 | 900 000 |
| **TOTAL costs related to FTEs, NLOs and SNEs** | | **164.5** | **174.5** | **174.5** | **174.5** | **174.5** | **17 975 318** | **89 876 590** |
| **TOTAL Option A.3 for ENISA** | | | | | | | | **165 374 188** |
| **Member States** | | | | | | | | |
| From Option A.2 NLOs seconded to ENISA (budget split between ENISA and MS) | MS budget | *(40)* | *(40)* | *(40)* | *(40)* | *(40)* | 2 260 000 | 11 300 000 |
| Additional SNEs Option A.3 (budget split between ENISA & MS) | MS budget | *(5)* | *(5)* | *(5)* | *(5)* | *(5)* | 282 500 | 1 412 500 |
| **TOTAL NLOs Option A.3 (Option A.2 + additional SNEs under Option A.3)** | MS budget | ***(45)*** | ***(45)*** | ***(45)*** | ***(45)*** | ***(45)*** | **2 542 500** | **12 712 500** |
| **Businesses & Citizens -** The same as Option A.2 (No additional costs under Option A.3.) | | | | | | | | |

Table 3: Costs of policy options A (ENISA mandate)

| Costs (EUR) over 5 years | Policy options [ENISA mandate] | | |
|---|---|---|---|
| | **A1** | **A2** | **A3** |
| Businesses | No costs | Administrative cost: potential fee to be paid to ENISA to apply for becoming authorised attestation provider and maintenance costs<br><br>Adjustment costs to meet the European individual cybersecurity skills attestation scheme requirements: one-off costs for first authorisation and marginal recurring costs to adapt to other schemes requirements or for renewal of authorisation | Administrative cost: potential fee to be paid to ENISA to apply for becoming authorised attestation provider and maintenance costs<br><br>Adjustment costs to meet the European individual cybersecurity skills attestation scheme requirements: one-off costs for first authorisation and marginal recurring costs to adapt to other schemes requirements or for renewal of authorisation |
| Public authorities | No costs | EUR 11.3M (40 national liaison officers)<br><br>Administrative cost: potential fee to be paid to ENISA to apply for becoming authorised attestation provider and maintenance costs | EUR 12.7M (45 national liaison officers)<br><br>Administrative cost: potential fee to be paid to ENISA to apply for becoming authorised attestation provider and |

| Costs (EUR) over 5 years | Policy options [ENISA mandate] | | |
|---|---|---|---|
| | A1 | A2 | A3 |
| | | Adjustment costs to meet the European individual cybersecurity skills attestation scheme requirements: one-off costs for first authorisation and marginal recurring costs to adapt to other schemes requirements or for renewal of authorisation | maintenance costs<br><br>Adjustment costs to meet the European individual cybersecurity skills attestation scheme requirements: one-off costs for first authorisation and marginal recurring costs to adapt to other schemes requirements or for renewal of authorisation |
| ENISA | FTEs: negligible<br>Other costs: negligible | **Total: EUR 148.12M** (one-off and recurrent adjustment costs)<br>**FTEs + NLOs: EUR 72.6M (102 FTEs +40 NLOs)**<br><br>Other costs over five years: **EUR 75.5M** (adjustment costs)<br>• Setting up and operating the CVD database: EUR 5M (one-off and recurrent)<br>• CTI single repository: EUR 20M (one-off and recurrent)<br>• Skills website & other attestation schemes activities: EUR 2.06 million (one-off and recurrent)<br>• Single reporting : EUR 10M (one-off and recurrent)<br>• CRA implementation: EUR 10M<br>• Single entry point: EUR 8M (one-off)<br>• Secure communications set-up and maintenance: EUR 5.5M (one-off and recurrent)<br>• Cyber maturity (recurrent): EUR 15M | **Total: 165.37 EUR** (one-off and recurrent adjustment costs)<br>FTEs + NLOs: EUR 89.88M million (102 FTEs + 45 NLOs)<br><br>Other costs: EUR 75.5M (adjustment costs) |
| Citizens | No costs | Potential cost of acquiring the individual skills attestation (one-off) | Potential cost of acquiring the individual skills attestation (one-off) |

(b) Cost savings for public authorities, citizens, businesses related to **efficiency and reduction of time to detect and respond to incidents.**

Under **Option A.1**, the anticipated economic impact on EU institutions and bodies, in particular on **ENISA,** is characterised by enhanced resource efficiency, improved

coordination, and sector-specific support, and would generate limited cost savings of almost EUR 70 000[147] in ENISA's annual budget, which would be absorbed by other activity areas that will be enhanced (such as operational cooperation). Currently, ENISA collaborates with several stakeholders on various activities related to cybersecurity market, research and development, i.e. national and EU R&I entities, academia and industry and the ECCC. Under this Option A.1, ENISA's research-related activities would be removed, avoiding duplication of efforts already undertaken by the ECCC or project consortia. In this view, ENISA would focus on strategic oversight, enabling a more targeted use of its resources.

For **national authorities**, by facilitating collaboration, the policy option aims to streamline efforts and avoid duplication, thereby reducing administrative overhead and improving the efficiency of cybersecurity initiatives across Member States. Additionally, this policy option enhances ENISA's role as the secretariat of two operational networks, the CSIRTs network and EU CyCLONe, which would lead to further procedural efficiencies.

Option A1 would also bring costs savings **for businesses**. As a facilitator of operational cooperation between Member States, particularly for cross-border incidents and information flows, ENISA would further contribute to incident response, which could potentially help with minimising potential financial losses for businesses by preventing prolonged disruptions and result in some cost efficiencies, by reducing the overhead associated with incident management.

Under **Option A2,** increased awareness and improved operational coordination could generate considerable costs savings related to **faster incident detection and response** for **businesses, public authorities and citizens** (*Annex 7)*. Data shows the importance of detecting and responding in a timely manner to reduce the impacts of cybersecurity incidents (time to resolve). Improved information flows, improved cybersecurity approaches and cooperation among Member States will impact also better preparedness and prevent cybersecurity incidents from occurring avoiding potentially very large material and non-material damages (see examples of incidents and real-world cases in *Annex 7*). Concretely, if the additional resources could lead ENISA to effectively increase its support on incident response and situational awareness[148], the potential cost savings for **businesses** and **public authorities** would very likely be significant.

Regarding situational awareness, currently, different EU entities are using CTI coming from different vendors that have different focuses and that leaves intelligence gaps creating a fragmented picture between the Union entities. A common repository of cyber threat intelligence feeds could, in turn, close those gaps and ensure the reliability of data, which, in turn would contribute to a common situational awareness. In addition to that, the EU-wide common threat landscape could benefit not only the Union entities but also the Member States representatives within the CSIRTs Network and CyCLONe, thus, potentially, with enriched and verified information, feeding into the work of the national

[147] Considering that the estimated budget for 2025 for conducting research-related activities is EUR 697 887 (reaching EUR 2.1 million when considering all direct and indirect budget allocations), if such streamlining - using a conservative estimate and focusing only on direct budget allocation - were to amount to 10% of the current effort, this could be dedicated to other activities.

[148] ENISA, *2023 Consolidated Annual Activity Report*, https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2023. , ENISA was involved in 775 incidents in 2022.

agencies/ institutions. This, however, cannot be quantified as the cost of each CTI feed depends on the needs for the service (the scope, whether the service includes CTI reports (and, if so, their breadth and frequency), whether it is only open-source or also closed/human intelligence, the extent to which this is tailored to a customer, institutions etc.

The quantification of the positive impact of the measures would in theory need to include both **avoided incidents** and **reduction of the impact of incidents** that occur. Both parameters are difficult to quantify. If ENISA, based on these additional resources, could double its involvement and support for incident response activities - from 1 550 incidents compared to the involvement in 775 in 2022 based on ENISA's reporting [149]- the potential cost savings related to impact reduction for EU businesses and national authorities would be substantial. It is possible to establish that due to the fact that ENISA's current capabilities would be already higher and that therefore additional resources could help manage incidents more effectively, it is likely that the response to incidents could be faster. While it is also possible to assume that through enhanced situational awareness, incidents could be avoided, no credible assumption could be defined as to the number of avoided incidents. When it comes to preventing incidents, the measures would particularly impact incidents with malicious intents (vs. incidents due to human error or natural disasters) as shared situational awareness would aim to target the detection of such activity. Considering available data regarding certain types of cybersecurity incidents, it is typically considered that 51% of the incidents can be attributed to malicious activities.

Looking at the impacts in terms of reducing the costs of incidents that occur, to quantify the possible cost savings related to enhanced situational awareness and better operational coordination, the assumption is taken that the measures will lead to a reduced recovery time thanks to faster detection and response (i.e. **reduction of the impact of malicious incidents**). It is found that **cost savings for businesses and public authorities could be of EUR 3.7 to 4.4 bn over five years thanks to faster recovery time from a cybersecurity incident**. This estimate is based on data available[150]related to the average cost of data breaches in Europe that serves as proxy. The assumption is that recovery time from data breaches would be reduced from 241 to below 200 days over five years after the application of the measures (in 2032), assuming 11,079 incidents affecting NIS entities (with malicious intent) and taking into account that existing measures under the BaU would lead to a reduction of cost related to incidents between 20 and 33%. (see *Annex 4, section 4.1.1.1*). These assumptions can be challenged and are informed by available data (e.g. estimates for the costs for recover times under 200 days vs. above 200 days), hence the quantitative benefits should be treated as very broad estimates that illustrate a possible impact of the proposed measures. In practice, the cost savings could be lower as the report assumes the same cost saving per incident across all NIS2 entities, while it is to be expected that they can be sectoral and size differences. Other approaches and proxies could have likely been chosen (e.g. make an assumption a percentage of

[149] ENISA 2023 Consolidated Annual Activity Report, https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2023.

[150] IBM, Cost of a data breach report 2025, https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91; IBM, *Cost of data breach: financial industry 2024*, https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry.

avoided data breaches), however have been discarded due to insufficient data. Additionally, the development of **European individual cybersecurity skills attestation schemes** would entail a number of benefits, further detailed in *Annex 4, section 4.1.1.2*. **National authorities** would not be constrained to develop or maintain in-house schemes as they could rely on the European individual cybersecurity skills attestations, notably to check the competence of individuals working for managed security service providers, for hiring purposes. Centralised EU individual attestation schemes, which would be developed with the support of national authorities themselves, industry and academia, would further rationalise the costs, avoiding proliferation of national schemes which aim at a similar objective across Member States but are developed in silos. **For businesses** authorised to deliver such attestations it will create new business opportunities. For the wider economy, it would support training and hiring practices by providing visibility of competences and quality assurance of candidates. In particular, SMEs, which have little chance of seeing their in-house developed attestations recognised by the market in the face of major cybersecurity players, would be given access to the market of "individual cybersecurity certifications". **For ENISA,** there are direct benefits counterweighting the costs of the development and maintenance of European attestation schemes, as this activity could be funded through fees charged to the providers. These fees would offset the costs for the Agency, as they would reflect the real costs of the related activity and would not generate a profit. The amount of the fees would be adapted to each European individual cybersecurity skills attestation scheme, to ensure a price as close as possible to the expenses incurred to perform this task. **Consumers, such as cybersecurity professionals,** will benefit from holding an individual skills attestation recognised at EU level which would not only enhance an individual's appeal in the job market but also foster wage increase. According to recent studies, 59 % of employees report a salary increase of 6–20 % within a year after being certified[151]. Attestations also support external career mobility[152] and skills portability, which is particularly valuable for entry-level professionals, young graduates, SMEs, and workers seeking mobility. This has a positive impact on salary levels, reflecting the recognised value of their expertise[153]. Moreover, defining the costs of an attestation at EU level could lead to **potential cost savings**, likely being closer to those delivered by public organisations and lower in cost than those delivered by private certification bodies *(ibid.)*.

Under **option A.3**, the benefits described for A2 related to **faster response and slowing down proliferation** of **cybersecurity incidents** would be likely increased. The direct operational support from ENISA to the NIS 2 Directive entities would bring cost savings for **national authorities**, as ENISA's team would, at least partially, take over support activities for incident response, which are now carried by national CSIRTs. As the support would be provided in a coordinated manner, especially in case of cross-border cybersecurity incidents, it could lead to higher savings than the cost of delegating additional national liaison officers. Closer collaboration between ENISA and the Member States would enhance the collective cybersecurity posture. Based on the quantitative

[151] Pearson VUE 2025 Value of Certification Report - Candidate Report

[152] Agence nationale de la sécurité des systèmes d'information (ANSSI) (2025), Etude 2025: Les professionnels de la cybersécurité, https://cyber.gouv.fr/sites/default/files/document/Etude_des_professionnels_de_la_cybers%C3%A9curit%C3%A9_VF2.pdf

[153] Fortinet. (2023). 2023 Cybersecurity Skills Gap Report, https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf

estimates provided under A2, it can be assumed that the reduced impacts of incidents would also apply here and be higher, ranging from **EUR 3.7 to 4.4 bn over five years**.

Table 4: Benefits of policy options A (ENISA mandate)

| Benefits | Policy options [ENISA mandate] | | |
|---|---|---|---|
| | A1 | A2 | A3 |
| Citizens | Neutral | > A1<br>• Indirectly benefit of enhanced cyber posture<br>• Better visibility on the labour market for cybersecurity professionals, increased career advancements, better wages<br>• Enhanced skills portability<br>• Attestation cost per attestation: ~EUR 300–350 (public) vs. ~EUR 677 (private) | Indirectly benefit from improved cyber posture >A2 |
| Businesses | Some cost savings related to cyber incidents | • Substantial benefits from reduced impacts of incidents, that could range from **EUR 3.7 to 4.4 bn over five years** > A1<br>• Reputation of skills attestation providers<br>• Access to the cybersecurity skills market (especially SMEs) | Substantial benefits from reduced impacts of incidents, that could range from **EUR 3.7 to 4.4 bn over five years** >A2 |
| Public authorities | Reduces administrative overhead | • Substantial benefits from reduced impacts of incidents, that could range from **EUR 3.7 to 4.4 bn over five years** > A1<br>• Cost avoidance for public authorities that are developing or envisage to develop attestation schemes (reduced compliance and supervisory burden for authorities) | • Substantial benefits from reduced impacts of incidents, that could range from **EUR 3.7 to 4.4 bn over five years** >A2<br>• cost savings through direct operational support by ENISA |
| EU institutions/ ENISA | Efficiency gains | Same as in Option A.1 | Same as in Option A.1 |

6.1.1.2. Certification (Policy Options B.1 to B.3)

The possible economic impacts regarding the policy options related to certification consider how the policy options (and their combination) would impact the scenarios for

the development of cybersecurity certification schemes by ENISA and the start of the maintenance period. *Annex 4 (section 4.2)* illustrates the timeline for maintenance if relevant schemes would materialize and shows in detail how this impacts the number of FTEs at ENISA and at national level. Depending on the policy options, the following schemes will be in maintenance for the next years: 2028 (**BaU**) - EUCC, MSS, EU ID Wallet; 2029 (**B + D2**) – EU5G; 2029 (**B + D3**) EUCS and EU5G; (**B2/B3**) 2030 - Cyber posture scheme.

(a) Costs for businesses, public authorities, citizens

Under ***Option B.1*** compliance costs would occur due to the setting up of the maintenance structure and the alignment of schemes with existing cyber legislation, in particular the CRA.

ENISA would carry **adjustment costs** to align existing schemes (EUCC) and draft candidates scheme under development (ID Wallet and MSS) with **existing legislation**. The technical review of draft candidate schemes would also include EU5G (with policy option D2/D3) and EUCS (with D3). A one-off adjustment cost is foreseen for the necessary technical updates and documentation revisions of existing schemes. At a minimum, the EUCC scheme would be reviewed. It is assumed that this work could be covered by the existing FTEs dedicated to scheme development.

Furthermore, the (one-off and recurrent adjustment) costs of the establishment of a maintenance mechanism for existing and upcoming schemes would be mainly sustained by ENISA. Additional recurrent (adjustment) costs for schemes maintenance would be added with an estimated **2 FTEs dedicated to the maintenance of each scheme**, for a total of EUR 256 554 per year (per scheme) taking 1 FTE = EUR 128,277 EUR (*see Annex 4, section 4.2*). Furthermore, the maintenance of schemes would lead to recurrent operational costs covering the activities of the dedicated ECCG sub-group, including regular in-person meetings and the work of experts supporting the technical work, that are estimated at EUR 200 000 per year (*See Annex 4 Section 4.1*). Under B1, those operational costs would not be compensated by any fees contrary to the option B2. These costs would gradually be carried by ENISA as candidate schemes is submitted, and maintenance phase starts following their adoption (see table below).

Regarding **businesses** and **public authorities,** compared to the *business-as-usual*, the **maintenance structure** would not lead to specific costs. In the long-term, more future-proof schemes could lead to higher demand for schemes, for instance in the context of public procurement. However, given that, compared to the baseline scenario, this policy option will not introduce any mandatory requirements, only the participating vendors would bear **possible additional adjustment and administrative costs**. The decision to certify would be driven by business considerations (i.e. cost to certify vs. revenues generated by winning tenders). As these costs would depend on the engagement of the manufacturers into voluntary initiatives, it is not possible to give aggregated cost estimates, under any scenario (see below).

Following cost indications can be provided related to **new schemes that could be finalised** under B1 depending on the scenarios: an additional 5G scheme could be adopted under B1 + D2 or D3. Both EU5G and EUCS would be adopted under B1 + D3. The **costs related to the adoption of a new scheme** would typically include the following:

For **businesses**: a certification process involves adjustment costs (to meet scheme requirements) and one-off and recurrent administrative costs (covering documentation;

certification; regular audits as illustrated in *Annex 4, section 4.2*[154]). These costs are not always directly communicated and depend greatly on the size and complexity of the assessment. Regarding cloud certification, based on available data, estimates range from a minimum of **EUR 5 000 to 160 000** depending on the certification process (*see Annex 4, section 4.2*). Maintaining a certification also entails **recurrent costs**, such as periodic updates and audits to comply with evolving scheme requirements. They are more demanding the higher the assurance level.

For **public authorities**: every new scheme would come with additional resources in terms of supervision of competent conformity assessment bodies and the compliance of businesses as well as possibly issuance of certificates at level high (one off and recurrent enforcement costs). The findings of a consultation run in July and August 2025, indicated that those could be in **average 5 FTEs**, taking an estimation of 56,500 EUR for one FTE (*see Annex 4, section 4.2*), this would lead 282.500 EUR for 5 FTEs of recurrent costs by Member State. The costs would be higher for Member States that have not yet any national schemes in place and/or that decide to issue certification at level high (to be issued by a public authority). Member States with existing national schemes would likely use existing resources to implement the European scheme. Member States with schemes in place would mainly bear adjustment costs. Assuming generously that 27 MS would adopt the new scheme in the first year, and allocate an average of 5 FTEs, this could mean **7 627 500 EUR per year for all 27 Member States for the adoption of a new scheme (compared to BaU)**. The aggregated costs are indicated in the table below.

**CABs** would support mainly adjustment costs (training and meeting requirements to get accredited) and one-off and recurrent administrative costs due to accreditation and monitoring of their competence by relevant authorities. The administrative costs for accreditation can range between EUR 4 000 and EUR 20 000 per accreditation according to secondary sources[155], with part of these costs being recurrent (payment of accreditation fees every one or two years). It is not possible to give an aggregated estimate as this would depend on the voluntary engagement of CABs. Furthermore, the costs would be largely offset by revenues (see sub-section on benefits).

Regarding the **alignment with existing legislation**, the adjustment costs for businesses would be mitigated thanks to transition periods. For EUCC, businesses would align with the reviewed scheme either when applying to a new certificate or reviewing their old certificate. Furthermore, for manufacturers covered by the CRA, this would likely build on on-going work related to the preparation for the presumption of conformity of EUCC with CRA (see baseline scenario). For **public authorities**, no additional compliance costs are foreseen.

Table 5: Overview of ENISA resources under option B.1

| **Option B.1 – FTEs (one-off and recurrent costs for ENISA) 1 FTE = EUR 128 277** | 2028 | 2029 | 2030 | 2031 | 2032 | **Average yearly cost (EUR)** | **Total costs over 5 years (EUR)** | |
|---|---|---|---|---|---|---|---|---|

[154] ENISA, *CONFORMITY ASSESSMENT OF Qualified Trusted Service Providers - Technical guidelines for conformity assessment of qualified trust service providers*, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Conformity%20Assessment%20of%20Qualified%20Trust%20Service%20Providers.pdf

[155] SWD(2022) 282 final, see in particular page 60.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **B1** | 6 | 6 | 6 | 6 | 6 | 769 662 | **3 848 310** | |
| **B1+ D2** | 6 | 8 | 8 | 8 | 8 | 974 905 | **4 874 526** | |
| **B1+ D3** | 6 | 10 | 10 | 10 | 10 | 1 180 148 | **5 900 742** | |
| **Operational costs (recurrent costs) EUR 200 000 / year** | 2028 | 2029 | 2030 | 2031 | 2032 | **Average yearly cost (EUR)** | **Total operational costs over 5 years (EUR)** | **Total recurrent adjustment costs over 5 years** (FTEs + operational**)** |
| **B1 (3 schemes)** | 600 000 | 600 000 | 600 000 | 600 000 | 600 000 | 600 000 | **3 000 000** | **6 848 310** |
| **B1+ D2 (4 schemes)** | 600 000 | 800 000 | 800 000 | 800 000 | 800 000 | 760 000 | **3 800 000** | **8 674 526** |
| **B1+ D3 (5 schemes)** | 600 000 | 1 million | 1 million | 1 million | 1 million | 920 000 | **4 600 000** | **10 500 742** |

Table 6: Overview of costs for public authorities under option B.1

| **Option B.1 – FTEs (one-off and recurrent costs) 1 FTE = EUR 56 500** | 2028 | 2029 | 2030 | 2031 | 2032 | **Average yearly costs (EUR)** | **Total costs over 5 years for 27 MS (EUR)** |
|---|---|---|---|---|---|---|---|
| **B1** | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| **B1+ D2** | 0 | 5 | 5 | 5 | 5 | 226 000 | **30 510 000** |
| **B1+ D3** | 0 | 10 | 10 | 10 | 10 | 452 000 | **61 020 000** |

***Option B.2*** would entail the same costs as under B1 and additional costs for ENISA, public authorities and businesses, that would exist due to changes in the governance framework and the extension of the scope to certification of entities.

Regarding FTEs, costs, the role of **ENISA** as 'scheme manager' would require some **additional resources to tackle horizontal tasks**, such as increased stakeholder engagement and involvement in drafting technical specifications and standardisation activities related to schemes. Hence, it seems appropriate to foresee **2 additional FTEs** (recurrent adjustment costs) compared to existing 2 FTEs dedicated to this work under the BaU scenario (one-off and recurrent costs starting in 2028). This estimation also considers the development of an **additional scheme related to the cyber posture of entities** that would require between 2 and 3 FTEs (based on the scheme development costs observed from past schemes). The resources to develop a new scheme could be taken from existing ENISA FTEs dedicated to scheme development as other schemes would move to the maintenance phase, however more resource might be necessary for instance if no available standards are available. A new scheme related to cyberposture (assumption is that the candidate scheme would be submitted in 2029 and maintenance to start in 2030) would also require additional dedicated resources (2 FTEs one-off and recurrent as of 2030).

Next to FTE related costs, as under option B.1, maintenance activities would involve operational costs. Under option B.2. those operational maintenance costs would be partly and gradually offset by a **fee mechanism** that would charge conformity assessment bodies when publishing their certificates on ENISA's website (see below). The expectations are that the revenues from these fees to raise in progression with the adoption of every new scheme, with the first revenues from the maintenance of the first adopted scheme (EUCC) to start in 2029 (see detailed explanations in *Annex 4 section 4.2*).

Table 7: Overview of ENISA resources under option B.2 *(same for B.3)*

| **Option B.2 – FTEs ENISA (one-off and recurrent costs) 1 FTE = EUR 128 277** | 2028 | 2029 | 2030 | 2031 | 2032 | Average yearly cost (EUR) | **Total costs over 5 years (EUR) FTEs** |
|---|---|---|---|---|---|---|---|
| **B2** | 8 | 8 | 10 | 10 | 10 | 1 180 148 | **5** 900 742 |
| **B2+ D2** (more schemes: EU5G) | 8 | 10 | 12 | 12 | 12 | 1 385 392 | **6** 926 958 |
| **B2+ D3** (more schemes: EUCS, EU5G) | 8 | 12 | 14 | 14 | 14 | 1 590 635 | **7** 953 174 |
| **Operational costs ENISA (without fees)** | | | | | | | **Over 5 years** |
| **B2** | 600 000 | 600 000 | 800 000 | 800 000 | 800 000 | | **3.6** million |
| **B2+ D2** (more schemes: EU5G) | 600 000 | 800 000 | 1 million | 1 million | 1 million | | **4.4** million |
| **B2+ D3** (more schemes: EUCS, EU5G) | 600 000 | 1 million | 1.2 million | 1.2 million | 1.2. million | | **5.2** million |
| **Fee revenues / charges for conformity assessment bodies** | | | | | | | **fees over 5 years** |
| **B2** | 0 | 100 000 | 400 000 | 400 000 | 400 000 | 260 000 | 1 300 000 |
| **B2+ D2** (more schemes: EU5G) | 0 | 100 000 | 400 000 | 400 000 | 700 000 | 320 000 | 1 600 000 |
| **B2+ D3** (more schemes: EUCS, EU5G) | 0 | 100 000 | 400 000 | 400 000 | 800 000 | 340 000 | 1 700 000 |
| **Operational cost ENISA (minus fees)** | | | | | | | **over 5 years (EUR) –** |
| **B2** | | | | | | | 2 300 000 |
| **B2+ D2** (more schemes: EU5G) | | | | | | | 2 800 000 |
| **B2+ D3** (more schemes: EUCS, EU5G) | | | | | | | 3 500 000 |

As under option B1, **certification would remain voluntary under option B2**. If they engage in certification activities, **businesses** would bear costs under existing schemes, the new scheme related to cyber posture or other schemes that could be adopted depending on the scenarios (EU5G and EUCS) in the next five years. The potential costs related to certification have been presented under option B1 and similarly cannot be aggregated. More specifically regarding a **voluntary scheme on the cyber posture of entities**, the following cost estimates for businesses can be provided:

- **Adjustments costs**: costs to meet cybersecurity requirements typically exist for a certification process as explained under B1 and will greatly depend on the size and the maturity of the business. They can be high for a business that has no or low cybersecurity risk management measures in place. Businesses who are in the scope of NIS2, would already have advanced requirements in place, hence marginal.
- **Administrative costs** related to certification costs for organisational security (comparable to ISO 27001) would range in average at **30 000 EUR** one-off and recurrent administrative costs incurred only by businesses that choose to certify (see *Annex 4, section 4.2*), while this can vary greatly. For NIS2 entities the recurrent costs would be similar to audits for the supervision (see option C2). It can be however assumed that additional one-off administrative costs would exist.

- **Fees** related to the maintenance of schemes would occur for conformity assessment bodies as illustrated in the table 7.
- Regarding **public authorities**, even more under the scenario where the scheme would provide demonstration of conformity with NIS2 (**B2 + C2/C3**), it can be assumed that the additional costs on public authorities would be partly offset by the availability of supervisory resources for NIS2 in the BaU scenario. At the same time, Member States might also want to make the scheme available for other entities not falling in NIS2 scope (certain SMEs). Resources would be required to monitor the competence of conformity assessment bodies and supervise additional businesses (not in NIS2). Hence, it seems reasonable to assume an average of **3 FTEs** (instead of 5) of one-off and recurrent and enforcement costs, with an estimate of 56,500 for one FTE, this totals to **4.536.000 EUR** for 27 Member States (27 x 168 000 EUR). Mention should be made that this is a generous estimate assuming that it is likely that all Member States would adopt such a scheme starting to apply in 2030 given the relevance for NIS2 compliance. It is to be noted that for those Member States that have already a national scheme on cyber posture in place, costs would likely be less important as existing resources could be re-allocated.
- The cost estimates related to CABs would be like those indicated under B1.

Table 8: overview of costs for public authorities under Option B.2

| **Option B.2 – FTEs MS (one-off and recurrent costs for 1 MS)** FTE = 56,500 EUR | 2028 | 2029 | 2030 | 2031 | 2032 | **Total costs over 5 years Aggregated for 27 MS** |
|---|---|---|---|---|---|---|
| **Scenario B2** | 0 | 0 | 3 | 3 | 3 | **13** 729 500 |
| **Scenarios B2+ D2** | 0 | 5 | 8 | 8 | 8 | **44** 239 500 |
| **Scenarios B2+ D3** | 0 | 10 | 13 | 13 | 13 | **74** 749 500 |

Under ***Option B.3*** compliance costs would occur for businesses due to selective mandatory certification for all essential entities under NIS2 under the cyber posture scheme (established under B2). Option B.3 envisages the same tasks for **ENISA** as option B.2 and therefore the **compliance costs (recurrent adjustment costs) would remain the same**. Regarding **public authorities**, the costs would be higher compared to option B2 as all essential entities would go through certification and hence supervisory tasks would be more demanding compared to B2. Hence, the assumption is taken that this would require 5 additional FTEs (instead of 3 FTEs under B2).

Table 9: overview of costs for public authorities under Option B.3

| **Option B.3 – FTEs MS (one-off and recurrent costs for 1 MS)** FTE = 56,500 EUR | 2028 | 2029 | 2030 | 2031 | 2032 | **Total costs over 5 years Aggregated for 27 MS** |
|---|---|---|---|---|---|---|
| **Scenario B3** | 0 | 0 | 5 | 5 | 5 | **22** 882 500 |
| **Scenarios B3+ D2** | 0 | 5 | 10 | 10 | 10 | **53** 392 500 |
| **Scenarios B3+ D3** | 0 | 10 | 15 | 15 | 15 | **83** 902 500 |

For **businesses**, the total estimated cost under Option B3 (with C1 or C2) is based on the assumption that mandatory certification would apply to all essential entities falling under NIS2, which is estimated to be sized down to approximately **16 700 essential entities** (*see Annex 4, section 4.3.2*). This would not apply to any SME. Furthermore, regarding the **administrative costs**, as indicated under B2, they would amount to one-off and recurrent of EUR 30 000. Additional **adjustments cost** may occur and would be similar

as described in option C1 and C2 (to meet cyber security risk management measures in line with NIS2). Regarding the recurrent costs, it is assumed that the recurrent adjustment and administrative costs would be similar to those that entities would carry for meeting and demonstrating compliance with NIS2, and hence no additional costs compared to the BaU scenario are considered. On the contrary, as described under option C2, recurrent cost savings would occur. Mandatory certification of NIS2 essential entities would lead to **aggregated one-off administrative costs of EUR 501 million** (30 000 EUR x 16 700 entities). The impacts of such a measure on trade, competitiveness, including indirect costs on citizens as well as on investment and innovation are outlined in the dedicated section.

For CABs, the costs estimates are like those indicated in B1 and B2.

For **citizens**, option B3 may entail additional indirect costs on prices for services and products offered by the relevant essential entities depending on how businesses would choose to compensate the one-off administrative costs. However, considering that no important additional recurrent costs would exist for businesses, the impact is not expected to be significant. Therefore, the costs cannot be estimated.

Table 10: Costs of policy options B (certification)

| Costs | Policy options [Certification] | | |
|---|---|---|---|
| | **B1** | **B2** | **B3** |
| Businesses | + (for certification on voluntary basis)<br>One-off and recurrent adjustment and administrative costs | ++ (with more schemes in place)<br>One-off and recurrent adjustment and administrative costs related to certification<br>**Cyber posture scheme**: 30 000 administrative one-off and recurrent costs by certification (for NIS2 entities: likely only one-off)<br>**Fees for maintenance of schemes over 5 years**: EUR 1.3 million to 1.7 million | • One-off administrative: **501 million EUR**<br>• Over 5 years: **501 million EUR**<br>• **Fees for maintenance of schemes over 5 years** - conformity assessment bodies: EUR 1.3 million to 1.7 million |
| Public authorities | **Over five years: 0 and EUR 61 million** depending on the scenarios for all 27 MS (enforcement costs). | FTEs for new schemes - **Over five years: between EUR 13,7 and 74,7 million** depending on scenarios (one-off and recurrent enforcement costs) for all 27 MS. | **Over five years: between EUR 22,8 and 83,9 million** depending on scenarios (one-off and recurrent enforcement costs) for all 27 MS. |
| ENISA | FTEs for maintenance - **Over five years: EUR 3.8 and EUR 5.9 million** depending on the scenarios (one-off and recurrent adjustment costs)<br><br>Operational costs between **EUR 3 and 4.6 million** (for 3 to 5 schemes)<br><br>**Total adjustment costs (recurrent) over 5 years: EUR 6.8 million to 10.5 million** (for 3 to | **Human resources** for new schemes/maintenance (8 to 14 FTEs) - **Over five years: between EUR 5,9 and 7,9 million** depending on the scenarios (one-off and recurrent adjustment costs)<br><br>**Operational costs** over five years for **4 to six schemes**<br>• Operational costs: **EUR 3.6 to 5.2 million**<br>Also:<br>• Revenues from collected fees from EUR 1.3 million to 1.7 million<br>• Operational costs (minus fees): from EUR 2.3 million to 3.5 million | Same as B2 |

| | | | |
|---|---|---|---|
| | 5 schemes) | **Total adjustment costs** (FTEs and operational recurrent costs) **over 5 years** (without fees)**: EUR 9.5 million to EUR 13.1 million** (for 4 to 6 schemes) | |
| Citizens | 0 | 0 | Possible price increase |

(b) Cost savings for public authorities, citizens and EU institutions related to procedural efficiencies and the likelihood of cybersecurity incidents.

The policy options related to certification would entail different cost savings related to procedural efficiencies and the likelihood of cybersecurity incidents. The cost savings related to internal market effect are outlined in the dedicated section.

Regarding option **B1**, **businesses and public authorities** would benefit from more streamlined and predictable maintenance processes, saving efforts and times in their engagement. In addition, under **option B2**, the time necessary to develop a certification scheme would likely be positively impacted and could be reduced from a current average of 4/4,5 years to potentially 2/2,5 years due to the introduction of deadlines and a clear development plan. This would overall improve **procedural efficiency** for all actors involved, including businesses, public authorities and ENISA.

Furthermore, under option B2, **businesses** would benefit from costs savings related to **reduced market fragmentation** thanks to harmonised European-wide schemes that would gradually replace existing national schemes (*see also Section 6.1.3*). To illustrate this point, taking the example of the future EUCS, there are currently at least four cloud certification schemes introduced by authorities of four of the largest EU Member States[156]. If a company would have to comply only with one scheme instead of four, it could have cost savings of up to 25% related to recurrent administrative costs and likely also adjustment costs (by removing cyber divergent requirements). Regarding the new certification scheme related to the **cyber posture of entities**, the cost savings would be significant if the scheme enables demonstration of conformity with NIS2 as outlined under **policy option C2**.

Furthermore, the adoption of new schemes under B2 and B3 (in combination with D2/D3) would **lower the potential financial impact of cyber-incidents for businesses** by enhancing the cyber resilience of products, processes, services, managed security services and, under B2 and B3, entities. This would indirectly also benefit to citizens, public authorities as well as other businesses as users. By nature, the existence of a certification, including regular audits, would increase the effectiveness of cybersecurity measures and hence decrease the likelihood of incidents of different types and related costs (*see Annex 7*). However, the degree to which a certification would increase the cyber resilience and the potential cost savings due to less likely incidents cannot be quantified in an accurate manner and therefore quantified. This can be corroborated by the indication that **businesses having a cybersecurity certification are likely to benefit from lower cyber insurance costs according to multiple sectoral studies**[157]. Between

[157] For instance, insurances like Embroker, https://www.embroker.com/blog/cyber-insurance-cost/, in the US specify the strength of the security measures as one of the criteria to determine the insurance cost. Other

2023 and 2025 a 15% reduction in the cyber insurance premiums was observed[158], attributed to the verified adoption of cybersecurity best practices by businesses. Such cost savings benefits would be even higher under B2 compared to B1, as more schemes would be in place and under option B3 compared to B2, as mandatory certification would increase the likelihood of businesses meeting state-of-the art cybersecurity measures.

For **CABs** it is reasonable to assume that the costs would be offset by the raise in turnover of such entities from delivering testing and certification activities. The engagement of CABs in activities related to a scheme remain voluntary in all scenarios and hence a business choice.

Table 11: Cost savings of policy options B (certification)

| Cost savings | Policy options [Certification] | | |
|---|---|---|---|
| | **B1** | **B2** | **B3** |
| Businesses | Procedural efficiency: +<br>Reduced cyber incident costs: 0/+ (D2,3)<br>Reduced market fragmentation: 0/+ (D2,3) | ++<br>+/++ (D2,3)<br>+/++ (D2,3) | ++<br>++/+++ (D2,3)<br>+/++ (D2,3) |
| Business total | 0/+<br>+ (D2,3) | +<br>++ (D2,3) | ++<br>+++ (D2,3) |
| Public authorities | Procedural efficiency: +<br>Reduced cyber incident costs: 0/+ | ++<br>+/++ (D2,3) | ++<br>+/++ (D2,3) |
| Citizens | Reduced cyber incident costs: + | ++ | +++ |
| ENISA | Procedural efficiency: + | ++ | ++ |

#### *6.1.1.3.*Simplification (Policy Options C.1 to C.3)

##### (a) Compliance costs

Under ***Option C.1***, the adoption of relevant implementing regulations might add to the fact that NIS2 entities will incur minimal **one-off adjustment** costs depending on the degree to which Member States have adopted detailed rules specifying the NIS2 requirements. It can be assumed that these costs would be covered by the estimated average cost of about EUR 94 355 per year that entities already bear to comply with NIS2 obligations (*see Annex 4, sections 4.3.1 and 4.3.2*).[159] Adjustment costs might also occur due to the implementation of guidelines. Regarding the guidelines related to ransomware reporting, additional one-off adjustment costs may occur in case Member States implement these guidelines in a legally binding way as businesses will have to adapt their reporting processes. As the implementation of these measures would vary across Member States and are of voluntary nature, it is not possible to provide any aggregated figures. The guidelines to clarify the NIS2 scope as well as the guidelines for suppliers to NIS2 entities are not expected to lead to any compliance costs. For **Member States**, **one-off**

---

insurers like Marsh, https://www.marsh.com/en/services/cyber-risk/expertise/cyber-self-assessment.html, active in the EU, provide detailed cyber risk assessment procedures and criteria – including organisation security control measures and details - in order to provide cyber insurances and correctly estimate the premium based on cybersecurity maturity compared to peer businesses, https://affinity.marsh.com/cyber-accelerate/application-requirements.html.

[158] Howden. *2024 Cyber insurance - Risk, resilience and relevance*, https://www.howdengroupholdings.com/sites/default/files/2024-06/howden-2024-cyber-report.pdf.

[159] As indicated in Annex 4, the average salary of a cybersecurity specialisation professional in Europe is EUR 56 500. Further explanations related to this calculation are provided in Annex 4.

**adjustment costs** would occur for updating the training of personnel in charge of supervision and enforcement of NIS2 entities in relation to the guidelines. It can be assumed that these costs are covered by the existing spending for training of staff. **ENISA** would not bear any compliance costs linked to option C.1. No costs would impact **citizens**.

The compliance costs for **NIS2 entities** and **Member States** under **option C.2** are comparable to option C.1 concerning the adjustment costs in case of implementing acts. Minimal **one-off compliance costs** would occur where an implementing act on incident reporting requires additional information in case of **ransomware attacks** to adapt reporting processes. Concerning the guidelines for suppliers to NIS2 entities, like in option C.1, no additional compliance costs are expected. While costs related to using a certification to demonstrate compliance with NIS2 are explained in option B.2, the possibility to acquire a **cyber posture certification** to demonstrate compliance with NIS2 on a voluntary basis would not lead to any additional costs in terms of compliance. The costs for **Member States** in regard to cyber posture certification is explained in option B.2 based on the assumption that all Member States will implement it. Regarding **ENISA**, additional costs for human resources with the need for minimum 4 additional FTEs would incur following its new role in assisting Member State in the supervision of multi-country entities under option C.2. These costs are described in A.2.

Concerning the **clarification and reduction of scope**, no additional cost are expected. Instead, significant savings would occur, as explained in the next section. However, given the fact that those entities would no longer be covered by NIS2 and/or subject to a different regime, this may impact their cybersecurity risk management measures over time, hence leading to **higher costs related to cybersecurity incidents** (*see Annex 7*). It is however not possible to provide any quantitative estimation in this regard. Those costs would also apply under C3.

**Option C.3** would introduce **one-off adjustment costs** for **businesses,** which would be required to adapt to a new legal framework, revise internal policies and procedures regarding obligations and cybersecurity risk-management measures, as well as provide new guidance to personnel. It is expected that, following the clarifications of definitions and scope, at least the **181 700 entities** falling under the scope of NIS2 and DORA[160] would need an **additional 0.5 FTE for this transition**, resulting in a total **one-off aggregated cost of EUR 5.2 billion** for businesses in Europe. If these transition adaptations were to be applied only by the ca. 22 000 financial institutions under DORA, this transition would result in a total one-off aggregated cost of **EUR 627 million**. At the same time, these would be offset by significant longer-term savings, as explained in the following section. Regarding ransomware reporting and questionnaires for NIS2 entities' suppliers, the same considerations apply as under Option C.2: no significant one-off adjustment costs are expected. Regarding **ENISA**, additional costs for assisting Member State in the supervision of multi-country entities would occur as in option C.2. For **Member States**, one-off adjustment costs would occur for training new or updating the training of personnel in charge of supervision and enforcement of the respective legal acts. Under the assumption that a training may cost EUR 600 (*see Annex 4, section 4.3.4*)

[160] 159 700 NIS2 entities [188 000 NIS2 entities minus 28 700 entities following the NIS2 scope clarifications] and 22 000 DORA entities, see https://www.pwc.com/mt/en/services/pwc-digital-services/cyber-security-and-privacy/cyber-security-services/dora.html.

and an average of 10 staff per Member State, an estimate total **one-off cost of EUR 162.000** would occur. **Citizens** would not bear costs linked to option C.3.

Table 12: Compliance costs of policy options C (simplification)

| Compliance costs | Policy options [Simplification] | | |
|---|---|---|---|
| | C1 | C2 | C3 |
| Businesses | Minor One-off adjustment costs 0/- | • Minor One-off adjustments costs > C1 (new measures) | • One-off: Adjustments costs (one-off - **EUR 5.2 billion)** |
| Public authorities | Minor One-off adjustment costs (training) | one-off and recurrent adjustments costs > C1 | • **EUR 162.000** Adjustments costs (one-off) for training |
| Citizens | 0 | 0 | 0 |
| ENISA | 0 | One-off and recurrent adjustment costs (see option A.2) | Same as in C2 (see option A2) |

(b) Administrative cost savings for businesses, including SMEs, and public authorities

Under **option C.1**, **NIS2 entities** that are subject to different national cybersecurity risk-management frameworks in transposition of the NIS2 Directive would benefit from a higher degree of harmonisation through implementing acts, reducing the administrative costs for these entities likely offsetting the one-off adjustment costs. Guidelines on scope, ransomware reporting, and suppliers would not lead to major direct benefits NIS2 entities and are not expected to meaningfully improve legal certainty and mitigate costs related to market fragmentation for their suppliers. For **Member States**, there would be no direct benefits deriving from the measures under option C.1.

**Option C.2** would reduce the number of entities in **scope** of the NIS2 Directive by approximately **6 200 DNS service providers**.[161] Moreover, after clarification on definitions and the types of entities referred to in Annex I and II, the NIS2 Directive would no longer apply to an estimated number of **22 500 entities**. This would diminish the compliance costs (adjustment and administrative costs) of average EUR 94 355 per year for these entities, summing up to EUR 2.7 billion per year, **totalling 13.5 bn EUR of total cost savings (adjustments and administrative costs savings)** over a period of five years (*see Annex 4, section 4.3.3*). Under the assumption that the administrative costs would amount to 10% of the compliance costs of average of EUR 94 355, **administrative cost savings would amount to EUR 270 million** per year, totalling to **EUR 1.35 bn** over five years.

In addition, introducing the new category of **small mid-caps** in the NIS2 Directive will address around **22 500 businesses** that fall under the small mid-caps classification (*see Annex 4*). These entities currently qualify as essential and would become important entities, which should not be required to systematically document compliance with cybersecurity risk-management measures. The designation of small mid-cap sized enterprises as important entities will therefore **reduce recurrent administrative compliance costs** for those entities. Under the assumption that these entities could save

[161] The estimation of the number of affected DNS service providers and number of entities affected by clarifying and the definitions and types of entities is based on an extrapolation of the number of essential and important entities that Member States notified the Commission of pursuant to Article 3(5) of the NIS 2 Directive as of October 2025.

10% of the compliance costs (administrative costs) of average EUR 94 355 per year (*see Annex 4*), this would amount to **EUR 212 million per year** (*see Annex 4, section 4.3.3*), totalling **1,06 bn EUR over five years**.

For **Member States' authorities**, it can be estimated that they need one FTE less per Member State due to the reduction of entities in scope and under ex ante supervision. Assuming one FTE less per year with an average salary of EUR 56 500, this would lead to EUR 1,5 million of recurrent administrative savings for all Member States per year, totalling **EUR 7.5 million cost savings over five years**.

Further, under option C.2, the ECCF could be leveraged to demonstrate compliance with the obligations to implement cybersecurity risk-management measures under the NIS2 Directive, and possibly other relevant Union legal acts. This would allow entities that operate cross-border and are therefore subject to different national supervision systems as well as entities possibly subject to cybersecurity risk-management obligations stemming from several relevant Union legal acts to demonstrate compliance only once. A cybersecurity audit would cost in average of 30.000 EUR. It is assumed that a cyber posture certification would lead to similar recurrent administrative costs of EUR 30.000 and that one-off adjustment costs would not be significant[162], and that at least **3% of essential and important NIS2 (ca. 5000 companies)**[163] are subject to at least two supervision frameworks and would make use of the cyber posture certification. Considering the simplification potential and attractiveness of the certification scheme, it is expected that certificates would be issued as of 2032 (scheme adopted in 2030 followed by a one-year transition period, including for the notification of CABs). Taking a gradual approach of 1000 certificates issued per year as of 2032, this could lead to cutting administrative costs by half for those entities, leading to **administrative cost savings of at least EUR 30 million per year** taking into account 1000 entities, and over the period considered in this report (2028-2032)(*see Annex 4, section 4.3.3*). Those cost savings would be increased for NIS2 entities operating under more than two supervision frameworks. Concerning **Member States' authorities**, demonstration of compliance by entities could streamline supervisory activities, decreasing the need for extensive manual checks and assessments. However, given the limited availability of detailed data on inspection efforts and budgets, accurately quantifying the potential savings for these authorities is not possible.

In summary for businesses, the measures proposed would lead to **EUR 14.6 billion administrative cost savings over five years.** For Member States, cost savings would be at least of **EUR 7.5 million cost savings** over the same period.

**Option C.3** would ensure that all cybersecurity risk-management obligations are governed by common definitions, requirements, timelines and templates, reducing legal fragmentation and significantly easing compliance burden across sectors. A unified framework for cybersecurity risk-management measures would **cut compliance costs** for

---

[162] Entities that would be important and essential entities that have a strong incentive to certify would be those having cross-border activities and/or covered by an ex-ante supervision regime under NIS2, hence they are expected to already have strong cybersecurity risk management measures in place. Sectors would include: manufacturing, digital service providers, transport.

[163] Calculated from 159 300 NIS2 entities which are 188 000 NIS2 entities minus 28 700 entities following the NIS2 scope clarifications.

entities by reducing the time needed to manage compliance with multiple legislative instruments. Assuming that an entity subject to the NIS2 Directive is in the scope of one other regulatory instrument, such as the GDPR, whose provisions on data security would be brought into the NIS2 framework, at least **159 300 entities** across the Union would benefit from monitoring compliance for only one regulatory obligation applicable to them. Further assuming that the change results in annual savings of 0.5 FTE of work per entity, the resulting savings for entities across the Union would be **EUR 4.5 billion** per year, in addition to the benefits under option C.2, leading to a total of **EUR 37.1 bn compliance cost savings**.

Like for businesses, Member States would benefit as they only have to supervise one set of cybersecurity rules (even for a larger number of entities). It can be estimated that authorities **need two FTE** less per Member State, amounting to **EUR 3 million in recurrent administrative savings per year, totalling to EUR 15 million over five years**.[164] The cost savings due to mandatory reporting of ransomware attacks would be higher under C3 as it would cover more entities.

c) Cost savings related to reduced cyber incidents

Under option C2, harmonising and improving the **collection of data on ransomware attacks,** in particular reports on any ransom payments made and on ransom payments that entities intend to make, paired with other relevant information, will provide insights to CSIRTs and national authorities which allow them to ensure any future ransomware interventions are appropriate and effective, support entities in growing their resilience and preventing future attacks, and compile the intelligence and evidence that law enforcement agencies need to disrupt and dismantle ransomware gangs and sanction their operatives. These measures would lead to prevention and faster detection of ransomware attacks, hence contribute to reduce the number of successful ransomware incidents leading to **cost savings for businesses and public authorities** (*see Annex 7*). Currently, the median ransom payment in Europe ranges between USD 0.2M and 2M (*Table 19 in Annex 7*) with only 55% of entities paying less than the requested ransom (*Table 26 in Annex 7).* Reporting on payments may indirectly lead to reducing ransom payments. At the same time, considering that several entities are taken out of the scope of the NIS2 Directive, these cost savings might be lowered. Hence, it is not possible to provide any quantitative estimation.

Table 13: Benefits of policy options C (simplification)

| Benefits | Policy options [Simplification] | | |
|---|---|---|---|
| | C1 | C2 | C3 |
| Businesses | + | **Total compliance cost savings (administrative and adjustment) over 5 years of EUR 14.6 billion** (including one-off and recurrent)<br>- Reduction of scope: EUR 2.7 billion per year = EUR 13.5 billion over 5 years (of which EUR 1.35 billion in recurrent administrative costs)<br>- Essential to important entities: | **Total compliance costs savings over 5 years of EUR 37.1 bn** (including one-off and recurring)<br>- Reduction of scope: EUR 2.7 billion per year = EUR 13.5 billion over 5 years (of which EUR 1.35 billion in administrative costs)<br>- Essential to important entities: EUR 212 million per year = EUR 1.06 billion over 5 years (recurrent administrative cost savings) |

[164] Average fully loaded FTE cost of 56 500 per year multiplied by two (for two FTE) by 27 (Member States).

| | | | |
|---|---|---|---|
| | | EUR 212 million per year = EUR 1.06 billion over 5 years (recurrent administrative cost savings)<br>- Use of cyber posture scheme for NIS2 compliance: EUR 30 million per year as of 2032 and over 5 years considered in this report (recurrent administrative cost savings)<br><br>Cost savings due to **reduced ransomware attacks 0/+** | - Use of cyber posture scheme for NIS2 compliance: EUR 30 million per year as of 2032 and over 5 years considered in this report (recurrent administrative cost savings)<br>- Savings from a consolidated framework: EUR 4.5 billion per year = EUR 22.5 billion over 5 years (recurrent compliance cost savings, including administrative and adjustment costs)<br><br>Cost savings due to **reduced ransomware attacks** > C2 0/+ |
| Public authorities | 0 | EUR 1,5 million per year = EUR 7,5 million over 5 years (due to scope changes) of enforcement costs savings (recurrent) | EUR 3 million per year = EUR 15 million over 5 years of enforcement costs savings (recurrent) |
| Citizens | 0 | 0/+ (reporting of ransom payments) | 0/+ (reporting of ransom payments) |
| ENISA | 0 | 0 | 0 |

6.1.1.4.ICT supply chain security (Policy Options D.1 to D.3)

(a) Compliance costs for businesses, public authorities and citizens

Measures related to ICT supply chain restrictions involve direct and indirect costs for **businesses** across sectors which deploy restricted ICT technologies and/or include them in their supply chains. These costs typically include as direct costs, replacing the hardware and buying new equipment, installation and integration, decommissioning, and software updates, as well as indirect cost, retraining staff to use the new equipment and ensuring interoperability with the legacy system. **Public authorities** would carry costs related to conducting risk assessments and supervision, as well as ICT users.

**Option D.1** would entail the use of soft law measures related to ICT supply chain security within the existing EU regulatory framework (NIS2). New coordinated risk assessments and toolboxes beyond 5G networks, would lead to **additional costs for businesses if Member States decide to implement restrictions recommended in the toolboxes** (scanning equipment, submarine cables, and electricity supply being potential topics for the first toolboxes). Each Member State could independently decide to designate high-risk suppliers and restrict certain assets from those suppliers (following the example of 5G). This would lead to **offsetting and transactions costs** for relevant economic operators to make necessary changes in their supply chain. For businesses having cross-border activities, additional **familiarisation costs** could stem from the fact that the measures may not be the same in each Member State. These costs would be one-off. Regarding 5G suppliers across the EU, the costs would not change compared to the BaU scenario.

Regarding the **costs for public authorities**, including Member States and EU institutions and agencies, in particular ENISA, option D.1 would mostly cover their involvement in conducting the additional EU coordinated risk assessments and recommending mitigation measures (toolboxes). Whilst the NIS Cooperation Group already performs coordinated supply chain cybersecurity risk assessments, compared to the business-as-usual where risk assessments would be continued, pursuing additional toolboxes for each risk assessment would entail **recurrent additional costs for national authorities**. Assuming that twenty-five experts participate in carrying out a risk assessment or toolbox, and that 20% of each expert's staff time over a period of six months is invested in the risk

assessment or toolbox, **each additional toolbox** would cost approximately **EUR 141 250** in staff time. In the next five years, it is reasonable to assume that there would be between 5 and 8 risk assessments and toolboxes adopted. This would amount to one risk assessment (BaU) and toolbox being developed per year as a minimum.

Option D.1 could entail **additional indirect costs for citizens** in terms of prices increases depending on the assets that are restricted and the implementation of the relevant toolboxes at national level. Hence, it is not possible to give any quantified estimates.

**Option D.2** would make requirements of the 5G Toolbox binding throughout the EU, with the same scope of applications of restrictions on high-risk suppliers in all Member States.

This option would have varied impact across **Member States**, depending on their reliance on high-risk suppliers in the 5G networks and whether they have properly implemented restrictions on them. Member States can be classified in different categories:

- Member States which have enacted restrictions on high-risk suppliers, covering all the key assets as recommended in the 5G Toolbox;
- Member States which have enacted restrictions on high-risk suppliers, but which are not or only partially covering the key assets;
- Member States which have not enacted any restrictions on high-risk suppliers but are still highly dependent on them in their 5G networks;
- Member States which have not enacted any restrictions on high-risk suppliers, but which have no high-risk supplier in their network.

The impacts on **businesses, public authorities and citizens** would therefore vary across Member States. The impact will be neutral on Member States which have already enacted restrictions covering the key assets as recommended in the 5G Toolbox, while it would be higher for Member States with no restrictions yet or not covering all key assets.

Studies have shown that a large number of Member States are highly dependent on high-risk suppliers, in particular eleven Member States have an over 40% share of high-risk suppliers in their 5G radio access network[165]. More recent estimates suggest that this share has slightly decrease in the past years and could be in average around 32%[166] (*Annex 4*).

For **businesses**, and in particular mobile network operators, this would entail direct and indirect **substitution and transaction costs** for replacing relevant 5G equipment coming from high-risk suppliers throughout the EU with comparable alternative, excluding the natural network modernisation costs. According to the available sources, it is estimated that 41% of the mobile subscribers in Europe have access to 5G RAN provided by one of the high-risk suppliers[167].

Based on available data from the 5G Observatory on investments in 5G RAN and core network equipment, and assuming a transition period of **three years**, it is estimated that

---

[165] Strand Consult, *The Market for 5G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 31 European Countries*, https://strandconsult.dk/the-market-for-5g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-31-european-countries/.
[166] https://www.lightreading.com/5g/huawei-has-hardly-been-weakened-in-european-5g-data-shows
[167] Ibid.

the **one-off cost** of replacement of the equipment coming from the high-risk suppliers[168] could amount to **EUR 3.4 bn to EUR 4.3 bn** for the non-upgradeable equipment[169] per year over three years (taking into account the BaU factor of 10 to 15% annual replacement). These costs would entail the costs of decommissioning the equipment from high-risk equipment (both hardware and software), the acquisition of new equipment from trusted suppliers, and the human resources to perform the replacement (see *Annex 4 section 4.4.1*). Estimations of costs were derived considering investments that were made in the EU for 5G non-standalone and standalone deployment since 2019. The share of high-risk assets is considered 40% to 32% of the total assets, of which 30 to 45 % of the equipment would have to be replaced over three years considering the technology cycles as explained in *Annex 4 section 4.4.1* when taking the assumption that 10-15% of equipment would be replaced on a yearly basis.

The mobile network operators might decide to transfer (fully or partly) these costs to the consumers as one possible strategy of network operators[170]. If so, this could amount to maximum **EUR 6.5 to EUR 8.3 per mobile subscriber** over three years (if the costs are fully transferred)[171], which could be reflected in the price of mobile subscriptions (see *Annex 4 section 4.4.2*). However, it is to be noted that that there is limited evidence as to whether such a price increase would take place. One report[172] estimates that such price increases would be limited.

The high reliance explains the high costs of replacement of the 5G equipment from high-risk suppliers. To compensate these costs, entities affected by restrictions on high-risk suppliers will have a transition period to phase out the risky equipment. These transition periods will be determined through the market analysis and takes into account the lifecycle of the equipment, to ensure the proportionality of the measures. Furthermore, looking at the overall economy, those short-term costs will be alleviated by new revenues created for trusted suppliers and a more trustworthy offerings for citizens (see *point a)* and *section 6.1.4 and section 6.2*).

The **compliance costs for public authorities** of option D.2 would depend on whether or not the Member States have already enacted restrictions on high-risk suppliers in 5G networks, and its level of dependency on high-risk suppliers in its telecommunications network. For example, a Member State which has already put in place restrictions on high-risk suppliers for all key assets of a 5G network, as recommended in the Toolbox, or a Member State which only has trusted suppliers in its telecommunications networks will

---

[168] C(2023) 4049 final.

[169] The non-upgradable equipment refers to 5G non-standalone equipment, i.e a 5G radio access network built on top of an existing 4G core network, both coming from the same supplier. Replacing this equipment requires replacing both the 5G RAN and 4G core. *A contrario*, a 5G standalone network means that both the RAN and the core are 5G equipment coming from the same supplier. According to GSMA, only 1.3% of the 5G coverage in the EU is 5G standalone by Q2 2025, meaning that 98.7% is non-standalone (GSMA, 5G Coverage in Europe: Progress Toward Goals Amid Lingering Disparities, 2025).

[170] Such a strategy has for instance been discussed in the context of the network cost contribution debate, see : European Parliamentary Research Service, Network cost contribution debate, at a glance, April 2023, available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745710/EPRS_ATA(2023)745710_EN.pdf

[171] Ibid., 85% of the population in Europe (465 million people) subscribed to mobile services in 2019. According to GSMA (GSMA, the mobile economy Europe 2025), there were 520 million mobile subscribers in 2025.

[172] Strand Consult, Ibid.

have no additional cost. On the contrary, a Member State which has not yet implemented restrictions as recommended in the 5G Toolbox and is dependent on such suppliers will face compliance costs, covering implementation of measures and their supervision.

As for **EU institutions**, there would be no additional compliance costs as it would be the continuation of the monitoring of the 5G Toolbox implementation as done today.

**Option D.3** would provide for a comprehensive framework for ICT supply chain security (*see Section 5.2*). In addition, this option would already include the identification of key assets in relation to 5G networks, in line with option D.2. The related costs would therefore be the same as presented for option D.2.

While the establishment of the framework would not involve any costs, its actual implementation and operation with regard to a specific asset beyond 5G networks would likely involve significant costs for **businesses** that may be required to phase out specific assets, similar as identified under option D.2 for 5G networks. These costs would be one-off and would also be reflected in the increased price paid by **customers** for specific products, as for 5G networks under option D.2. At this stage, in the absence of detailed assessments of assets beyond 5G, such costs cannot be fully estimated, as they will depend on the assets assessed, the cost of replacement and the transition period established for the implementation of measures. It is therefore necessary to assess these costs and benefits as part of the implementation of the framework. Such an assessment would also be necessary to ensure that mitigating measures also reflect the market reality, and will include an assessment of economic feasibility, available alternatives, lifecycle of products, ensuring proportionality and necessity of adopted measures. The methodology is further explained under the *section 5.2*.

Regarding costs for **public authorities and EU institutions**, option D.3 would require additional staffing at both national and European level to implement the supervisory tasks related to the application of restrictive security measures. Those would be proportionate to the number of sectors gradually covered; hence no specific estimation can be made at this stage. An impact analysis would precede any potential triggering of the empowerment to apply such mitigating restrictive measures. In addition, under this option additional staffing should be taken into account for the Commission for supporting Member States' supervision activities regarding assessment of corporate ownership structures and establishing the list of subsidiaries of high-risk suppliers.

The broader costs related to **market access, competitiveness and innovation** are in the dedicated section (*section 6.1.4*).

Table 14: Costs of policy options D (supply chain)

| COSTS | Policy options [Supply chain] | | |
|---|---|---|---|
| | **D1** | **D2** | **D3** |
| **Businesses** | • Costs to adjust to measures adopted by Member States<br>• Familiarisation costs for businesses with cross-border activities | Substitution and transaction costs for replacing 5G equipment: **EUR 3.4 to 4.3 bn per year for three years** (one-off cost of replacement of the 5G equipment – adjustment costs) | Higher than for D2, in addition to costs to phase out specific assets in other ICT supply chains<br><br>For 5G: **EUR 3.4 to 4.3 bn per year for three years** (on-off cost of replacement of the 5G equipment – adjustment costs) |
| **Public authorities** | EUR 141 250 in staff time to conduct multiple coordinated risk assessments and toolboxes / per year | Will vary across each Member State: Compliance costs would occur for the Member States which have not implemented the 5G | D1+D2 + Additional staffing to implement the supervisory tasks related to the application of restrictions on high-risk suppliers |

| | | | |
|---|---|---|---|
| | (assuming five exercises in total) | Toolbox | |
| **Citizens** | Neutral | If transfer of costs (unlikely scenario): EUR 6.5 to EUR 8.3 per mobile subscriber per year over three years | Same as for D2, in addition to costs to phase out specific assets in other ICT supply chains to be outsourced to customers<br><br>For 5G: If transfer of costs (unlikely scenario): EUR 6.5 to EUR 8.3 per mobile subscriber per year over three years |

6.1.1.5. Cost savings of ICT supply chain options

**Options D** will lead cost savings related to **internal market effects**, especially for **businesses.** While under **D.1**, the measures recommended at EU level would remain non-binding under **option D.2 and D.3**, cost savings for businesses could exist related to reduced market fragmentation (being higher under D.3 and in particular in the area of 5G under D.2). In particular, businesses having cross-border activities would have the same set of requirements across Member States, which would entail less administrative burden for them to comply to different rules in each Member State. Those benefits are analysed in more details in *section 6.1.3*.

Furthermore, options D would be linked with broader benefits that are analysed in more details in *sections 6.1.4 and sections 6.2.* Benefits would exist especially in qualitative terms for all categories of stakeholders (citizens, businesses and public authorities) as ICT users as it would **reduce cybersecurity risks stemming from reliance on high-risk suppliers** and improve the level of resilience of critical infrastructure and contribute to strengthen the overall resilience of our economy and society (these impacts are *see Section 6.2*). Those benefits would be the highest under D3, followed by D2 and D1.

Furthermore, while there will be short-term costs related to substitution of assets for companies that have assets provided by untrusted suppliers, **new revenues** will be created by **trusted suppliers** stimulating investments in R&D and hence innovation and competitiveness. Those benefits are analysed in more details in *Section 6.1.4.* Based on the known value of annual investments in key assets (5G RAN and core networks), and assuming that 32% of the investments would go to untrusted suppliers under business as usual, the value created for trusted suppliers, could amount to EUR **2 bn per year** during the three years transition period and beyond as these market shares would be retained by trusted suppliers (See *Annex 4 section 4.4.3).* In comparison with the costs for replacing untrusted equipment, this represents an overall net benefit for the economy and enhanced cyber resilience. For example, a European MNO has recently renewed its contract with a high-risk supplier to supply equipment for its 5G core network for five more years in a Member State. The restrictions on high-risk suppliers under option D.3 would give the opportunity for trusted suppliers to win such a contract. A report[173] analyses the fact that the phasing out of untrusted suppliers in certain regions of the world have led to the increase of market shares of trusted suppliers.

Table 15: Cost savings of policy options D (supply chain)

| **COST SAVINGS** | **Policy options [Supply chain]** | | |
|---|---|---|---|
| | **D1** | **D2** | **D3** |
| **Businesses** | Limited | • Stimulating new market opportunities: **EUR 2bn EUR per year** (recurrent | > D2 |

[173] Strand Consult, Ibid.

| | | | |
|---|---|---|---|
| | | benefits) during the 3-years transition period and beyond<br>• Increased cyber resilience<br>• Internal market | |
| **Public authorities** | Depending on MS | • Trusted offering (as ICT user) | > D2 |
| **Citizens** | Depending on MS | • Trusted offering (as ICT user) | > D2 |

#### 6.1.2. *Impact on SMEs*

SMEs are particularly vulnerable to cybersecurity incidents (*see Section 2*). Examples included in *Annex 7* illustrate the possible impacts of cybersecurity incidents on SMEs. SMEs, due to their limited resources are likely to be more impacted by cybersecurity attacks and might be a specific target for malicious actors[174]. Hence, SMEs are expected to benefit even more, compared to large companies, from an enhanced role of ENISA, well-functioning ECCF and ICT supply chain security measures. They are expected to gain cost savings due to a more harmonised implementation and streamlined scope of NIS2.

Under **options A (1 to 3)**, the different policy options would generally have a positive role on SMEs who would benefit from increased cyber resilience due to an enhanced role of ENISA. Furthermore, SMEs impacted by European cybersecurity legislation, such as the CRA, will benefit from the increased involvement of ENISA in providing support and technical guidance. Thanks to the European individual cybersecurity skills attestation schemes, an SME as provider of cybersecurity attestations will gain visibility, reputation and gain customers by being part of the scheme (see also *section 6.1.1.1(b)*). Furthermore, it will support SMEs in identifying candidates with the right skillset. Lastly, the initial application fee will be levied in two steps to minimise the risk of barrier to entry for SMEs: the first part of the fee will be levied for the examination of eligibility and processing of applications to becoming an authorised attestation provider and the second part of the fee will be levied when issuing and renewing authorisations to providers of European individual cybersecurity attestations, including audits.

Under **options B 1 and 2**, a well-functioning ECCF and European certification schemes can ease the choice of trusted ICT technologies for SMEs and contribute to enhance their overall cyber resilience. SMEs as vendors applying to certification will benefit even more from the harmonised effect of European schemes as they have less resources to cope with market fragmentation. The costs applicable to vendors can be partly alleviated by the obligation of conformity assessment bodies to apply proportionate fees foreseen under the ECCF. The mandatory certification under **B3** would not affect SMEs as they cannot be essential entities.

SMEs will benefit from measures related to the implementation of the NIS Directive (**options C**). As DNS vendors, they would benefit from cost savings under **option C2 and C3** due to the exclusions from the scope of DNS providers. Furthermore, they would benefit from the scope clarifications that would limit the application of the obligations to

[174] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024, see example of Dark Angels ransomware group on page 54.

companies that have core activities of the sectors listed in NIS2. As previously mentioned, also under option C, increased harmonisation will benefit even more SMEs in the scope of the Directive.

For ICT supply chain security measures (**Options D**), SMEs would benefit from the use of trusted technologies. As suppliers active in the sectors subject to restrictions, they would be impacted more heavily compared to larger companies by substitutions and transactions cost. Under option D3, such impacts would be part of the methodology for the assessment. At the same time, SMEs as trusted suppliers will benefit from new market opportunities.

#### 6.1.3. *Functioning of the internal market*

The impact on the internal market depends on how effective the regulatory framework is in preventing the emergence of obstacles and fragmentation by national initiatives aiming to address the problems set.

The internal market impact of **Options A** is indirect. In particular A2 and A3, related to the ENISA mandate, would have a positive impact on the internal market by granting ENISA a more effective role on support to the implementation of Union legislation. The European skills attestation scheme, while not introducing a direct harmonisation effect, could reduce market fragmentation and be gradually recognised as a reference by Member States.

A more effective functioning of the ECCF (**options B**) will have a direct impact on reducing and preventing market fragmentation as European schemes have a direct harmonisation effect on national schemes. The internal market effect will be higher as its scope is extended under option B2 (to the cyber posture of entities) and if more schemes are adopted (see links between options B and D2 and D3 and the adoption of EU5G and/or EUCS).

Under **options C**, the internal market effect will be the strongest with C3 followed by C2 and C1. Under C1, the adoption of implementing acts under the NIS 2 Directive would maximise the available tools under the existing empowerments to achieve a coherent set of rules for essential and important entities, contributing to a more level playing field across the internal market. However, Member States would still be able to maintain and introduce additional national requirements (minimum harmonisation). **Option C.2** will help further reduce the impact of obligations coming from the NIS 2 Directive, diminishing the remaining burden stemming from currently diverging implementation by introducing maximum harmonisation of implementing acts. This option aims to enhance interoperability, improve legal certainty, and facilitate compliance across Member States. C3 would provide full harmonisation.

Regarding ICT supply chain measures, the internal market effect would be the strongest under D3 followed by D2 and D1. **Option D.1** would likely maintain the current fragmentation in the internal market, as the mitigating measures resulting from the different toolboxes would remain non-binding. This would lead to measures in one Member State that are not applicable in another one, also negatively impacting businesses that have cross-border activities. **Option D.2** would have a positive impact on the internal market in the field of 5G, as restrictions on high-risk suppliers would be harmonised throughout the EU. **Option D.3** would have a positive impact on the internal market in the field of 5G and other ICT supply chains. Restrictions on entities established in or controlled by entities from countries posing cybersecurity concerns (high-risk suppliers)

in key ICT assets for specific ICT supply chains would be the same in all Member States. This would also facilitate business for cross-border entities.

#### 6.1.4. *Impact on trade, competitiveness and innovation: impact on EU and non-EU companies*

This section explores the four aspects of **competitiveness** regarding **(i)** cost and price, **(ii)** international competitiveness, **(iii)** capacity to innovate and **(iv)** competitiveness of SMEs. The most significant impacts would stem from options D related to ICT supply chain security.

Reforming ENISA's mandate (**Options A)** is not expected to have significant **impacts on market and trade** patterns. Under option A.3, the expansion of ENISA's mandate to the direct operational support to NIS 2 entities would mean that ENISA is active in providing services that are also offered by managed security service providers (MSSPs). However, given that a Member State need to request ENISA's support for incident response, it is not expected that the change will have a noteworthy effect on the demand for services from private MSSPs. Furthermore, **option A2 and A3** are expected to have a positive impact on the EU industrial ecosystem, its innovation potential and international reputation and competitiveness. An enhanced ENISA mandate will contribute to enhancing the cyber resilience of businesses and positively contribute to education and training in cybersecurity. The European skills attestation schemes is expected to lower the price of skills certifications, including by increasing the offering on the market. New providers would gain visibility in a market which is currently dominated by a few providers, which would foster competition and innovation. This will particularly benefit SMEs as outlined in *section 6.1.1*. A stronger engagement of ENISA in standardisation (A2 and A3) will foster competitiveness of European companies by promoting alignment between international and European standards. ENISA would contribute to foster timely and state-of-the-art European standards supporting the CRA and ECCF ensuring the adoption of more advanced standards compared to competitors. High quality standards will also contribute to innovation in cybersecurity.

Under **Options B1 and B2**, certification would remain voluntary. An efficient and well-functioning ECCF will foster a competitive and innovative European cybersecurity testing ecosystem by promoting state-of-the art cybersecurity requirements and evaluation methodologies. In the area of product security certification, the European Union is hosting some of the most competitive testing laboratories[175] attracting customers worldwide. An enhanced ECCF would strengthen Europe's competitive advantage and create a market for cybersecurity ICT suppliers. New market opportunities would be created thanks to increased consumer trust in certified ICT solutions. The demand for certifications (for instance in public procurement processes) could favour certified European vendors. However, since such schemes would be developed considering international standards, they would not disadvantage per se non-European companies. The ECCF would contribute to strengthen the reputation of European vendors, including SMEs, in the European Union and globally. Under a voluntary setting, as certification remains a business choice, the impacts of costs transferred to consumer prices are not expected to be significant.

[175] JTSEC, *2022 Common Criteria Statistics Report*, https://www.jtsec.es/files/2022_CC_Statistics_Report.pdf.

On the contrary, mandatory certification of NIS2 essential entities envisaged under **Option B.3** may lead to direct negative effects on competitiveness and prices but is not expected to be significant. The mandatory certification would involve compliance costs for essential entities, which they could transfer to consumers, resulting in higher end-user prices in key sectors such as relating to energy or ICT infrastructure services. Being subject to mandatory certification may in general also have a negative impact on essential entities' ability to innovate, which may be more significant in high-technology sectors such as relating to digital infrastructure. However, the impact is not expected to lead to significant market distortions. The impact on SMEs would be limited as NIS2 only applies to enterprises that include or exceed the ceiling of medium-sized enterprises (see options C). Additionally, essential entities are currently already subject to the NIS2 ex ante supervision regime and are thus already capable to manage and demonstrate compliance with legislative requirements on cybersecurity. Likewise, the absolute costs relating to mandatory certification would not expect to have a major impact on the competitiveness of essential entities as they would apply to all entities in those sectors, including non-EU competitors that want to be active on the EU market. Considering the likely positive impact of the mandatory certification on the cyber posture of covered entities, this option will likely have a positive effect on the resilience of EU companies in case of shocks or international crises, which could benefit their international position vis-à-vis non-EU competitors.

Under **Option C.1,** a better level playing field in the internal market would benefit essential and important entities subject to jurisdiction of several Member States or entities scaling up and creating establishments in several Member States, increasing the competitiveness of the Union. The actions foreseen under **Option C.2** would further increase the positive impacts on competitiveness. **Option C.3** demands full repeal of existing Union legal acts and assumes rapid replacement through a single legal basis, which poses legal and institutional risks during the transition. This legal uncertainty may carry risks to competitiveness and innovation in the short term but is likely to have a strong positive impact on competitiveness in the long term.

The considered **options related to ICT supply chain security** could have a significant impact on the international trade, investments, innovation and competitiveness of EU businesses. On the one side, when implemented, market restriction affecting ICT key assets may have an impact on the availability of specific components in the EU market, which could lead to higher prices for consumers and businesses. Market restrictions may also have an impact on competition in the EU market, as well as on international trade relations between the EU and its trading partners. Those effects could be Member State-related under D1, more prominent at EU level for 5G technologies under option D2 and potentially extended to other sectors under option D3. However, the overall impact of the options considered would be limited to entities active in a limited number of critical sectors and for specific assets. On the other side, the restriction related to untrusted assets would also create **new market opportunities for trusted suppliers**, estimated at **EUR 2 bn per year** during the transition period of three years and hence stimulate innovation, R&D and competitiveness in the internal market.

**Option D.1** would have a limited impact on competitiveness and innovation as it would only entail non-binding measures which would leave discretion to Member States to assess the potential impact and, depending on the specific outcome, decide whether to implement them. **Option D.2** would have an impact on competitiveness and innovation in the 5G market, as some suppliers would be designated as high-risk suppliers, which would affect EU market access for those companies, which would in turn reduce the

choice of available suppliers in the EU. There are currently several suppliers of 5G equipment in the market (Qualcomm, Sharp, LG Electronics, Samsung, ZTE), with three of them having the biggest market shares (Huawei, Ericsson, Nokia). Two of these suppliers have already been assessed as high-risk suppliers in the Commission Communication C (2023) 4049 final. Evidence from some Member States or third countries where the high-risk suppliers have been made subject to restrictions showed that the other suppliers generally have the capacity to provide the equipment and fill in the space left by the high-risk suppliers. In view of the presence of sufficient other suppliers in the market, the negative impact on innovation and competition would likely be limited. Furthermore, the new market opportunities created for trusted suppliers would further incentivize investments and innovation stimulating a **trustworthy, innovative and competitive 5G offering**. The impact on competitiveness and innovation of **Option D.3** will be more effectively analysed through the market analysis that will be conducted in parallel to the EU coordinated security risk assessments, for each specific sector/technology. As for D2, measures to restrict entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers) and avoid dependency could be beneficial for European and non-EU trusted companies and their competitiveness.

As for the **impact on international competitiveness and trade**, the considered options are compatible with the EU's legal commitments under the World Trade Organisation (WTO) Agreements as well as bilateral, multilateral and plurilateral agreements. The options D.1–D.3 provide for a necessary and proportionate intervention to ensure cybersecurity of critical ICT supply chains. Whilst measures taken under these options could have a trade restrictive effect for certain goods and services, these measures would be justifiable in view of the overall legitimate objective to ensure the security of critical ICT supply chains in the EU. It is estimated that the economic impact arising from trade implications would be the smallest under option D.1 and the largest under D.3, given that option D.3 provides for the most comprehensive policy intervention. As regards the potential impact of **option D.2**, one report estimates that the proportion of 5G sites in the EU and five other countries provided by Huawei and ZTE was 32%, with a predicted share of 29% in 2028.[176] This could lead to substantial market impact depending on the level of dependency of each Member States as outline in *section 6.1.1.4*. Looking at the overall economy, market opportunities would also be created for trusted suppliers. Under option D.3, the precise impact depends on the sectors addressed and on the specific measures taken. Accordingly, as is outlined in section 5.2.4, the use of empowerments would be informed by a risk assessment and market analysis, to ensure that the measures taken are both necessary and proportionate taking into account, e.g. the configuration of the EU's trade balance for specific high-tech goods and services. Whilst the overall high-tech import and export for the EU remains balanced, this may evolve over time and be different for specific sectors and / or products or services .Overall, potential disruptive impact on international trade could be mitigated in bilateral contacts between the EU and third countries through regulatory dialogues and other high-level forums, i.e. the G7, where the EU is already engaged in deliberations on supply chain security, with the intention of building synergies between similar approaches or be mitigated through

[176] Morris Iain, Huawei *has hardly been weakened in European 5G, data shows, Light Reading*, https://www.lightreading.com/5g/huawei-has-hardly-been-weakened-in-european-5g-data-shows.

reinforced cooperation with trusted partners in line with the European Economic Security Strategy[177].

### 6.2. Impacts on security, including hybrid threats[178], resilience, technological sovereignty, open strategic autonomy and security of supply

#### 6.2.1. *Impacts on security, including hybrid threats*

An enhanced ENISA mandate (options A.2 and A.3) would have a positive impact on the **European Union's security interests** insofar as it would enhance ENISA's in-house expertise and capabilities, which would in turn benefit its stakeholders, at the forefront of which Member States. While this reinforced mandate would not prevent the cybersecurity threats and incidents from happening, preparedness and response would be enhanced as ENISA would be better prepared to perform its mission of assistance to Member States. By becoming a high expertise, technical hub, ENISA would **push the overall level of security in the Union upwards.**

Under option A.2, ENISA would be in a position to act as an authority for vulnerability identification systems and create synergies with the CRA single reporting platform. In this regard, whereas the option would no per se reduce the risks of hybrid threats, it would nevertheless support the **reduction of the exposure to hybrid attacks or cybersecurity incidents by developing expertise and enriching vulnerability records.** ENISA would be in a better position to issue guidance on highly technical dimensions, hereby complementing CERT-EU where its field of action is not covered. Similarly, the development of cybersecurity threat intelligence (CTI) expertise within ENISA would be beneficial to Member States and industry. ENISA would develop a capacity to **better address in particular hybrid threats, should ENISA enhance its cooperation with other specialised agencies** such as Europol. Option A2 would therefore lead to an increase in ENISA's technical in-house expertise which would entail enhanced capacity for ENISA to provide support to Member States and industry where needed, strengthening cybersecurity across the Union.

Options A.2 and A.3 would further support the development of a skilled cybersecurity workforce, trained to the state-of-the-art, such as those laid down in a European individual cybersecurity attestation scheme. With lifelong learning and individual attestations, cybersecurity professionals remain trained against emerging threats, new technologies and evolving regulations. A skilled workforce with recognised and portable skills further has an enhanced capacity to irrigate all sectors, ensuring skills portability across civilian and military organisations, and gaining in turn in expertise. In this regard, cybersecurity skills certification plays a role in strengthening overall security and countering hybrid threats: hybrid threats require multi-layered defence, requiring teams with a variety of skillsets. Certifications acknowledge the skills against a designated skillset, leading to a common understanding of an individual's capacities, serving as

[177] JOIN/2023/20 final.

[178] Hybrid activities by State and non-state actors aim to destabilise countries by undermining public trust in government institutions and by challenging the core values of societies and deepening social divisions. Hybrid threats range from cyber-attacks disrupting the economy and public critical services to targeted disinformation campaigns and hostile military actions.

benchmark of trust. It allows to build **teams with complementary expertise, which can collaborate effectively across disciplines and across borders and enables interoperability in joint operations**. More generally, supporting the growth and enhancement of the cybersecurity workforce would contribute to recuing the risk of attacks. For instance, a recurring root cause for suffering from a ransomware is lack of people/capacity or lack of expertise (*see Annex 7, Part 5*). Therefore, whereas ENISA's mandate on skills under options A.2 and A.3, and notably on European individual cybersecurity skills attestations, would not solve the dramatic skills gap, it would support Member States and industry in growing and strengthening their workforce, contributing to a stronger and more resilient European Union.

A stronger ENISA **mandate** (options A.2 and A.3) **combined with NIS2 targeted amendments** (option C.2) would have indirect impacts on Member States as ENISA would position itself as a cross-border cybersecurity reference point, developing here again its expertise and being in a position to better **assist Member States, to act as a bridge between them** in the event of a cross-border cybersecurity incident.

Beyond demonstrating compliance (with the certification of organisation) combination of options B.2/ B.3 and C.2/C.3, according to which the scope of the ECCF is extended and certification of organisation introduced would have a direct effect on the overall level of security. Mechanically, by pulling upwards entities into organisation-wide cybersecurity posture and ensuring synergy amongst cybersecurity frameworks, implementation of cybersecurity requirements is rendered easier for organisations. By **facilitating the implementation of cybersecurity requirements, the overall level of security of organisations is strengthened**. Additionally, a more efficient certification governance would lead to the adoption of **more schemes, which in turn would enhance security** by ensuring they meet recognised standards and have been rigorously tested for vulnerabilities. Lastly, certification would have the incidental effect of promoting secure-by-design practices.

#### 6.2.2. *Impacts on resilience, technological sovereignty, open strategic autonomy and security of supply*

Policy options, in particular options D, will impact cybersecurity risks that can be related to strategic dependencies (non-technical risks). Reducing dependencies as well as the reliance on entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers) in ICT supply chains are important aspects of security as well of technological sovereignty and will reduce related cybersecurity risks as outlined in *section 2* (*Sections 2.1.4.2 and 2.2.3*).

Both options A and B could have some positive impacts (similarly strong for A2 and A3) on Europe's technological sovereignty by promoting the competitiveness of the European industrial cybersecurity ecosystem, including through a greater involvement on standardisation (*Section 6.1.4*). Options B, by strengthening the ECCF, will enable to identify vendors that can be trusted and strengthen the reputation of European players.

Measures to adjust the scope of the NIS2 Directive outlined in **option C.2** and **C.3** are estimated to have an overall neutral effect on the overall level of cyber resilience of critical sectors in the EU. Entities removed from the scope of the Directive may lower their level of cybersecurity risk-management measures: nonetheless, those entities are assessed as not being high priority for the overall resilience of infrastructure. On the other hand, targeted addition of entities in sectors of high societal importance to the scope of the Directive will add to the level of resilience.

The impact of ICT supply chain measures on Europe's strategic autonomy would depend on their binding and harmonised nature. The impact of **option D.1** on digital sovereignty and strategic autonomy would rather be limited as per its non-binding nature, and it would depend on how Member States implement them at national level. **Option D.2** would have a positive and strong impact on the security and resilience of 5G networks as they would only be based on trusted suppliers following the end of the transition period. By extending this approach to other ICT supply chains, **option D.3** would most effectively decrease the dependency on high-risk suppliers or entities originating from or controlled by countries posing cybersecurity concerns at Union level and hence enhance the security of supply.

### 6.3. **Social impacts, including fundamental rights**

The policy options were assessed based on their potential to enhance or risk fundamental rights and promote equality and trust, with a particular focus on societal impacts and rights, including privacy, data protection and the ability of individuals to understand, exercise and enforce their rights. Furthermore, the policy options were assessed against the *"digital by default"* principle which facilitates the transition to seamless, digital-first service delivery.

An enhanced ENISA mandate will contribute to more cyber resilience of the economy and society in general and hence a better protection of the citizen's privacy and personal data (strongest in A.3 followed by A.2 and A.1). Furthermore, A.2 and A.3 would also positively contribute to education and training in cybersecurity as it will clarify ENISA's role in the development of skills for the cybersecurity workforce.

Furthermore, the ECCF would improve trust of EU citizens and business in certified ICT solutions that support their everyday life. […] Under B3, mandatory certification of essential entities could further contribute to the protection of citizens and trust in the protection of sensitive data, such as in the healthcare sector.

Options C.1–C.3 would contribute to citizens' trust in organisations acting in critical sectors. In particular, options C.2–C.3 (in combination with B2/B3) would contribute to citizens' trust by incentivising entities in these sectors to obtain cybersecurity certification, thereby publicly demonstrating their high level of cybersecurity. Moreover, by ensuring harmonised reporting about ransomware incidents, Options C.2–C.3 would increase public trust in the protection of sensitive data in critical sectors. This could however be slightly undermined by the scope changes under C2/3.

All options D would have some impact on the protection of fundamental rights by limiting the interference of malicious third countries. Activities such as espionage and surveillance heavily undermine citizens' fundamental rights. Under option D.1, the impact on privacy and citizens' trust in organisations acting in critical sectors will depend on how Member States implement the recommended measures. Under option D.2 would have a positive, although indirect, impact on the social sphere. The envisaged codification of measures for 5G networks would contribute to the security of data by protecting the confidentiality, integrity and availability of information in 5G equipment enabling EU citizens to trust 5G networks solutions used in the everyday life. It would also prevent unlawful access and exfiltration of data. Option D.3 would have the most impact on fundamental rights. The horizontal framework would have the potential to improve the trust, security and privacy in various technologies.

Options D.2 and D.3 could also have a high impact on digitalisation as they would entail the replacement of components from high-risk suppliers or entities originating from or controlled by countries posing cybersecurity concerns in 5G networks (option D.2) and, subject to further implementation and assessments, also for other ICT supply chains (option D.3). Moreover, options D.2 and D.3 are expected to positively impact customers trust to digital solutions.

### 6.4. Impacts on the environment

Each policy option was assessed in line with the EC's Green Deal and its commitment to the *"green oath"*[179], stating that no legislative proposal should cause harm to the environment.

Regarding options A.1 and A.2, the changes to ENISA's mandate would have a negligible environmental footprint. However, slightly improved coordination and inclusion of liaison officers under Option A.2 could reduce the frequency of ad hoc meetings and travel, potentially lowering emissions related to in-person coordination activities. Similarly, under option A.3 potential environmental benefits could result from further consolidation of operational functions and reduced duplication across Member States, including with the use of ENISA's operational team. However, the increased operational role for ENISA would likely require greater data handling capacity, resulting in higher energy consumption.

Options B.1 would have little to no environmental impact. Option B.2 could have limited positive impact environmental sustainability as it introduces more efficient certification development process aiming to reduce footprint of maintaining multiple national certification schemes. Nonetheless, these benefits could be offset by increase in certification uptake leading to a rise in data collection and energy use. The success of this balance would depend on the energy profile of the certification platforms and their hosting environments. Selective mandatory certification envisaged under option B.3 would have similar effect.

Options C.1 and C.2 would have little to no environmental impact. The introduction of binding templates indirectly influences the environmental efficiency of data systems by promoting harmonised practices. Option C.3 would maximise the environmental benefits by fully harmonising all cybersecurity risk-management and incident reporting obligations under a single framework.

Option D.1 would have a limited impact on the environment. Options D.2 and D.3 with the replacement of products or equipment provided by high-risk suppliers or entities originating from or controlled by countries posing cybersecurity concerns is expected to have a neutral environmental impact on the environment, as both options will take into account the product lifecycle of such product or equipment and include appropriate transition periods.

## 7. HOW DO THE OPTIONS COMPARE?

This chapter presents a comparison of the policy options presented in this impact assessment. The comparison builds on the preceding analyses and integrates the assessment of effectiveness, efficiency, coherence, proportionality and uncertainties. It

[179] COM(2019) 640 final.

follows the methodology outlined in the Better Regulation Toolbox and aims to identify the most suitable policy package in relation to the general and specific objectives described in Chapter 4. It also reflects on trade-offs, potential synergies, and how the options would perform under different assumptions, including implementation uncertainty.

### 7.1. Methodology

The options were compared using a qualitative multi-criteria analysis supported by quantitative cost and benefit data wherever available. The analysis considers five core assessment criteria:

- **Effectiveness:** Likelihood and extent to which each option contributes to achieving the specific objectives.
- **Efficiency:** Relationship between benefits in terms of cost savings and broader positive impacts and costs linked to implementation of the policy measures.
- **Coherence:** Consistency with broader EU policies and legal instruments, including the Charter of Fundamental Rights and the Sustainable Development Goals.
- **Proportionality:** Appropriateness of the policy response in relation to the magnitude of the problem and stakeholder burden.
- **Uncertainty:** Sensitivity to external factors, implementation risk, and reliance on stakeholder engagement or institutional cooperation.

The comparative analysis considers each criterion in turn, evaluating the relative performance of the full range of policy options considering the available evidence. Where applicable, quantified estimates were used to assess implementation and compliance costs, as well as projected benefits such as administrative savings, improved trust, or reduction in incident-related damages. It should be noted that limited availability of reliable market data did not allow for granular and accurate quantitative assessments of cost savings related to the specific policy measures being assessed (*see for explanation in Annex 7*). Due to this lack of available data, it is difficult to quantify the causality between the measures included in the different policy options and related cost savings in terms of probability and impact of cybersecurity incidents. Those limitations need to be taken into account also in the comparison of the options, in particular relevant for criterium of efficiency and effectiveness. All measures contribute to different degrees to the general objective of mitigating risks (and related costs) of cyber incidents occurring (e.g. through faster detection) and safeguard against potential adverse cybersecurity events (e.g. faster response) of unpredictable nature. The comparison of the options draws a distinction and classify the options based on the data and to what extent the options and their combination can contribute to achieve the specific objectives (for effectiveness) or where is the best ratio of costs/benefits that can be deduced, taking into account the data limitations (for efficiency). The analysed options offer a balanced trade-off between policy ambition and practical feasibility, with special attention to institutional synergies, legal clarity and stakeholder support. The options are not assessed in isolation, but as part of an intervention framework where interactions between measures can strengthen or weaken overall outcomes.

The overall comparison is summarized in a **table** at the end of this section.

## 7.2. **Effectiveness**

The effectiveness of the policy options is closely linked to their capacity to remove existing bottlenecks, provide legal clarity, and foster cooperation and trust in cybersecurity across the EU. The assessment of effectiveness of one policy option could be reinforced or limited if is accompanied by another option from another intervention area of the CSA revision which can either further enhance it or be less compatible with it. Therefore, combinations of certain options will reinforce effectiveness of the options in question (in green) or ensure that options can materialise at all (in red). Those combinations explained in section 5.4 can be summarised in the below table.

Table 16: Combination of options: effectiveness of options

| | A.1 | A.2 | A.3 | B.1 | B.2 | B.3 | C.1 | C.2 | C.3 |
|---|---|---|---|---|---|---|---|---|---|
| A.1 | | | | | | | | | |
| A.2 | | | | | | | | | |
| A.3 | | | | | | | | | |
| B.1 | | | | | | | | | |
| B.2 | | | | | | | | | |
| B.3 | | | | | | | | | |
| C.1 | | | | | | | | | |
| C.2 | | | | | | | | | |
| C.3 | | | | | | | | | |

The effectiveness of how the options fulfil the specific objectives will be conducted with the links as presented above in mind, which will exclude certain ineffective combination of options from further analysis.

### *7.2.1 Specific Objective (SPO) 1: Create the capacity to effectively implement Union cybersecurity policies and continuous operational cooperation and in that way enable more structured cooperation between Member States.*

Options A are addressing this specific objective. Option **A.1** clarifies ENISA's mandate, bringing together all the tasks from other legislations and enhancing somewhat the support for operational cooperation in the CSIRTs network and EU-CyCLONe. It does not however create additional capabilities, nor provides for additional resources, which makes its **effectiveness low,** especially for creation of capacities for effective operational cooperation.

Options **A.2 and A.3** are much more effective in achieving this objective, as these options combine structural changes and operational tools to address the objective. A.2 strengthens ENISA's structure and role in implementation support and coordination, contributing positively to the overall resilience and shared situational awareness. It also strengthens ENISA's mandate in terms of providing operational support to Member States, while strengthening ENISA's capacity and resources to ensure effective delivery of the Agency's tasks. A.3 empowers ENISA to provide operational incident response support directly to entities, making it more effective in responding to cross-border cybersecurity threats but requiring substantial investment in developing such capabilities. The exact degree to which extent both options can contribute to overall cybersecurity resilience cannot be defined. However, with the additional tools and clarification of the mandate of ENISA, it is to be assumed that the agency will be able to enhance policy implementation and even more so operational cooperation among Member States significantly, therefore both options are assessed to have **high effectiveness to meet this objective**.

### *7.2.2 SPO2: Develop and implement the means and mechanisms to effectively support and address the needs of Member States, industry and other stakeholders.*

Options A are delivering on this specific objective. While option **A.1** will have a **low effectiveness** as it does not reform ENISA's mandate as such and only provides for certain prioritisation, options A.2 and A.3 provide for better clarity of the mandate itself and prioritisation of tasks, putting focus on the three tasks that were identified as the most important ones in the public consultation, namely certification and standardisation, support for policy implementation and support for operational cooperation[180]. They also deliver for a new resourcing model for the Agency, which was underlined in the Evaluation Report (*Annex 8*) as one of the root causes for the need to reform. Option **A.2** develops new tools and mechanisms through which ENISA will support the stakeholders and it addresses the stakeholders' needs (offering what was missing, providing for added value as indicated in the public consultation responses) and is assessed to have **high effectiveness** for this objective, while option **A.3,** while offering new tools and mechanisms, it does not meet the stakeholders' needs as is proposing an operational role for ENISA which goes beyond the acceptance of Member States, the effectiveness of **A3 in meeting this objective is thus assessed as low**.

Options **A.2 and A.3** empower ENISA to strengthen its role in the standardisation processes, which was underlined by the stakeholders as important tasks of the agency. **They are reinforcing options B1/B2/B3.**

Similarly, **options C.2 and C.3** would not be possible to deliver on further facilitation of compliance with cybersecurity risk-management measures for multi-country entities **without options A.2 and A.3** giving ENISA a task to support Member States.

Overall, taking SPO1 and SPO2, the effectiveness of A1 can be assessed low, while A3 would be moderate (given shortcomings in meetings Member States' needs) and A2 would be **high**.

### *7.2.3 SPO3: Create the prerequisites for faster delivery of cybersecurity certification schemes driven by market needs by broadening the scope of the ECCF, ensuring effective maintenance and agile procedures and increasing transparency.*

Options B are addressing this specific objective (in combination with other policy options). Option **B.1**, while providing for clarification, will not provide for an in-depth reform of the ECCF, therefore its effectiveness to achieve the objective is **low** as the procedural shortcoming of the ECCF will remain in place.

**B.2** establishes a structured, inclusive, and forward-looking process for certification scheme development, including organisational certification. These changes are expected to result in faster scheme delivery time, thus reducing fragmentation of certification and improving level of cybersecurity across the EU. This will ultimately foster a chain of trust among economical operators and facilitate uptake of digital technologies. It provides for all the necessary changes to ensure effective maintenance, agile procedures and enhanced

[180] Across all respondents, the task most frequently rated as *"Very important"* was market, cybersecurity certification, and standardisation, selected by 58.6% of participants. This was followed by development and implementation of Union policy and law at 47.2 %, and operational cooperation at Union level at 45.1%. The task least frequently rated as *"Very important"* was research and innovation, at just 20.2%.

transparency to effectively achieve the objective. **B.3** builds on B.2 providing for mandatory certification in specific risk scenarios / uses for NIS 2 entities operating in the highly critical sectors. This could have an enhanced effectiveness on delivering on cybersecurity assurance for critical infrastructure.

While **B.2 (and B.3)** provide for an effective approach to achieve procedural shortcomings, the adoption of schemes and their successful implementation and uptake will depend on the availability of a mechanism to address non-technical risks in a harmonised way that is provided by **option D2** (for 5G) and to a greater extent by **option D.3**. Without D3, both options **B.2 and B.3** will most probably fail to deliver the EUCS and EU5G schemes (and potentially managed security services scheme). The combination with option D.2 could have a partial improvement of effectiveness as it would allow to deliver the EU5G scheme (but not the other schemes). Therefore, **only in combination with option D.3 those options are consider of high effectiveness and of medium effectiveness if combined with option D.2.**

Options B are also interlinked with options C.2 and C.3 when it comes for the certification of organisations. Without the possibility to demonstrate compliance as provided by options C2/C.3, the added value of this additional certification scheme will be very limited, and in case of option B.3 - not proportionate (mandatory certification). Therefore, **only in combination with options C.2/C.3, options B.2 and B.3 can be considered of high effectiveness.**

#### *7.2.4 SPO4: Create mechanisms and conditions to facilitate compliance with cybersecurity requirements, thereby making their implementation more coherent and effective.*

Options C are addressing this specific objective to a different extend. Option **C.1** in a soft law option. While the envisaged measures may generate marginal improvements in the understanding of the existing frameworks and their functioning, further specifying measures within the limits of implementing act empowerments (minimal harmonisation). Enhanced cooperation would not address structural fragmentation, nor ensure legal certainty where there is unclarity on scope, nor address fragmentation of compliance requirements or supervisory approaches across Member States. Therefore, this option is assessed as of **low effectiveness**.

Option C.2 delivers major gains through different scope changes, creating the framework for a cyber posture certification that can allow entities providing services across several Member States to demonstrate compliance with cybersecurity legislation in one go, while also creating the basis for more coherent and less burdening supervisory approaches across the internal market, providing also for maximum harmonisation for the NIS 2 Directive implementing acts. While option C.3 takes this further by repealing sector-specific obligations and centralising compliance under the NIS 2 framework, in the short term it would also lead to significant legal uncertainty among stakeholders that are in the process of adapting to the recently adopted legal frameworks that would be subject to a deeper harmonisation (see criteria related to certainty).

Both options **C. 2 and C.3** would not be able to facilitate of compliance with cybersecurity risk-management measures for multi-country entities subject to supervision by competent authorities from several Member States, if they are not combined with **options A.2 or A.3**, giving ENISA a clear mandate to support Member States in the supervision of these entities and facilitate mutual assistance. Similarly, options C.2 and C.3 will not be able to facilitate compliance by allowing for assumption of conformity with the organisational certification for entities, if those are not possible under the ECCF

(so without options B.2 or B.3). Therefore, those options are of **high effectiveness if combined with options A.2/A.3 and B.2/B.3.**

Considering the effectiveness of these policy options under the specific policy objectives previously analysed. **The combinations of B2/B3 and C2/3 should be considered of high effectiveness to address this objective.**

*7.2.5 SPO5: De-risk critical ICT supply chains from entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers) and reduce critical dependencies by developing a coherent and effective framework at EU level to address ICT supply chain security risks*

Options D are contributing to this specific objective by providing for a solution to improve implementation of measure with objective to de-risk the ICT supply chains in the Union. A non-legislative option **D.1** provides for non-binding mitigating measures. While this option can address the specific objective as it addresses the possibility to adopt such measures across the ICT supply chains, its effectiveness is **low** due to its non-binding nature. It would not address the fragmentation and difference in implementation among the Member States and not allow for a coherent approach at the EU level (as also judging by the current implementation of the 5G cybersecurity toolbox). Option **D.2** would provide for an effective solution to address this objective but only for the 5G networks, by codifying the toolbox. It would not however address the specific objective to provide for an effective and coherent framework for the ICT supply chains. Its overall effective, therefore, should be assessed as **medium,** as it would only improve implementation of the harmonised measures in one area.

Finally, the option **D.3** addresses the full scope of the specific objective in question. The framework would be future-proof and common to all Member States, which makes the process of identifying non-technical risks more effective at EU-level. It also addresses the specific objective in the most comprehensive way, providing for a framework that allows to identify risks to key assets and propose proportionate measures, resulting from an evidence-based process, in any critical supply chain. It should be noted that the actual degree of de-risking that can be achieved depend on whether the framework will be used in all areas where the risk is to be identified and the de-risking measures implemented. With this caveat, it is considered **of high effectiveness**, as it provides for most comprehensive solution from the options offered.

The effectiveness of option D.3 will be reinforced by measures introduced by options B (B.1, B.2, B.3) providing for the ECCF for technical risks related to the ICT supply chains, and options C (C.2, C.3) which foreseen to provide for the guidelines on the application of the supply chain security measures in accordance with the NIS 2 Directive. Considering the effectiveness of these policy options under the specific policy objectives previously analysed. **The combinations of D3 with B2/B3 and C2/3 should be considered of high effectiveness to address this objective.**

## 7.3. Efficiency and cost-benefit analysis

The efficiency of the policy options depends on the ratio of costs (compliance costs or price increases) to main expected direct benefits. Furthermore, broader (negative and positive) impacts of specific relevance to the proposal, such as internal market, SMEs, and trade & competitiveness and cyber resilience/technological sovereignty are also taken into consideration (next to social and environmental impacts). To the extent possible, the net value of the cost-benefit ration has been calculated. However, several impacts, including cost reductions due to the reduced cybersecurity incidents, are compared in a

qualitative manner, hence it has not been possible to provide a full cost-benefit ration comparison of all policy options. In addition, it should be noted that limited availability of reliable market data did not allow for granular and accurate quantitative assessments of cost savings related to the specific policy measures being assessed. Due to this lack of available data, it is difficult to quantify the causality between the measures included in the different policy options and related cost savings in terms of probability and impact of cybersecurity incidents. Furthermore, in several instances the costs could not be aggregated, for instance in the case of voluntary measures. The costs and benefits are assessed and compared considering each stakeholder category. For a better overview, the **table** below compares the costs-benefits by policy option by combining quantitative and qualitative assessments. A more **detailed overview** of the cost-benefits analysis by policy option is included in *Annex 13*.

Regarding the **options on the ENISA mandate, A.1** would have the best net value compared to A2 and A3 based on estimated quantitative data (mainly impacting ENISA), however it would likely lead to minor benefits in terms of cost reduction related to cybersecurity incidents. While those impacts could not be quantified in a comparative manner, the impact of option A1 on efficiency is expected to be **moderate**. Between A2 and A3, the efficiency appears similar, as substantially higher costs for ENISA would likely lead to equally higher benefits related to impacts on cybersecurity, and comparably positive impacts on SMEs, internal, trade/competitiveness, and technological sovereignty. It is to be noted however, that those benefits could only be broadly estimated for option A2 and A3 and not to a level of granularity that would allow for a refined comparison. Hence, both **A2 and A3 are similarly high on efficiency**. **Public authorities** will be significantly impacted under options A2 and A3. Option A.3 would be slightly more costly than option A.2 due to the transfer of additional national liaison officers, while option A.1 would not involve direct resources for Member States. At the same time, Member States would benefit from enhanced operational support from ENISA (higher under A3 compared to A2). Options A will not significantly impact businesses. **Businesses,** including SMEs**,** are expected to save costs thanks to faster detection and response to cybersecurity incidents (expected to be higher under A3 than in A2 with the above-mentioned data limitations), whole costs related to participation in the skills attestation scheme would remain voluntary commitment to the initiative. **Citizens** will overall benefit from improved cyber resilience thanks to an enhanced ENISA mandate and more attractive offering of skills attestations (expected to be higher under A3 than A2).

Regarding the **certification framework**, between B1 and B2, the net value would be negative in both cases due to adjustment costs for **ENISA and public authorities** in the implementation of schemes. These costs would be higher in absolute terms under B2 than B1 due to the existence of an additional scheme. At the same time, an expanded scope under B2 would also bring additional benefits in terms of cyber resilience. In both cases, higher costs for ENISA and public authorities would arise if more schemes are adopted . Given that B2 would add procedural efficiencies and alignment, overall, it is assessed as being more efficient than B1. Furthermore, it is to be noted that under B2, ENISA would be able to levy charges for the maintenance of schemes, hence able to compensate part of the costs. Taking these fees into account, remaining operational costs for ENISA would be lower under B2 compared to B1. At the same time, charges would be incurred by conformity assessment bodies. B3, building on B2, by introducing mandatory certification for essential entities, would lead to high results on cyber resilience, while impacting a limited number of large companies and including mainly one-off costs (in

combination with C2/C3). However, B3 may come with some negative impacts on trade and prices for citizens, while no such effects are expected under B2 and B1. The competitiveness of companies is not expected to be significantly impacted as the certification of entities would also lead to compliance benefits (see option C2). Looking at the **impacts on stakeholders,** overall, **ENISA** and **public authorities** would be most impacted in terms of costs by these policy options. Under B1 and B2 as the schemes would remain voluntary, no significant costs would occur for **businesses**, including **SMEs**, . Under B2, charges levied by ENISA would compensate operational costs while adding some burden on businesses. B3 would lead to one-off costs for NIS2 entities, that could be transferred on prices for citizens. Hence, in comparative terms, **B1** would rate low on efficiency with fewer schemes in place , **B2** would rate moderate alone (with an additional scheme) and **B3** would rate moderate to low alone.

Regarding **simplification**, C.1 would not lead to substantial cost savings for businesses and the impact on the internal market would be positive but limited. Both C2 and C3 are expected to bring substantial compliance cost savings for **businesses including SMEs and medium-caps companies**, while having also strong impact on the internal market (greater for C3 than C2, while C3 would have some one-off adjustment costs). In addition, C3 would also lead to savings for **public authorities** related to supervision. Both for C2 and C3, the impact on cyber resilience is expected to be nuanced due to the scope changes, while measures such as certification (link with B2/3) and reporting of ransomware would be positive, while it is to be mentioned that those impacts could not be quantified. Looking at other stakeholders, ENISA would be impacted by both C2 and C3 due to support given to Member States (link to A2/3). As a result, **C3 would appear most efficient (high), followed by C2 (moderate) and C1 (low)**.

Regarding **ICT supply chain security**, under D1 the costs for **businesses** related to restrictions (and related benefits in terms of cyber resilience) would be uneven and driven by Member States implementation and add market fragmentation. On the contrary, D.2 would entail the economic costs for **suppliers** of replacing equipment from high-risk suppliers in the key assets of the 5G networks as well as identifying those suppliers and assets related to 5G networks, however the benefits this would also create new market and investment opportunities for trusted suppliers. Furthermore, the positive impacts in terms of internal market approach and cyber resilience would be substantial. The efficiency of D3 would be higher than for D2 as D3 would ensure in addition a common and harmonised approach for other sectors ensuring a consistent approach over time and economies of scale for trusted suppliers. D3 would calculate the costs and benefits for measures effecting other critical supply chains. For both D2 and D3, negative impacts on trade and consumer choice are not expected to cause major disruptions. Furthermore, it is expected that European competitiveness and innovation will be stimulated (see also *section 6.1.4*), while in the short-term price increases are likely for **citizens**. **SMEs** could be affected across the supply chains and substitutions costs under D2 and D3, while they would also benefit from higher cyber resilience and new market opportunities. **Public authorities** would face higher supervision costs under D3 with new sectors added compared to D2, while they would also greatly benefit from increased cyber resilience as ICT users. ENISA would not be specifically affected by these policy options. Overall, the efficiency of **D3 is rated high followed by D2 (high to moderate) and D1 (low).**

Table 17: Overview net values and comparative analysis *by stakeholders*

Legend: * broad estimate base on limited available data ; ** recurrent for three years; (D2/3) if a combination of policy options materialise.

| **Efficiency** | **Policy options** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ENISA mandate | | | Certification | | | Simplification | | | Supply chain | | |
| | A.1 | A.2 | A.3 | B.1 | B.2 | B.3 | C.1 | C.2 | C.3 | D.1 | D.2 | D.3 |
| **Compliance costs (savings/revenues)** For businesses | + | +/++ | ++/+++ | 0/+ | + (D2/3) - EUR 1.3 M to 1.7 M | - - EUR 1.8 M to 2.2 M | - | **+ EUR 14.6 bn** | **+ EUR 32 bn** | - | **- EUR 1.4 bn to EUR 2.3 bn** per year ** | **< - EUR 1.4 bn to EUR 2.3 bn** per year ** |
| for public authorities | 0/+ | **- EUR 11.3M** | **- EUR 12.71M** | **- EUR 0 -61 M** | **- EUR 13.7 to 74.7 M(D3)** | **- EUR 22.8 to 83.9 M (D3)** | 0 | **+ 7,5 M** | **+ 14.8 M** | - | + | + |
| for ENISA | 0/+ | **-EUR 148.12M** | **-EUR 165.37M** | **- EUR 6.8 to 10.5** | **- EUR 9.5 to 13.1 M (D3)** | **- EUR 9.5 and 13.1 M (D3)** | N.A. | (A2/3) | (A2/3) | N.A | N.A | N.A |
| for citizens (price increase) | N.A | N.A | N.A | N.A | 0/- | - | N.A | N.A | N.A | 0/- | - | - |
| **Internal market** | 0 | 0/+ | 0/+ | 0/+ | +(+) (D2/3) | ++(+) (D2/3) | **+** | ++ | **+++** | 0/- | + | ++/+++ |
| **Trade, innovation & competitiveness** | 0/+ | + | + | 0/+ | + | - | 0/+ | + | ++(-) | 0/- | + | **++** |
| **SMEs** | 0/+ | + | + | 0/+ | + | N.A | 0/+ | ++ | ++ | (+)(-) | (+)(-) | (+)(-) |
| **Cyber resilience/ Technological sovereignty** (citizens, businesses and public authorities) | + | ++ **EUR 3.7 to 4.4 bn over five years *** | +++ **EUR 3.7 to 4.4 bn over five years *** | 0/+ | +(+) (D2/3) | ++(+) (D2/3) | + | + (-) | +(-) | 0/+ | ++ | + + /+++ |
| **Social & fundamental rights** (citizens) | 0/+ | + | + | 0/+ | +(+) (D2/3) | ++(+) (D2/3) | 0/+ | +(-) | +(-) | 0/+ | ++ | ++/+++ |
| **Environment** | 0 | 0/+ | 0/+ | 0 | 0/+ | 0/+ | N.A | N.A | N.A | N.A | N.A | N.A |

### 7.4. **Coherence**

The assessment of coherence focuses on alignment with the EU's overarching policy framework, including the EU Cybersecurity Strategy and key existing and future legislative instruments. It also considers whether the options are coherent with the international developments.

More in depth comparison among the options based on the coherence criterium is presented in *Annex 14*.

The result of the assessment of the options shows that **options A.2, combination of B.2/B.3 with C.2/C.3 and option D.3** are of the **highest coherence** with other legal instruments and international developments.

Option **A.1** streamlines ENISA's mandate and does not contradict objectives of NIS 2 Directive, but it does not enhance synergies among ENISA's tasks and therefore does not contribute for the enhanced delivery on the NIS 2 Directive objectives. This option is assessed therefore as of **moderate coherence**. Option **A.2** reinforces the NIS 2 Directive objectives, in particular in the area of the operational cooperation and contributes to effective achievement of the CRA's objectives, it is assessed as of **highly coherence**. Option **A.3** going further in support of operational cooperation diverge from the NIS 2 Directive model, where it is national CSIRT at the centre of the operational cooperation, for that reason it is assessed as of **low coherence**.

Options **B.2/B.3 in combination with options C.2 and C.3** are assessed of **highly coherence** because they provide for the certification of entities that allow to demonstrate compliance with the NIS 2 Directive (and other legal acts). In addition, options **B.2 and B.3** both options are **highly coherent** with the CRA (and the New Legislative Framework). They are also coherent with international developments. **Option B.1** is assessed as neutral to the NIS 2 Directive and therefore assessed as of **moderate coherence**.

Options C.1 and C.2 are assessed as coherent with the CER Directive, as they will not affect it. Option C.3 is of low coherence with the CER Directive. All options C are coherent with the international developments on ransomware. Therefore, **options C.1 and C.2** could be assessed as **highly coherent,** while **option C.3** should be assessed as of **low coherence**. The combination of options are presented above.

Options D are assessed as coherent with the NIS 2 Directive and CER Directive, with D.3 as most coherent for providing for effective framework for the ICT supply chain security. Options D are also coherent with the CRA, as they complement market surveillance mechanism addressing non-technical risk factors, with D.3 most and D.2 of moderate coherence (as only 5G network is covered). Similarly, their coherence is assessed vis a vis the Multiannual. Financial Framework proposal (D.3 – highly coherent and D.2 - of moderate coherence.). Options D.2 and D.3 are also coherent with international developments. Overall, **option D.3 should be assessed as highly coherent, D.2 and D.1 – of moderate coherence**).

### 7.5. **Proportionality and trade-offs**

Proportionality examines whether policy interventions are justified considering their intended impact and the burdens they create. Options **A.1, C.1 and D.1** carry low cost and minimal risk, but their limited scope does not sufficiently address the scale of the challenges identified and offers no capacity to scale with the evolving threat landscape. Option **B.1** carries a substantial risk that the blockage in adoption of the schemes will persist. As a result, they risk

perpetuating exiting fragmentation and inefficiencies. Option B.3 proposes an ambitious solution of mandatory certification, but its application is limited to a well-defined group of entities. Therefore, both are assessed of **medium proportionality**.

Most ambitious reforms such as Options **A.3 and C.3** may align well with long-term objectives but carry a higher risk of overreach. These options introduce significant administrative and financial requirements that may not be justified by their expected outcomes in the short to medium term. They also increase implementation complexity and the likelihood of legal or institutional conflict and carry potential political and trade related costs. While they could be effective in addressing the specific objectives, their cost and disruption their propose make them **not proportionate** to the effect achieved. Especially in comparison with options **A.2, B.2 and C.2** that offer similar high effectiveness while their cost is lower and their coherence with existing legal framework, stakeholder expectation is **higher.** They are designed to be incremental rather than disruptive, focusing on coordination, governance and harmonisation without imposing rigid obligations or creating institutional overlap.

Option **D.3** relies on gathering evidence of what constitutes key assets and what measures would be proportionate and necessary to ensure de-risking of the critical supply chains. Prior to defining these measures, an objective impact assessment and market analysis would be performed, which would look at, among others, economic feasibility, available alternatives in the market, lifecycle of the specific products which would help to determine appropriate phase-out periods for high-risk products. These assessments would inform what risk-based measures are needed and most appropriate, making this option **highly proportionate**. Similarly, option D.2 is considered **highly proportionate**, although it is much less effective

The trade-offs between ambition, feasibility and stakeholder support are most balanced in options A.2, B.2, C.2 and D.3. These options generate clear added value while managing costs and maintaining compatibility with situations where such interventions would be addressed on national level. They also offer opportunities for mutual reinforcement, such as the alignment between improved certification governance and demonstration of compliance between options **B.2 and C.2** or the solution to tackle non-technical risks between options **B.2 and D.3**, making those options **highly proportionate**.

### 7.6. Uncertainty analysis

Uncertainty affects all policy options to varying degrees, depending on the complexity of implementation, the level of institutional cooperation required, and the assumptions on stakeholder engagement and adoption. Options A.1, B.1, C.1 and D.1 face limited uncertainty, as their scope is narrower, and they introduce fewer substantial changes. They should be assessed as of low uncertainty.

By contrast, **Options A.2, B.2+C.2, D.2 and D.3 are moderately sensitive (moderate uncertain)** to implementation challenges, particularly regarding cross-border coordination, administrative capacity and uptake by stakeholders. For instance, Option A.2 assumes enhanced cooperation between ENISA and Member States, which depends on timely agreement on operational roles and funding arrangements. It also depends on the skills attestation uptake. In Option B.2, the creation of a predictable certification lifecycle assumes strong participation from industry and consistent Commission's oversight, both of which are contingent on political commitment and administrative resources. Option C.2 relies on Member States and stakeholders developing a cyber posture scheme, which may be subject to delays due to legal or technical barriers, however this option should be taken in combination

with option B.2. Option D.2 relies on already agreed identification of key assets in the EU coordinated risk assessment process with Member States. Option D.3 relies on the risk and evidence-based mechanism to define key assets and high-risk suppliers or entities originating from or controlled by countries posing cybersecurity concerns. Those are defined in a cooperative process and assumes strong participation of Member States. While the defining key assets brings relatively lower degree of uncertainty, identification of high-risk suppliers or countries posing cybersecurity concerns might become very political and therefore its level of uncertainty might be significant. However, this uncertainty becomes lower as the measures taken will be targeted and based on the evidence-based process. As these options are structured in a modular way that allows for incremental deployment and iterative improvements, reducing exposure to risk, even in conservative adoption scenarios, partial implementation is expected to deliver meaningful improvements over the baseline.

**Options A.3, B.3 and C.3 exhibit higher uncertainty**. These options rely heavily on significant institutional reform, large-scale behavioural change, and political consensus across Member States. Option A.3's direct operational role for ENISA risks friction with the role of national CSIRTs and may require complex agreements that could delay execution. Option B.3 introduces selective mandatory certification, which could pose institutional and competitiveness risks. Option C.3 demands full repeal of existing Union legal acts and assumes rapid replacement through a single legal basis, which poses legal and institutional risks during the transition. Also, since stakeholders are currently adapting to these relatively recent legal acts, a full repeal thereof would lead to a significant legal uncertainty. Sensitivity analysis confirms that these more ambitious options are less resilient to delays, stakeholder resistance or partial implementation. Their benefits are highly dependent on full uptake and coordination, while their costs are largely front-loaded and unavoidable. Therefore, while they may offer high potential in ideal conditions, they are more vulnerable to real-world constraints.

### 7.7. **Multi-criteria assessment**

The multi-criteria assessment provides a synthetic overview of how each option performs across the main evaluation criteria. While no formal weighting was applied, the analysis reflects an implicit prioritisation of effectiveness, efficiency and coherence, in line with the nature of the initiative. The **table** below summarises the results.

Table 18: Multi-criteria assessment

| Option | Effectiveness | Efficiency | Coherence | Proportionality | Certainty | Overall performance |
|---|---|---|---|---|---|---|
| **Low** | A.1<br>B.1<br>C.1<br>D.1 | B1<br>B3 (> B1)<br>C1<br>D1 | A.3<br>C.3 | A.3<br>C.3 | A.3<br>B.3<br>C.3 | |
| **Moderate (Medium)** | B.2/B.3+D.2<br>A.3<br>D.2<br>D.3 + C.1<br>D.3 + B.1 | A1<br>B2<br>B1+D3/D2<br>B3 + D3/D2<br>C2<br>D2 | A.1<br>B.1<br>D.1<br>D.2 | A.1<br>B.1<br>B.3<br>C.1<br>D.1 | A.2<br>B.2+C.2<br>D.2<br>D.3 | |
| **High** | A.2<br>B.2/B.3 + D.3<br>B.2/B.3+C.2/C.3<br>C.2/C.3+A.2/A.3<br>D.3<br>D.3+C.2/C.3 | A2<br>A3<br>B2 +D2/D3<br>C3<br>D3 | A.2<br>B.2/B.3 + C.2/C.3<br>D.3<br>C.1 C.2<br>B.2 B.3 | B.2+D.3<br>B.2+C.2<br>D.2<br>D.3<br>A.2<br>B.2<br>C.2 | A.1<br>B.1<br>C.1<br>D.1 | Preferred options<br>A.2<br>B.2 +D.3<br>B.2+C.2<br>D.3 |

## 8. PREFERRED OPTION

### 8.1. Rationale and benefits of the preferred option

The package consisting of Option A.2 (functional reform of ENISA), Option B.2 (reform of ECCF – scope extension, new procedure and revised governance) and Option C.2 (Targeted intervention – further simplification of compliance with relevant Union cybersecurity legislative framework) and D3 (Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks) is the preferred option, as it offers the most balanced and effective response to the policy problems identified in this impact assessment. This combination would address all specific objectives, ensure high levels of efficiency and coherence, and avoid excessive regulatory burden. The overall benefits of the preferred option are summarised in *Annex 3*.

In particular, Option A.2 would provide for a strengthened ENISA, equipped with the necessary tools, capacity and resources to address the challenges linked to the evolving cyber threats landscape, which would be a significant improvement to the status quo. It will bring all the tasks of ENISA into its mandate, providing clarity of the scope and remit of the Agency, while ensuring the necessary prioritisation of its primary tasks. This option would ensure that the stakeholders receive adequate support for policy implementation, operational activities and overall coordination. Moreover, it would also foster effective synergies with other EU bodies and agencies. Option A.2 would also provide for a diverse resourcing mechanism, relying on the combination of resources from different sources, including creating own resources and integrating national liaison officers into the resource

structure. In this way, Option A.2 would contribute to the future-proof mandate of ENISA, to strengthening of the overall EU cybersecurity governance and, as a result, to the EU cyber posture and global leverage.

Option B.2 would highly contribute to address the problem of limited impact of the ECCF, addressing lack of clarity of the framework, expanding its scope and improving its governance model. The reputation of adopted schemes will be increased thanks to the establishment of a maintenance structure and the introduction of a timely and transparent development process. The extended scope of the framework will ensure that European schemes can effectively meet stakeholder needs for security assurance, including for entities. In addition to delivering a future-proof technical assurance tools, schemes will be further aligned with the existing legislative framework and hence better serve implementation efforts and support compliance needs of businesses. Combined with option D.3, the adoption of currently blocked schemes will be enabled.

Option C.2 will yield significant **economic benefits for businesses, including SMEs**, of more than **EUR 14.7 billion** and **for public authorities of EUR 7.5 million over five years**. It will limit fragmentation in cybersecurity measures and requirements, providing for legal clarity and substantially reducing the administrative burden, without leading to significant legal uncertainty among stakeholders that are in the process of adapting to the recently adopted legal frameworks. In combination with option B.2, this option would facilitate compliance for NIS2 entities, while also making the supervision process on the authorities' side more efficient.

Option D.3 provides for a long-term comprehensive solution to the ICT supply chain security issues. It provides for a balanced, risk-based framework to analyse the risk and provide for proportionate measures to reduce dependencies and de-risk the most critical ICT supply chains. Furthermore, the framework is horizontal, allowing to tackle supply chain security challenges in any of the critical and highly critical sectors. The framework allows for a risk-based, targeted and proportionate approach to identify the key assets, appropriate mitigation measures and, in case of restrictions or removal of high-risk supplier equipment, a reasonable phase-out period. Option D.3 provides already for identification of key assets in 5G networks based on the EU coordinated risk assessment in this area, ensuring harmonisation in the single market. As for other areas, the framework envisages conducting assessments to analyse the risks and the economic impacts and ensuring proportionality and necessity of the measures to be proposed at a later stage, once the implementing measures to address concrete critical supply chain are proposed.

Options A.2, B.2, C.2 and D.3 also represent the most efficient options. The benefits in terms of cyber resilience, administrative savings and procedural efficiencies are expected to surpass the overall costs. The preferred option will contribute to **strengthen the EU's cybersecurity posture and technological sovereignty, streamline compliance efforts, reduce market fragmentation and stimulate competitiveness, investments and innovation in trusted technologies**. The package would also be resilient to implementation challenges and would support long-term policy coherence across the digital and cybersecurity ecosystem.

The package consisting of Options A.2, B.2, C.2, D.3 is therefore recommended as the most appropriate and evidence-based course of action for the revision of the CSA, which would strengthen the defence operational capability of the EU.

### 8.2. REFIT (simplification and improved efficiency)

The revision of the CSA, through the selected policy options A.2, B.2, C.2 and D.3, strongly contributes to improving clarity, removing inefficiencies and aligning procedures across legal frameworks. More concretely, Option A.2 proposes a full reform of ENISA's mandate providing effective support for the policy implementation and an added value in terms of supporting operational cooperation among the Member States. This consolidation will also help eliminate fragmented practices, improving coordination while lowering compliance and operational costs in the long term. Option B.2, which involves repealing the current CSA and introducing a reformed ECCF, enhances efficiency by revising the governance model and supporting more predictable, coherent and agile certification procedures. This will allow for faster scheme adoption and better alignment with horizontal legislation, reducing regulatory fragmentation and easing the burden on both public and private stakeholders. Option C.2 reduces compliance costs for entities subject to relevant Union cybersecurity legislation, through scope changes and by enabling organisational cybersecurity certification schemes for entities in scope of the NIS 2 Directive and other legal acts. This approach will significantly simplify regulatory obligations for entities subject to multiple requirements and ensure a more effective use of resources across national authorities. Option D.3 creates a harmonised framework to tackle non-technical risks affecting ICT supply chains, reducing the current fragmentation of approaches across Member States. Together, these options represent a substantial simplification and modernisation of the EU's cybersecurity legal framework, fully aligned with the REFIT principles of clarity, efficiency and digital readiness.

### 8.3. Application of the 'one in, one out' approach

In line with the Better Regulation Toolbox, the *"One in, one out"* approach aims to ensure that any new administrative burden introduced by an initiative is balanced by the removal or reduction of existing burdens. This section identifies administrative costs (INs) and corresponding cost savings (OUTs) resulting from the preferred policy options (A.2, B.2, C.2, D.3) for businesses, public authorities and businesses. The detailed analysis table of the *"One in, one out"* approach can be found in *Annex 3, section 5*, supported by an SME check (*see Annex 6*).

**Administrative burdens introduced ("INs")**

The preferred option will somewhat increase administrative costs for businesses. Under A2, administrative costs would be limited to obtaining an authorisation to deliver European skills attestations. Under B.2, businesses choosing to pursue voluntary certification under the revised ECCF will face administrative costs stemming from obtaining (one-off) and maintaining (recurrent) a certificate. Recurrent costs could emerge from the continued need to comply with certification requirements such as by means audits and internal documentation. Under C.2, minor administrative costs could occur for updating reporting requirements (one-off and recurrent). Under D.3, no significant administrative costs could be identified.

To summarise, as outlined in *Annex 3 Table 7,* main **one-off and current administrative costs** for businesses would include:

- Certification (on voluntary basis): costs related to documentation and obtaining certificate (one-off and recurrent), as well as maintenance (e.g. audits). For cyber posture scheme, 30 000 EUR (one-off and recurrent) (B2)
- European skills attestation (on voluntary basis): costs for skills attestation vendor to obtain authorisation (one-off and recurrent) and to maintain it. (A2)
- Minor (one-off) costs related to adapting notification procedures for ransomware attacks (C2)

These costs would only occur to the extent businesses chose to engage in relevant activities (certification and skills attestation), except for ransomware reporting requirements. However, the latter are not expected to be significant compared to the BaU.

No significant administrative costs have been identified for public authorities and citizens.

**Administrative savings ("OUTs")**

Despite the above INs, the preferred options would also generate meaningful administrative cost reductions for businesses, which would qualify as OUTs under the *"One in, one out"* approach. Those savings would include:

- NIS2 scope removals for DNS providers and other entities: **EUR 1.35 bn** over five years (EUR 94 355 per entity for 28 700 entities)
- NIS2 new mid-cap category: EUR 212 million per year (EUR 94 355 per entity for 22 500 entities) totalling **1,06 bn EUR over five years**
- NIS2 compliance through cyber posture scheme: **EUR 30 million** per year as of 2032 **of administrative cost savings** (for 1000 companies – EUR 30 000 per year per entity) **and over the five years** considered in the report.

This would lead to a total of **EUR 2.4 bn over five years** (2028-2032) affecting in total 52 200 companies, including SMEs.

For **public authorities**, cost savings include EUR 1.5 millionof supervision costs due to the cyber posture scheme, totalling **EUR 7.5 million over five years**.

For citizens, no significant administrative cost savings could be identified.

**Conclusion**

The preferred option introduces significant administrative cost savings and can be considered compliant with the *"One in, one out"* principle.

### 8.4. SME test

In line with the Better Regulation Toolbox, an SME test has been carried out, as this initiative is highly relevant for SMEs. The preferred policy option that improves legal clarity, aims at simplification and reduces reporting obligations, will bring several direct benefits for SMEs, e.g. decreased compliance costs. The most relevant sectors impacted are ICT manufacturing and ICT services, where about 1.2 million SMEs operate, impacting about 4-5 million workers. However, there are also SMEs indirectly affected in other sectors. The ICT supply chain framework and possible restrictions of high-risk suppliers or entities originating from or controlled by countries posing cybersecurity of

concerns could also strengthen the competitive stance of SMEs, which could be leveraged in integrating, procuring, and distributing ICT products and services. Additionally, there are indirect positive impacts, such as enhanced cross-border interoperability, facilitated by ENISA's expanded mandate and through standardised reporting practices. Enhancing the cybersecurity framework, streamlining certification processes and simplifying compliance supports the achievement of the 35% burden reduction target for SMEs. Moreover, due to ENISA's increased engagement in handling cybersecurity incidents, it is projected that the costs incurred by affected entities could be reduced by 15% to 20% *(see Annex 6).*

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

The effectiveness of the initiative will be assessed through regular monitoring and evaluation of its main components: ENISA's mandate, the ECCF, and the simplification of compliance with cybersecurity requirements. An evaluation of the act would be foreseen four to five years after the entry into force and every four years thereafter, with the findings presented in a report to the European Parliament and the Council. To enable this assessment, a set of qualitative and quantitative indicators will be monitored over time. These will rely on existing sources such as ENISA's annual activity reports, Member States', and Commission-led consultations with businesses and consumers. ***Annex 15*** outlines the potential and non-exhaustive indicators, baselines, frequencies of data collection, targets and data sources for each of the specific objectives.

# ANNEX 1: PROCEDURAL INFORMATION

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

Lead DG: Directorate-General for Communications Networks Content and Technology (CNECT).

Decide: PLAN/2024/2819.

Policy objective A new plan for Europe's sustainable prosperity and competitiveness

## 2. ORGANISATION AND TIMING

The Cybersecurity Act revision constitutes a key part of the digital single market and as announced in **the ProtectEU strategy[1], t**he upcoming revision of the Cybersecurity Act will look to improve the European Cybersecurity Certification Framework, to ensure that future certification schemes can be adopted in a timely manner and respond to policy needs and will look more broadly at the security and resilience of ICT supply chains and infrastructure. The revision is looking as well at amending the mandate of the European Union Agency for Cybersecurity (ENISA) and provides for simplification and facilitation of compliance with the existing cybersecurity legal framework.

It is based on Article 114 TFEU since it empowers the European Union to adopt measures aimed at establishing and ensuring the functioning of the internal market. Regulation (EU) 2019/881, the Cybersecurity Act, was originally adopted under this provision. The impact assessment process started with the launch of a public consultation and publishing the Call for Evidence to gather feedback from stakeholders for a period of 10 weeks from 11 April 2025 to 20 June 2025. For a detailed analysis of the consultation process, see *Annex 2*. The inter-service group (ISG) met on for the informal meeting on 9 January 2025 and for the ISG on 21 May 2025, on 26 June 2025 and on 18 July 2025 before submission of the Staff Working Document to the Regulatory Scrutiny Board (RSB) on 27 August 2025. The ISG consists of representatives of the Secretariat-General, and the Directorates General CNECT, JUST, GROW, FISMA, ENER, HOME, SANTE, EEAS, TRADE, GROW, TAXUD, DIGIT, INTPA, HR, AGRI, EMPL, EAC, BUDG, ENEST, DEFIS, MOVE, ECFIN, COMP, SJ and JRC.

## 3. CONSULTATION OF THE RSB

On 27 August 2025, DG CNECT submitted the draft Impact Assessment to the RSB, in view of a hearing which took place on 24 September 2025. On 26 September, the RSB issued a negative opinion. On 9 October, the ISG group met before resubmission of the Staff Working Document to the Regulatory Scrutiny Board (RSB). On 20 October 2025, the Impact Assessment to the revision of the Cybersecurity Act was resubmitted to the RSB. On 13 November 2025, the RSB issued 'positive opinion with reservations'. The remarks of the RSB were addressed in this Impact Assessment as follows below.

**Changes made in the revised version of the impact assessment report**

The table hereafter provides an overview of the main changes made in the revised version of the impact assessment report in the light of the RSB recommendations accompanying its second positive opinion on the draft assessment report. In addressing these points, the lead Service has further extensively reviewed the draft impact assessment report.

*Table 1: Changes made in the revised version of the impact assessment report*

| **RSB Opinion Point** | **Key issue/what to improve** | **Addressed in revised IA report: section number and annex** | **How have the issues been addressed** |
|---|---|---|---|
| (B)(1) | The report does not provide sufficiently clear and robust estimates of the benefits of the intervention. | Sections 6.1.1.1(a)<br><br>6.1.1.1(b)<br><br>6.2 | The cost savings of European individual cybersecurity skills attestation schemes for public authorities, citizens, and businesses have been complemented with qualitative analyses by adding the benefits for national authorities, detailing the benefits for citizens and clarifying the added value for SMEs. The table on *Benefits of policy options A (ENISA mandate)* has been updated accordingly.<br><br>Regarding compliance costs for ENISA, cost-offsetting estimation was added to cover the share of providers that should participate in European individual cybersecurity skills attestation schemes to cover operational costs. |
| (B)(2) | The report does not sufficiently present the rollout of measures aiming to enhance ICT supply chains security for critical sectors, nor the form of subsequent impact | Section 5.2.2 option D.3 | Further clarifications were included regarding the description of the framework and how the framework could be initiated and roll-out |

| | | | |
|---|---|---|---|
| | assessments. | | |
| (B)(3) | The report is unclear about the problems and impacts related to the simplification measures targeting the NIS2 Directive. | Sections 2.1.3, 2.2.8, 6.2.2 | Added analysis of issues around NIS2 scope in the explanation of the problem and the problem driver. Added explanation on the resilience implications of adjusting NIS2 scope in section 6.2.2. |
| (C)(1) | The report should further specify key concepts and parameters of the initiative along two axes: the distinction and interplay between technical vs non-technical cybersecurity risks, and the mandatory vs non-mandatory application of the proposed measures across the policy options | Section 2.1.4.1 | Problem 4 "Key concepts" subsection was complemented to add the interplay between technical and non-technical risks and subsequently renamed to cover this interplay. |
| | | Section 5.2.2 option B.1, section 5.2.4 option D.3 and section 5.5 | Clarifications were inserted regarding interlinkages between certification and supply chain options, in particular, a clarification was added that an entity does not have to be certify not to be considered a high-risk supplier (certification remains voluntary for options B.1 and B.2). |

| | | | |
|---|---|---|---|
| (C)(2) | The report should provide more informative and more granular estimates of the benefits anticipated from the intervention, including avoided cyber incidents. It should further analyse the main types of incidents (malicious vs non-malicious, technical vs non-technical risks etc.), and their distribution. To the extent possible, the probabilities and costs of the diverse types of such cyber incidents need to be transparently quantified. The report should better substantiate the estimates of<br><br>faster recovery times. | Section 6.1.1.1. b) | The report elaborates on the rationale for the estimates chosen to quantify the benefits linked to the impact of cybersecurity incidents. In terms of avoided cybersecurity incidents, explanations related to the available data and their limitations are further explained in the report. Additional clarifications are included to explain the choice of the quantitative methodology based on faster recovery times as proxy to estimate the impact of the proposed measures. The quantitative data provide has been further nuanced. |
| | It should better demonstrate the added value of measure on skills. | Sections 6.1.1.1(a)<br><br>6.1.1.1(b)<br><br>6.2 | See line (B)(1) on European individual cybersecurity skills attestation schemes<br><br>Additionally, compliance costs for public authorities and businesses were clarified, distinguishing in the text between administrative costs and adjustment costs. Adjustment costs were further explained, in particular the cost variation from one provider to another and from one scheme to another, specifying as well the frequency (one-off/recurring) of the costs.<br><br>Additionally, an explanation was added regarding how the potential barrier to entry for SMEs caused by a fee could be lifted. |

| | | | |
|---|---|---|---|
| | | | The table on *Costs of policy options A (ENISA mandate)* was updated accordingly. |
| | An improved assessment of avoided costs and benefits for companies should be used as a basis for a strengthened analysis of effectiveness, efficiency and competitiveness. | Sections 7.1, 7.2, 7.3 | Explanation added regarding the limitation of data and the difficulties in quantifying the causality between the measures included in the different policy options and related cost savings in terms of probability and impact of cybersecurity incidents.<br><br>Based on those limitations and improved assessment of avoided costs and benefits, the comparison of options under criteria effectiveness and efficiency (that also includes competitiveness aspects) was adjusted. |
| (C)(3) | Claims regarding the effectiveness and efficiency of the intervention need to reflect any limitations and uncertainties in the analysis of benefits and costs. The assumptions and estimates underlying the main costs should be subject to sensitivity analysis. | Section 7.1<br><br>Section 6.1.1.1 | Explanation added regarding the limitation of data and the difficulties in quantifying the causality between the measures included in the different policy options and related cost savings in terms of probability and impact of cybersecurity incidents.<br><br>The financial impacts of extended ENISA mandate and more effective certification were assessed in further detail (6.1.1.1). It was clarified that the additional EUR 148.12 million is an incremental cost compared to the baseline cost and it does not include ongoing activities. A comparison of these additional costs compared to ENISA's current annual budget and staffing level was provided. It |

| | | | |
|---|---|---|---|
| | | | was clarified that certification-related FTEs (Option B.2) do not overlap with ENISA Option A.2, and that the costs are mutually exclusive. The list of operational pillars under A2 was complemented and justifies now the full amount. |
| | The report is insufficiently clear on the nature and components of the various costs and cost-savings as well as the economic impact of replacement costs for ICT supply chain restrictions on the businesses in scope and downstream. | Section 6.1.1.5 | Further explanations were included regarding the nature and components of the various costs and costs savings, including the replacement costs of ICT supply chain restrictions. |
| (C)(4) | Regarding the ICT supply chain restrictions, the report should provide clearer<br><br>explanations on the estimated range in annual replacement costs, including the<br><br>assumed proportion of equipment considered non-upgradeable or sourced from<br><br>high-risk suppliers. The transfer of costs to consumers should be more clearly<br><br>analysed. Claims that short-term costs will be offset by new revenues for trusted<br><br>suppliers or a more trustworthy offering for citizens should be substantiated with<br><br>evidence. | Section 6.1.1.5 | The explanation regarding the estimated range in annual replacement costs have been clarified in the text of the main report, including the proportion of equipment considered non-upgradeable or sourced from high-risk suppliers.<br><br>The potential transfer of costs to consumers has been further explained and nuanced as one potential strategy of companies.<br><br>Explanations have been added in the report regarding the claims that costs for operators would be offset by revenues for trusted suppliers. |

| | | | |
|---|---|---|---|
| (C)(5) | The report should better explain how the proposed ICT supply chain security framework will be rolled out and the form of the subsequent impact assessments for the sectors in scope of the framework respecting the Better Regulation guidelines and toolbox. | Section 4.2 specific objectives | Specific objective 5 updated |
| | | Section 5.2.2 option D.3 | Further clarifications were included regarding the description of the framework and how the framework could be initiated and roll-out, including |
| (C)(6) | The report should further analyse the interlinkages between options on<br><br>certification and options for supply chain restrictions, for example if it will be<br><br>possible for companies to avoid the fees and costs associated with certification if<br><br>they want to be able to form part of approved supply chains. | Section 5.2.2 option B.1, section 5.2.4 option D.3 and section 5.5 | Clarifications were inserted regarding interlinkages between certification and supply chain options, in particular, a clarification was added that an entity does not have to be certify not to be considered a high-risk supplier (certification remains voluntary for options B.1 and B.2). |

| | | | |
|---|---|---|---|
| | The report should clearly outline the current scope of the tasks of ENISA and the scope of ECCF and better demonstrate any identified gaps. | Annex 10, new table<br><br>Section 5.1 | Annex 10 was reviewed to distinguish between the scope of the tasks of ENISA and the scope of the ECCF in the current mandate, leading to two distinct tables:<br><br>• General overview of ENISA's key stakeholders, their expectations and unmet needs in relation to ENISA's current tasks<br>• ENISA's key stakeholders, their expectations and unmet needs in relation to the ECCF<br><br>Further clarifications what is now in the scope of ENISA's mandate and the ECCF and what are the gaps. |
| | The report should better distinguish<br><br>problem drivers related to the implementation and management from those related<br><br>to the scope. | Section 2.2, new table | Elements of the drivers were identified and divided into two categories: "scope" and "implementation and management", reflected in a new table |
| (C)(7) | The report should analyse the problems, and the problem drivers related to the simplification of NIS2. The report should transparently outline possible measures including changes in the scope and assess how these measures would reduce costs for companies and what the impacts on cybersecurity would be. | Sections 2.1.3, 2.2.8, 6.2.2 | Added analysis of issues around NIS2 scope in the explanation of the problem and the problem driver. Added explanation on the resilience implications of adjusting NIS2 scope in section 6.2.2. |

| | | | |
|---|---|---|---|
| (C)(8) | The report should further address the most significant gaps concerning administrative costs and cost savings, ensuring comprehensive coverage beyond businesses. Transparent classification is needed, distinguishing between compliance and administrative costs. All costs should be categorised in a comparative manner, respecting distinctions between one-off/recurring and annual/over 5 years costs. | 6.1.1.3; Annex 3 section 5<br><br>Section 8.3.<br><br>Section 6.1.1. | Clarifications were added to indicate which cost savings arising from Option C.2 are interpreted as administrative costs.<br><br>Accordingly, the 'one-in-one-out' calculations have been reviewed. The impact on public authorities and citizens has been made explicit.<br><br>The classification of costs has been reviewed throughout the document to ensure a transparency classification following the Better Regulation Toolbox #56. |
| (C)(9) | The report should be reduced in length, avoiding repetitions, in line with better regulation requirements. | | The overall report has been reviewed in view of possible shortening of the text. |

## 4. EVIDENCE, SOURCES AND QUALITY

The Commission carried out an extensive consultation in preparation of this Impact Assessment report. It benefited from preparatory activities conducted in 2024 in the framework of the Evaluation of European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework[181].

To collect evidence and different insights to support the revision of the Cybersecurity Act, the Commission conducted the public consultation aimed at collecting perspectives from different stakeholders and collected the feedback through the Call for Evidence. To ensure a comprehensive level of coherence and comparability of analysis and assess potential policy approaches, the Commission also conducted targeted consultation. These series of structured interviews were conducted with selected stakeholders ranging from ENISA representatives, public authorities to certification experts, and delved deeper on more technical or strategic issues. To guarantee that the analysis of the policy options benefits

[181] The 2024 Evaluation report.

from the contributions of other institutional stakeholders and more accurately reflects the perspectives of Member States, the Commission also collected evidence stemming from high-level discussions held with Member States representatives, in particular within the working party of the Council of the EU, in the NIS Cooperation Group and within the ECCG.

In addition to the Commission's public consultation and feedback on the Call for Evidence, extensive desk research was conducted, covering a wide spectrum of policy studies and reports. They have been quoted in the main body of the Impact Assessment.

The quality of the analytical methods is detailed in *Annex 4*.

# ANNEX 2: STAKEHOLDER CONSULTATION (SYNOPSIS REPORT)[182]

## 1. CONSULTATION SCOPE AND OBJECTIVES

The stakeholder consultation supported the revision of the Cybersecurity Act by gathering evidence and practical insights from those affected. It contributed to the impact assessment by refining the problem definition, objectives, and policy options, and explored perceptions of the current framework, implementation challenges, and possible improvements.

The consultation focused on five core areas identified as central to the future functioning and coherence of the EU cybersecurity framework:

- **ENISA's mandate and operational role**, including support for Member States and expertise in emerging technologies.
- **Effectiveness of the European Cybersecurity Certification Framework (ECCF)**, including governance and development processes.
- **Complexity and fragmentation of cybersecurity obligations**, with attention to reporting burdens and potential simplification.
- **Proportionality of requirements for SMEs** and the potential for differentiated compliance paths.
- **Societal and economic impacts** of harmonised cybersecurity rules, including effects on consumers, rights, innovation, and competitiveness.

The insights gathered through the stakeholder consultation informed every step of the impact assessment. Stakeholder feedback helped refine the problem definition, test the relevance of proposed measures, and calibrate the design of policy options. Input was particularly influential in shaping proposals around certification governance, lifecycle obligations, and reporting simplification.

## 2. MAPPING OF STAKEHOLDERS

To ensure that the consultation captured a wide range of views and experiences, stakeholders were mapped according to their position in the cybersecurity ecosystem, their level of technical and operational involvement, and their potential exposure to regulatory changes. This mapping was used to tailor the consultation activities, ensuring a balanced and inclusive approach. Stakeholder categories to be consulted included:

---

[182] **Disclaimer:** The information and views set out in this document reflect the input received through the public consultation conducted via the European Commission's 'Have Your Say' web portal. These contributions cannot be regarded as stating an official position of the European Commission or its services. They do not bind the Commission in any way. Moreover, the responses received cannot be considered as a statistically representative sample of the EU population.

- **EU institutions and decentralised agencies**: This group includes EU institutions and EU-level bodies involved in cybersecurity policy, oversight, or implementation. Their input focused on cross-border coordination, regulatory coherence, and alignment with broader EU objectives.

- **National Public authorities:** This group comprised national cybersecurity agencies, competent ministries, regulators and EU institutions responsible for the oversight, enforcement or coordination of cybersecurity policy.

- **Businesses:** Companies involved in the production, distribution or operation of digital products and services were targeted, including hardware manufacturers, software developers, cloud service providers, and cybersecurity solution vendors. These stakeholders are users and subjects of certification schemes and cybersecurity obligations.

- **Business and industry associations:** These organisations represent the collective interests of companies operating in relevant sectors and often act as intermediaries in consultations. Their input reflects the aggregated concerns of both large and small enterprises, including sector-specific challenges.

- **Small and medium-sized enterprises:** SMEs were consulted both directly and via associations. Given their limited resources compared to larger firms, their perspective was critical in assessing the proportionality and accessibility of the current and future regulatory framework.

- **Academic and research institutions:** Institutions with expertise in cybersecurity, standardisation, policy evaluation and digital innovation were consulted for their analytical and technical input. Their contributions supported a more robust assessment of the strengths and limitations of the current framework.

- **Consumer and civil society organisations:** These groups were consulted to ensure that the public interest, including privacy, digital rights, transparency, and security-by-design principles, was reflected in the assessment. They also provided insights on user-facing issues such as product labelling and minimum-security guarantees.

- **Trade unions:** Given the growing importance of cybersecurity in critical infrastructure sectors, input was also gathered from labour organisations with knowledge of workplace safety, workforce digitalisation, and cybersecurity skills.

- **Individual citizens:** Members of the general public were invited to contribute their views particularly with regard to their experiences as users of digital products and services, their perceptions of cybersecurity risks, and their expectations for protection and transparency.

The consultation strategy aimed to ensure balanced representation across these groups and to avoid over-reliance on any single category. The mapping exercise also informed the

development of survey logic and interview targeting, ensuring that different types of stakeholders were asked relevant questions.

## 3. CONSULTATION ACTIVITIES

The consultation activities aimed to collect stakeholder views on the key areas under review: the role and functioning of ENISA, the ECCF, and the simplification of reporting obligations. These inputs helped assess the current framework and inform the design of potential policy options. The main activities were:

- **Call for evidence:** Stakeholders were invited to submit written contributions, including position papers, technical reports, or comments on specific reform proposals. These submissions allowed for the presentation of detailed arguments and documented evidence, which could not be fully captured through the structured survey format. A total of 184 individual contributions were received from a broad range of stakeholder categories, including industry associations, cybersecurity firms, SMEs, academic institutions, and public interest organisations. Contributions originated from both EU and non-EU countries, ensuring diverse representation across the cybersecurity ecosystem. This activity provided a rich source of qualitative input, reflecting the perspectives of businesses, academia, and civil society on the mandate of ENISA, the certification framework, and the simplification of cybersecurity obligations.

- **Public consultation (PC):** The PC was conducted in the context of the ongoing revision of the Cybersecurity Act (Regulation (EU) 2019/881), running from 11 April to 20 June 2025. It aimed to gather feedback from a wide range of stakeholders on the effectiveness of the current legislative framework and potential areas for improvement. The consultation consisted of 38 questions, both closed and open-ended, covering the cybersecurity certification framework, ENISA's mandate, governance structures (ECCG, SCCG), and broader issues such as fragmentation, compliance burden, supply chain risks, and harmonisation. The survey was open for 10 weeks (shorter than the standard 12 weeks due to legislative planning needs), and respected the Commission's minimum standards for stakeholder engagement, including clear objectives, accessible tools, transparent data processing, and integration of feedback into policy design.

The consultation was launched through the European Commission's EU Survey online platform and was open to all stakeholders. A total of 193 responses were received, with partial responses accepted. Quantitative and qualitative data were analysed using statistical and text-mining techniques, with results broken down by stakeholder type, company size, and country of origin. The consultation attracted a diverse pool of respondents from various stakeholder groups. The breakdown below shows the number and proportion of responses by stakeholder type, reflecting balanced input from both private and public sector actors, as well as individual citizens.

*Table 2: Respondents by stakeholder type (n = 193)*

| Stakeholder type | Number of respondents | Percentage (%) |
|---|---|---|

| | | |
|---|---|---|
| Company / business | 79 | 40.9 % |
| Business association | 54 | 28.0 % |
| EU Citizen | 26 | 13.5 % |
| Public authority | 8 | 4.1 % |
| Other | 8 | 4.1 % |
| Academic / research institution | 7 | 3.6 % |
| Non-governmental organisation | 6 | 3.1 % |
| Trade union | 4 | 2.1 % |
| Non-EU citizen | 1 | 0.5 % |

Among company and business respondents, a majority represented large enterprises, though a substantial share of micro, small, and medium-sized enterprises also participated. The table below provides a detailed breakdown of company size.

*Table 3: Company size distribution among business respondents (n = 79)*

| **Company size** | **Number of respondents** | **Percentage (%)** |
|---|---|---|
| Large enterprises | 50 | 63.3 % |
| Medium-sized enterprises | 8 | 10.1 % |
| Small enterprises | 9 | 11.4 % |
| Micro enterprises | 12 | 15.2 % |

Total number of SMEs (micro + small + medium): 29 (36.7 %)

Responses were received from across 26 countries, including all EU Member States and a few non-EU countries. The table below presents the distribution of respondents by country, sorted by descending order, with non-EU countries grouped under "Other countries" unless they recorded a significant number of replies.

*Table 4: Respondents by country (n = 193)*

(Non-EU countries grouped under "Other countries" unless they had relevant participation)

| **Country** | **Number of respondents** | **Percentage (%)** |
|---|---|---|
| Belgium | 30 | 15.5 % |
| France | 27 | 14.0 % |
| Germany | 23 | 11.9 % |
| United States | 14 | 7.3 % |
| Spain | 11 | 5.7 % |
| Italy | 10 | 5.2 % |
| Hungary | 9 | 4.7 % |
| Austria | 9 | 4.7 % |
| Netherlands | 8 | 4.1 % |
| Poland | 6 | 3.1 % |
| Czechia | 6 | 3.1 % |
| Ireland | 5 | 2.6 % |
| Greece | 5 | 2.6 % |
| Cyprus | 3 | 1.6% |
| Sweden | 2 | 1.0 % |
| Bulgaria | 2 | 1.0 % |
| Luxembourg | 2 | 1.0 % |
| Estonia | 2 | 1.0 % |
| Slovakia | 2 | 1.0 % |
| Finland | 2 | 1.0 % |
| Malta | 1 | 0.5 % |
| Latvia | 1 | 0.5% |
| Other countries[2] | 10. | 1. % |

- **Targeted consultation (interviews):** A series of semi-structured interviews were conducted with selected stakeholders. These included ENISA's representatives, as well as national public authorities that developed or manage national reporting platforms. Interviews focused on ENISA's role and capacity, the operational functioning of the ECCF, practical challenges in aligning national and EU-level certification processes, reporting burdens, and implementation obstacles. These discussions provided qualitative insights that enriched the interpretation of PC results and supported the refinement of policy options.

Interview participants included ENISA representatives (such as Heads of Unit), national cybersecurity agencies, competent ministries, regulators, and certification experts. This ensured coverage of both EU-level and Member State perspectives, with a focus on institutional and expert stakeholders directly involved in the implementation and governance of cybersecurity policy.

- **The 2024 Evaluation report:** The final report of the *Study to Support the Evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework carried out for the Commission by PwC, Intellera Consulting, PPMI (2024) was* completed in December 2024[183].

The study included 65 interviews - of which 52 focused more on ENISA and 13 concentrated most of the questions on the ECCF - a survey programme with 209 responses (of which 70 were on the ECCF), the results of the public consultation, and two workshops on SWOT analysis and recommendations with 26 and 70 participants respectively. (See also Annex 7 for more details).

- **Consultation of Member States representatives within the framework the Council working party and in bilateral discussions,** where Member States could express their views on the review of the Cybersecurity Act.

- **Targeted consultation (ECCF groups – ECCG, SCCG):** The Commission in its capacity as the chair of both groups has presented the state-of-play on the revision of the Cybersecurity Act at the previous ECCG meetings on 12 March and 3 July 2025, and SCCG meeting on 17 March. In addition, supplementary expert opinions from ECCG members were collected through a tailormade questionnaire designed to explore key questions to inform a potential revision of the ECCF.

No campaign-type submissions or coordinated responses were identified during the consultation.

This combination of consultation activities ensured the robustness and transparency of the evidence base underpinning the impact assessment. It enabled the European Commission

[183]The study is available at: https://data.europa.eu/doi/10.2759/7122638; its final report (summary) at: https://data.europa.eu/doi/10.2759/7260328; and the annexes to the study at: https://data.europa.eu/doi/10.2759/6529756

to gather information from both generalist and expert perspectives and to triangulate findings across methods and stakeholder categories. Advanced computational tools were used to support the analysis of data gathered through these consultation activities. Generative Pre-trained Transformer (GPT) technology employing robust security measures and encryption protocols to ensure the confidentiality and integrity of data was used. Human oversight remained central in the analysis to ensuring accuracy, interpreting nuanced results, and making informed decisions based on the insights generated by GenAI.

## 4. SUMMARY OF CONSULTATION RESULTS

This section presents a synthesis of stakeholder feedback collected through three main consultation activities: the Call for Evidence, the Public Consultation, and targeted Interviews. The analysis follows the thematic structure of the public consultation questionnaire, covering the mandate and operational role of ENISA, the ECCF, and the simplification of reporting obligations. For each topic, findings from the Call for Evidence and interviews are integrated alongside survey results, with sources clearly indicated.

### *4.1 Section 1: ENISA's mandate*

Stakeholders contributing to the Call for Evidence expressed strong support for enhancing ENISA's role and capabilities. Many emphasised the importance of increasing ENISA's funding, staffing, and operational capacity to enable it to meet the growing demands of the EU's cybersecurity landscape. There was also a recurring call for clarifying and consolidating ENISA's mandate before considering any expansion. Some contributors cautioned against overextending ENISA's responsibilities, suggesting that its current functions should be streamlined and reinforced first. Additionally, several stakeholders advocated for improved governance structures and better alignment with broader EU digital and cybersecurity strategies, such as the NIS2 Directive and the Digital Decade initiative. Concerns were also raised about the potential for duplication of efforts with national authorities, with some contributors urging caution to avoid overreach and inefficiencies.

Interviews with ENISA's Heads of Unit highlighted the agency's evolving role in EU cybersecurity. ENISA representatives emphasised the need to formalise ENISA's de facto leadership in networks such as the CSIRTs network and EU-CyCLONe, and to facilitate more effective cooperation within these structures. They called for scaling up existing initiatives like the Cyber Partnership Programme and enhancing infrastructures supporting operational cooperation. ENISA was also seen as well-positioned to support harmonisation of cybersecurity practices, provide sector-specific guidance, and lead on vulnerability services and strategic foresight. Interviewees identified a flexible mandate, stronger collaboration frameworks with Member States, and improved access to funding as key enablers for these goals.

The stakeholder consultation provided more detailed information regarding the current tasks of ENISA, its support to policy implementation, the provision of technical support, its collaboration with other bodies, support in situational awareness, and also about skills and awareness. These findings are summarised hereafter.

**Current tasks of ENISA**

The consultation assessed stakeholders' views on the relevance of the eight core tasks currently assigned to ENISA. Respondents were asked to indicate the importance of each task on a five-point scale. The results reveal broad support for maintaining ENISA's mandate, with significant differences in perceived importance across stakeholder groups, especially between public authorities, businesses of different sizes, and EU citizens.

Across all respondents, the task most frequently rated as "Very important" was *market, cybersecurity certification, and standardisation* (58.6%), followed by *development and implementation of Union policy and law* (47.2%), and *operational cooperation at Union level* (45.1%). *Research and innovation* was least often rated "Very important" (20.2%).

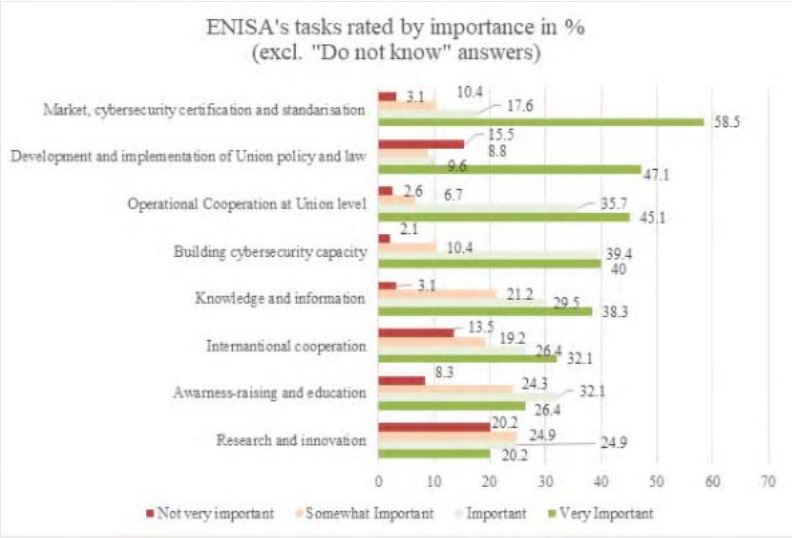



*Figure 1 Stakeholder's views in ENISA's tasks rated by importance*

Large companies consistently supported most tasks, with 60% rating *certification and policy implementation* as "Very important", and 58% for *operational cooperation. International cooperation* (44%) and *knowledge/information* (42%) were also valued, while *awareness/education and research* received lower ratings. Medium-sized companies showed more selective support, prioritising *certification and operational cooperation* (37.5%), with lower ratings for other tasks, indicating a focus on practical support. Small and micro enterprises placed greatest emphasis on *certification* (66.7% "Very important"), but gave less importance to *strategic, educational, or analytical* roles.

EU citizens expressed high support for *knowledge/information* (53.9%) and *certification* (57.7%), and significant shares valued *awareness/education and international cooperation* (both 42.3%), highlighting the importance of transparency and public protection.

Public authorities emphasised ENISA's coordination and compliance roles, with 62.5% rating *policy implementation, operational cooperation, and certification* as "Very important", but less emphasis on *capacity-building, awareness, research, and international cooperation.*

In conclusion, the tasks of *cybersecurity certification*, *operational cooperation*, and *policy implementation* received the strongest and most consistent support across stakeholders. These functions are seen as central to ENISA's mandate. On the other hand, *research and innovation*, *awareness-raising*, and *capacity-building* were viewed as lower priorities by most business and institutional actors, although citizens valued them more highly. These findings suggest that while ENISA's overall mandate is seen as appropriate, its activities could be more clearly differentiated in terms of audience relevance and impact.

**ENISA providing support in policy implementation**

This section describes stakeholders' views on ENISA's support for Union cybersecurity policy, focusing on assistance to Member States, support to the Commission, guidance to industry, and international cooperation. Results show broad support for ENISA's policy-related functions, with differences across stakeholder groups. Assisting Member States and supporting the Commission were most frequently rated as "Very important" (both 45.6%), followed by industry guidance (43.5%). International cooperation received 27.5%.

Large companies consistently rated all areas highly, with 56–60% considering assistance to Member States, support to the Commission, and industry guidance as "Very important", and 48% for international cooperation. Public authorities were even more supportive: 75% rated assistance to Member States and support to the Commission as "Very important", and 62.5% for industry guidance. Only 12.5% of public authorities considered international cooperation "Very important", showing a preference for ENISA to focus on internal EU coordination. Medium-sized companies showed more selective support: 50% rated assistance to Member States as "Very important", 25% for industry guidance, and lower ratings for other areas. Small companies prioritised industry guidance (55.6% "Very important"), but gave less importance to other functions, especially international cooperation. Micro enterprises valued industry guidance most (41.7% "Very important"), but showed limited support for other areas.

EU citizens showed high support for all tasks, especially assistance to Member States (42.3%), support to the Commission (42.3%), and industry guidance (46.2%), though international cooperation was less frequently rated as "Very important" (23.1%). Business associations showed a balanced view, with around 40–46% rating the first three areas as "Very important", and moderate support for international cooperation.

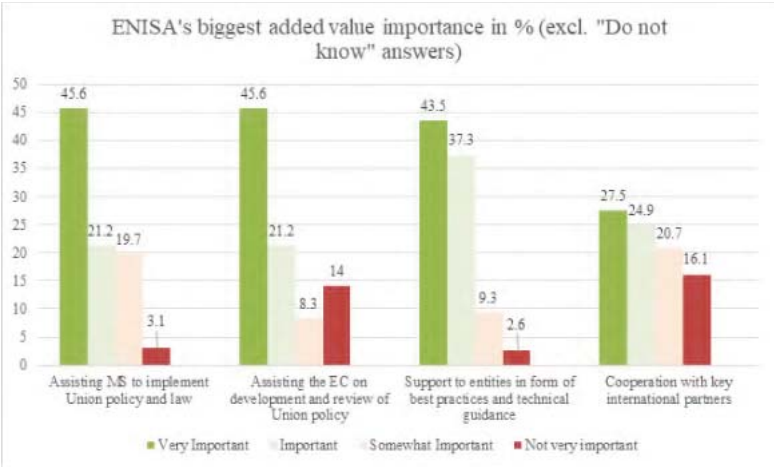



*Figure 2 Stakeholder's views on ENISA's biggest added value*

Assisting Member States, supporting the Commission, and providing industry guidance received the strongest and most consistent support across stakeholders, and are central to ENISA's mandate. International cooperation, while valued, was a lower priority for most business and institutional actors, although large companies and non-EU respondents rated it more highly. ENISA's mandate is seen as appropriate, but its activities could be more clearly differentiated by audience relevance and impact.

Open-ended questions highlighted strategic and operational opportunities for ENISA. Several stakeholders proposed expanding ENISA's mandate to address emerging technological challenges, including cybersecurity standards for artificial intelligence, the Internet of Things, quantum computing, and 6G networks. Others emphasised the need for ENISA to coordinate professional training and certification frameworks with universities and industry associations, especially in areas such as 5G/6G security, incident management, and critical systems auditing.

There was strong support for ENISA to play a more active role in developing open security standards and promoting secure-by-design protocols, especially for interoperability across digital services and infrastructure. Some respondents called for ENISA to strengthen its position as a European cyber intelligence hub, providing forward-looking analysis on threats such as ransomware, vulnerabilities in critical infrastructure, and quantum computing risks.

Stakeholders suggested ENISA could help harmonise audit procedures and reporting practices across Member States, reduce regulatory fragmentation, and support common cybersecurity practices. Others advocated for more structured engagement with industry, including appointing national liaison officers to facilitate dialogue and responsiveness. Additional proposals included simplifying and reducing the cost of cybersecurity certification, supporting sovereign European cybersecurity projects, and mapping alternatives to non-European technologies.

These contributions reflect a shared desire for ENISA to become a more proactive, technically authoritative, and strategically aligned agency that supports policy

implementation and drives innovation, coherence, and resilience across the European cybersecurity landscape.

**ENISA providing technical support**

This section describes stakeholders' views on ENISA's technical support role, focusing on whether additional technical tasks should be added to its mandate and how well it performs its current responsibilities. Responses were more divided than for policy implementation, with many stakeholders expressing uncertainty or reservations about expanding ENISA's technical scope.

When asked about integrating additional technical tasks, 28.5% supported expansion, 42.5% opposed, and 29% had no opinion. Business associations were split, large companies leaned toward uncertainty, and medium-sized, small, and micro enterprises were generally opposed or undecided. EU citizens were cautious, with half opposing expansion, while trade unions were strongly supportive. Public authorities were evenly divided, and other respondents showed mixed views.

Open-ended responses suggested a wide range of potential technical tasks for ENISA, such as developing frameworks for vendor participation, supporting mutual recognition of certifications, enhancing incident reporting interoperability, and integrating threat intelligence. Stakeholders also called for ENISA to harmonise regulatory practices, assist in auditing, create sovereign cybersecurity tools, and evaluate supply chain risks. Further suggestions included developing risk assessment tools, sector-specific training modules, standardized reporting templates, and support centres for Member States and critical infrastructure. There was also support for ENISA to lead initiatives in certification simplification, cloud security, stewardship of critical software, guidance on emerging technologies, and coordinating cybersecurity exercises.

When asked about ENISA's current technical performance, 25.4% said yes, 28% said no, and 46.6% had no opinion. Business associations and large companies were cautious, medium-sized companies were more critical, and small and micro enterprises were generally sceptical. EU citizens and non-EU respondents expressed dissatisfaction, while public authorities and trade unions were more supportive.

This reveals a more cautious and divided perspective on ENISA's technical role. Some stakeholders, especially trade unions, public authorities, and large companies, support expanding ENISA's technical mandate, while small and micro enterprises express scepticism or uncertainty. Open-ended responses show strong interest in more proactive and technically robust engagement from ENISA, but the mixed quantitative results indicate that any expansion of its technical functions should be carefully aligned with stakeholder expectations and capacities.

**ENISA's collaboration with other bodies**

This section covers ENISA's collaboration with other EU agencies, bodies, and institutions, and whether these partnerships should be better specified in the founding act.

Results show diverse perspectives on the clarity and structure of ENISA's institutional relationships.

Overall, 37.8% of respondents agreed and 18.7% strongly agreed that ENISA's partnerships should be better defined, while 17.1% disagreed, 2.6% strongly disagreed, and 23.8% had no opinion. This indicates a general tendency towards agreement, but with varied intensity and a notable share without opinion.

Business associations reflected this pattern, with 38.9% agreeing, 9.3% strongly agreeing, and 18.5% disagreeing. Large companies showed stronger support, with 48% agreeing and 22% strongly agreeing, and only 2% disagreeing. Medium-sized companies were more polarised: 37.5% strongly agreeing, 25% agreeing, 25% disagreeing, and 12.5% strongly disagreeing.

Small companies and micro enterprises were evenly split between agreement and disagreement, with many expressing no opinion or strong disagreement. EU citizens leaned towards agreement, but a significant portion also disagreed or had no opinion. Public authorities were more cautious, with equal shares agreeing and strongly agreeing, and a notable proportion expressing no opinion. Trade unions were more supportive, with half strongly agreeing. Other respondents showed mixed views.

These results reflect a broad spectrum of stakeholder perspectives on whether ENISA's partnerships should be more clearly defined in its founding legislation. While there is a general tendency towards agreement, the level of support varies considerably across groups, with some expressing strong endorsement and others showing hesitation or opposition.

**ENISA's support in situational awareness**

This section assesses stakeholders' views on ENISA's role in situational awareness and how this function should evolve. Respondents reflected on which aspects should be strengthened, phased out, or added to enhance ENISA's contribution to EU cybersecurity resilience.

For capacity building (including ransomware prevention, sector-specific support, and exercises), 51.8% supported strengthening ENISA's role, 27.5% opposed, and 20.7% had no opinion. Large companies (66%) and public authorities (62.5%) were especially supportive, while medium-sized, small, and micro enterprises were more divided or sceptical. EU citizens and non-EU respondents generally supported a stronger role, but small businesses and trade unions were split.

Open-ended responses highlighted the need for ENISA to take a more prominent role in crisis coordination, support Member States during large-scale incidents, and lead cross-border response efforts. Stakeholders also called for ENISA to expand its mandate in certification, especially for cloud services and critical infrastructure, and to lead cross-sector simulation exercises. Some suggested phasing out technical development tasks in favour of strategic coordination and capacity building, and advocated a more bottom-up approach, especially for SMEs.

New responsibilities proposed included vulnerability disclosure, threat intelligence sharing, and unified incident reporting. There was support for ENISA to help implement NIS2 and the Cyber Resilience Act, develop a European vulnerability database, and broker external technical intelligence. International cooperation was emphasised, with calls for ENISA to build global partnerships, align with international standards, and support strategic capabilities in emerging areas.

For building a shared EU situational awareness picture, 77.2% supported ENISA's role, with strong endorsement from large companies, public authorities, and business associations, while medium-sized and small companies were more cautious.

Section 1.d shows broad and varied expectations for ENISA's situational awareness role. While there is no single consensus, responses point to a desire for ENISA to become more strategic, technically capable, and internationally connected. Stakeholders see ENISA as a central hub for coordination, guidance, and capacity building, with an ambitious and clearly defined mandate.

**ENISA and skills and awareness**

This section covers stakeholder perspectives on ENISA's role in cybersecurity skills and awareness. Most respondents supported ENISA's continued development of the European Cybersecurity Skills Framework (ECSF), with 75.1% agreeing or strongly agreeing. Large companies and EU citizens showed strong support, micro enterprises were highly positive, while small companies and public authorities were more divided, and trade unions were more critical.

ENISA's coordination of EU-wide awareness campaigns and educational tools also received broad support (78.8% agreeing or strongly agreeing), especially among large companies, micro enterprises, and EU citizens. Public authorities and trade unions were more polarised, and the non-EU citizen respondent strongly disagreed. For ENISA leading the development of an attestation scheme for cybersecurity skills, 69.4% supported the idea, though opinions were mixed. Medium-sized companies and micro enterprises were generally supportive, while EU citizens, public authorities, and trade unions showed divided views.

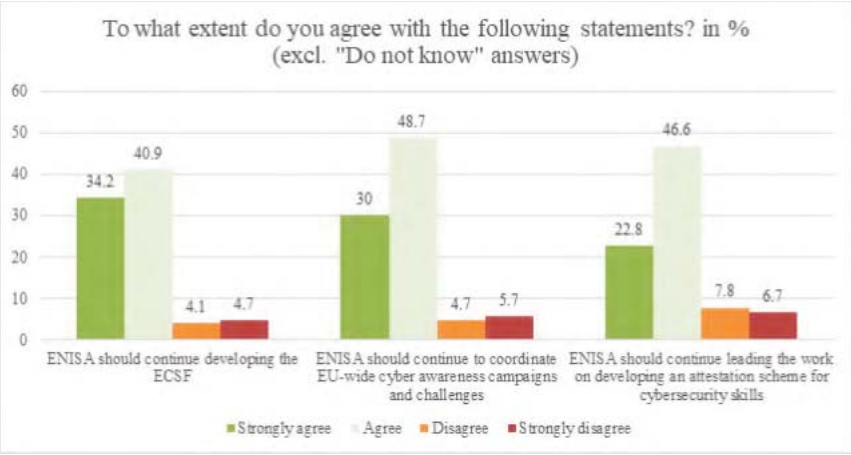


*Figure 3 Stakeholder's agreement with statements about ENISA*

Overall, stakeholders support ENISA's continued work in cybersecurity skills and awareness, especially in developing frameworks and coordinating campaigns. Views on certification and attestation schemes are more mixed, with some groups expressing strong support and others showing caution or opposition. These findings suggest ENISA's efforts in this area are valued, but future initiatives should reflect the diverse expectations of its stakeholders.

### *4.2 Section 2: Certification*

According to written submissions in the Call for Evidence, stakeholders highlighted the need to modernise and harmonise the certification framework. There were calls to integrate emerging technologies, such as artificial intelligence, into certification schemes, and proposals for risk-based, outcome-oriented models to better reflect evolving cybersecurity threats. Contributors emphasised transparency, traceability, and harmonised risk assessment for supply chain security, as well as clear standards to manage third-party risks and ensure accountability. Stakeholders also advocated streamlined certification processes and mutual recognition across Member States to reduce fragmentation and compliance burdens, with some requesting tailored schemes for different sectors.

The certification expert interviewed as part of these consultation activities identified challenges in the current framework, including the lack of mechanisms to resolve political deadlocks, a shortage of technical expertise, and a product-centric bias in the legal text. The current governance model limits ENISA's ability to act on politically sensitive issues, despite its formal responsibility for scheme development. Interviewees suggested expanding certification to cover services and organisational processes, clarifying ENISA's mandate to maintain and update schemes, and emphasised ENISA's role in coordination and support rather than as a certification body.

Public consultation results show strong interest in advancing ECCF implementation. Certification is widely seen as a tool to enhance product and service security, with 41.45% of respondents strongly agreeing. Similarly, 47.67% strongly support its role in regulatory compliance, and 41.45% emphasise its importance for market access through mutual recognition. These views are echoed across stakeholder groups, though with varying intensity. Among business associations, 33.33% strongly agree on security benefits and 40.74% on compliance. Large companies show 36.0% strong agreement on security and 62.0% on compliance. Medium and small enterprises demonstrate strong support, with 50.0% to 55.56% strongly agreeing on security, while micro businesses are the most supportive, with 66.67% strongly agreeing that certification improves security. These figures, combined with qualitative feedback calling for clearer guidance, harmonised schemes, and more inclusive governance, underscore the urgency of improving ECCF implementation to overcome current limitations and fragmentation, and to strengthen the EU's cybersecurity posture.

**Scope, objectives, elements of schemes and harmonisation principle**

This section summarises stakeholder views on factors encouraging application for European cybersecurity certification, including regulatory compliance, market access, legal exposure, customer trust, and administrative costs.

Stakeholders broadly recognised certification as a way to improve product and service security, with 41.5% strongly agreeing and 31.1% agreeing. Support was consistent across business associations, large companies, and micro businesses, while medium and small companies showed more varied responses. Regulatory compliance and international market access were also key benefits, with strong agreement among large companies and micro businesses.

Certification was seen as valuable for reducing legal exposure, enhancing market compliance, competitiveness, and customer trust. Notably, 47.7% strongly agreed that certification builds customer credibility, with micro businesses and large companies expressing the highest support. Views on reducing administrative costs were more mixed, with 41.9% agreeing and 21.2% strongly agreeing, but a notable share expressing disagreement or no opinion.

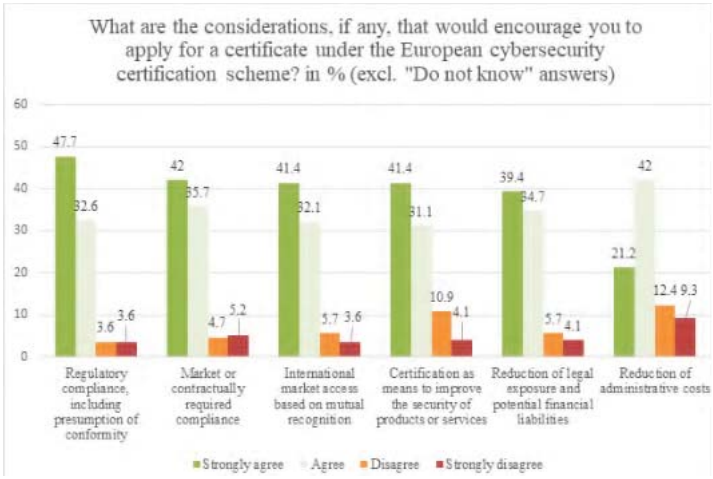



*Figure 4 Stakeholder's views on the considerations that would encourage them to apply for a certificate under the European cybersecurity certification scheme*

Open-ended responses emphasised the need for streamlined, consistent certification processes, alignment with international standards, and adaptability to different organisational sizes and sectors, especially SMEs. Stakeholders highlighted certification's role in competitiveness, internal processes, and legal clarity, as well as its value for customer confidence and brand reputation. Technologies identified as benefiting from certification included IoT, cryptographic services, cloud computing, AI, and critical infrastructure.

Opinions on the clarity of the European Cybersecurity Certification Framework were divided: 41.97% agreed the scope and objectives were clear, while 27.46% disagreed. Micro enterprises were most supportive, while other groups wanted more guidance and transparency. There was strong support for harmonisation across certification schemes (68.4%), especially among large companies, micro enterprises, and public authorities.

Views on mandatory certification were more divided, with 36.3% supporting and 51.3% opposed. Tailored certification schemes also received mixed responses, with 37.8% in favour and 40.9% opposed. Integration of privacy and data protection requirements was generally supported (41.5%), though some groups remained cautious. Voluntary certification to support compliance with multiple requirements was rated highly, with 41.4% giving the highest score.

Overall, stakeholders recognise certification's benefits for security and regulatory alignment, while debates on mandatory versus voluntary schemes, harmonisation, tailored provisions, and privacy integration reflect diverse priorities among stakeholder groups. Open-ended responses and scale ratings further highlight the desire for clarity, technical specificity, and practical guidelines.

**Process of development and adoption of certification schemes**

This section evaluates the development and adoption process for European cybersecurity certification schemes. Satisfaction with the time required for scheme development was low, with only 11.4% agreeing and 40.9% strongly disagreeing. Business associations, large companies, and micro enterprises were particularly critical, while medium-sized and small companies were more balanced but still sceptical.

There was strong consensus on the need for regular updates to certification schemes, with 52.9% agreeing and 23.8% strongly agreeing. Support was consistent across stakeholder groups, especially micro enterprises and public authorities.

Transparency in the development and adoption process received overwhelming support, with 60.6% strongly agreeing and 24.4% agreeing. Large companies, small companies, and business associations were especially supportive, and public authorities and trade unions also endorsed greater transparency.

Stakeholders had mixed views on the effectiveness of the Union Rolling Work Programme, with industry seen as the main driver of certification scheme development. There was strong support for involving public authorities, ENISA, and the ECCG in the process.

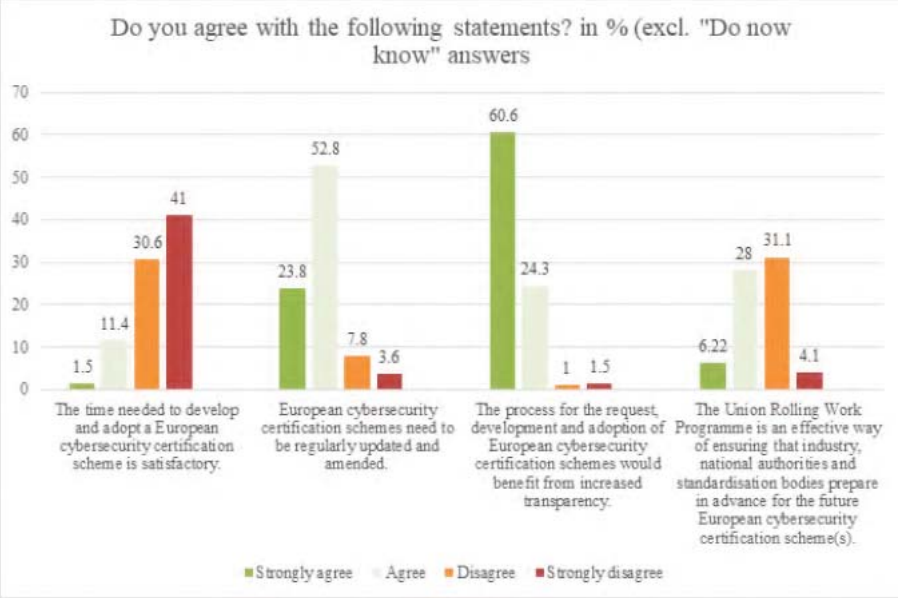



*Figure 5 Stakeholder's agreement with statements about certification schemes*

Overall, stakeholders want a more efficient, transparent, and inclusive certification process. While there is broad support for the current framework's principles, improvements are needed in governance, stakeholder engagement, and procedural clarity. Responses reflect a commitment to strengthening the European cybersecurity certification ecosystem and making it more responsive to diverse needs.

**Governance of the certification framework**

This section explores stakeholder perspectives on the role of ENISA within the ECCF, focusing on its involvement in scheme development, maintenance, guidance, promotion, and support. The responses reflect a nuanced understanding of governance, with varying degrees of ENISA's involvement across different functional areas.

A majority supported ENISA having a leading or supporting role in preparing and developing candidate schemes (52.3% leading, 30.1% supporting), with large companies and public authorities most in favour. Similar patterns were seen for scheme maintenance and technical specifications, where large companies and public authorities again strongly supported ENISA's leadership, while medium-sized, small, and micro enterprises preferred a supporting role.

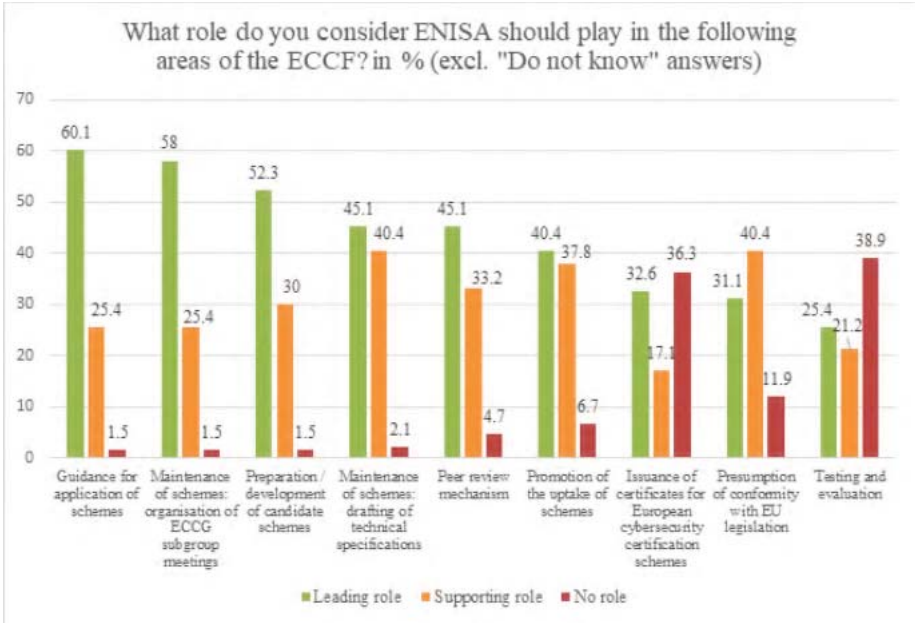



*Figure 6 Stakeholder's views on the role of ENISA regarding multiple areas of the ECCF*

For organising ECCG subgroup meetings and providing guidance for scheme application, most stakeholders favoured a leading role for ENISA, with strong support from business associations, large companies, and public authorities. Promotion of scheme uptake and peer review mechanisms saw more balanced support between leading and supporting roles, while issuance of certificates and testing/evaluation revealed more scepticism, especially among small and micro enterprises. For presumption of conformity with EU legislation, 31.09% supported a leading role for ENISA, 40.41% preferred a supporting role, and 11.92% opposed any role. Large companies, medium-sized companies, micro-enterprises, and EU citizens were more open to ENISA's leadership, while small companies were more sceptical.

Open-ended responses highlighted broad support for ENISA's technical leadership, especially in scheme development, guidance, and coordination. Stakeholders emphasised ENISA's role as a facilitator and knowledge hub, not a certifier or regulator, and stressed the importance of avoiding duplication with national authorities. Calls for greater transparency, stakeholder engagement, and alignment with existing standards were also prominent.

Overall, stakeholders strongly endorse ENISA's technical role, supporting a leading or supporting role across most ECCF areas. There is a clear preference for balancing EU-level coordination with national-level implementation, ensuring ENISA's role complements existing structures. Responses reflect a commitment to a robust, coherent, and inclusive cybersecurity certification framework that leverages ENISA's strengths and respects the diversity of the European digital landscape.

**Stakeholder involvement**

This section summarises stakeholder views on the efficiency, clarity, and inclusiveness of the ECCG and SCCG. Representation in the ECCG was very low among private sector actors and civil society (6.2% overall, with public authorities at 87.5%), showing institutional stakeholders are well-represented, but SMEs and citizens are largely absent.

Confidence in the ECCG's effectiveness was limited: nearly half of respondents had no opinion, and most others rated its effectiveness as low or very low, especially among business associations, small companies, and public authorities. Only a minority felt the ECCG's roles and responsibilities are clearly defined, with widespread calls for greater transparency and clarity.

There was broad consensus, especially among SMEs and business associations, on the need for more organised and inclusive stakeholder engagement in ECCG and ECCF processes. Open-ended responses called for formal ECCG subgroups, annual certification roadmaps, clearer documentation, tools for sensitive data management, and better coordination with public-private partnerships. Stakeholders also suggested strengthening national schemes, clarifying regulatory interplay, and assigning long-term governance roles.

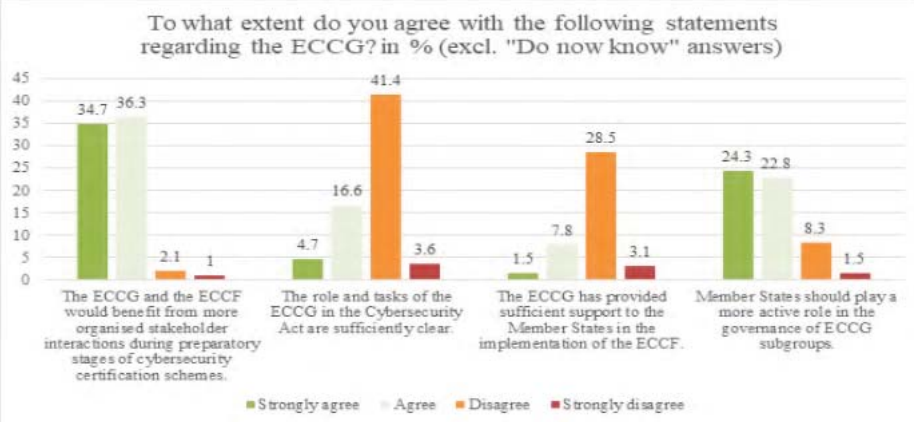



*Figure 7 Stakeholder's agreement with statements about the ECCG*

Stakeholder involvement in certification scheme development was widely seen as insufficient, particularly among SMEs and civil society. Most felt involvement was only to a little extent, with business associations and small companies most critical. Respondents emphasised the need for better harmonisation, clarification of roles, improved coordination, and mechanisms to include SMEs and international perspectives.

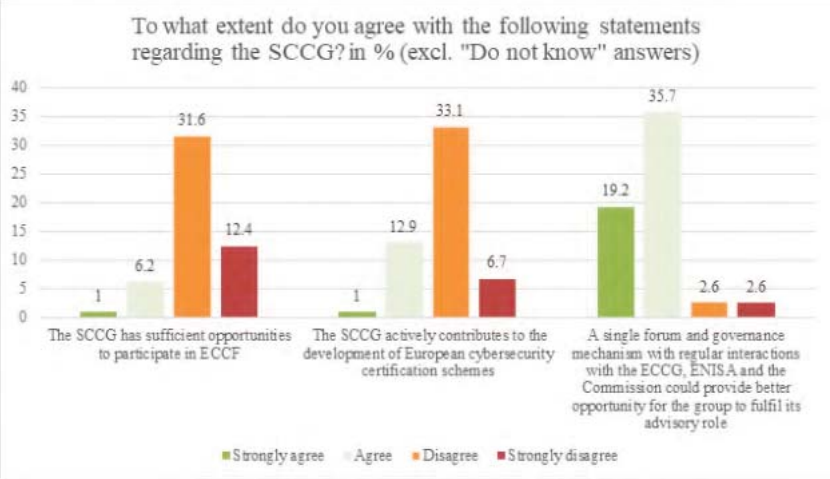



*Figure 8 Stakeholder's agreement with statements about the SCCG*

Participation in the SCCG was higher among institutional actors but limited among individuals and civil society. While 25.9% of respondents reported SCCG involvement, this was mainly among large companies and business associations. Many felt the SCCG had limited opportunities to participate meaningfully in the ECCF, with most expressing scepticism or uncertainty about its contribution to scheme development.

Open-ended responses suggested formalising ECCG subgroups, developing roadmaps, and simplifying regulation language. Views mainly indicated insufficient involvement, with many stakeholders feeling not adequately engaged. Suggestions focused on harmonisation, alignment with directives, and improved coordination and inclusion. Responses about SCCG opportunities were generally mixed, with many indicating room for improvement. Views on active SCCG contribution to scheme development were mixed, and a separate question about a single forum and governance mechanism found strong support.

Overall, Section 2.d reveals a consistent call for greater transparency, clearer roles, and more inclusive stakeholder engagement in the governance and development of European cybersecurity certification schemes. While institutional stakeholders are well-represented and generally supportive of current structures, there is a clear need to broaden participation, especially among SMEs and civil society, and ensure all voices are included in shaping the future of cybersecurity certification in Europe.

### *4.3 Section 3: Simplification*

According to written submissions in the Call for Evidence, there was a strong consensus among stakeholders on the need to reduce complexity and administrative burden, particularly for SMEs. Several contributors highlighted the challenges faced by smaller entities in navigating the current regulatory landscape and called for simplified compliance procedures. Stakeholders stressed the importance of clearer, harmonised guidelines to avoid fragmented implementation and ensure consistent application across the EU. Others emphasised the disproportionate impact of complex obligations on SMEs and advocated for tailored support mechanisms, including exemptions and simplified reporting frameworks. Several contributors also proposed the development of centralised EU

platforms for reporting and compliance tracking, which would enhance efficiency and reduce duplication across different legislative instruments.

National authorities and ENISA representatives provided practical perspectives on implementation barriers, highlighting the need for streamlined reporting mechanisms, clearer guidance, and improved coordination across legislative instruments. They stressed the importance of making compliance processes more efficient and responsive to the needs of both Member States and industry.

The Public Consultation offers a detailed exploration of stakeholder perspectives on the complexity, applicability and harmonisation of EU cybersecurity legislation. The section draws on both quantitative and qualitative data, with particular emphasis on questions rated on a 1-to-6 scale. These ratings provide insight into the intensity of stakeholder concerns and implementation challenges, especially when disaggregated by stakeholder group and business size.

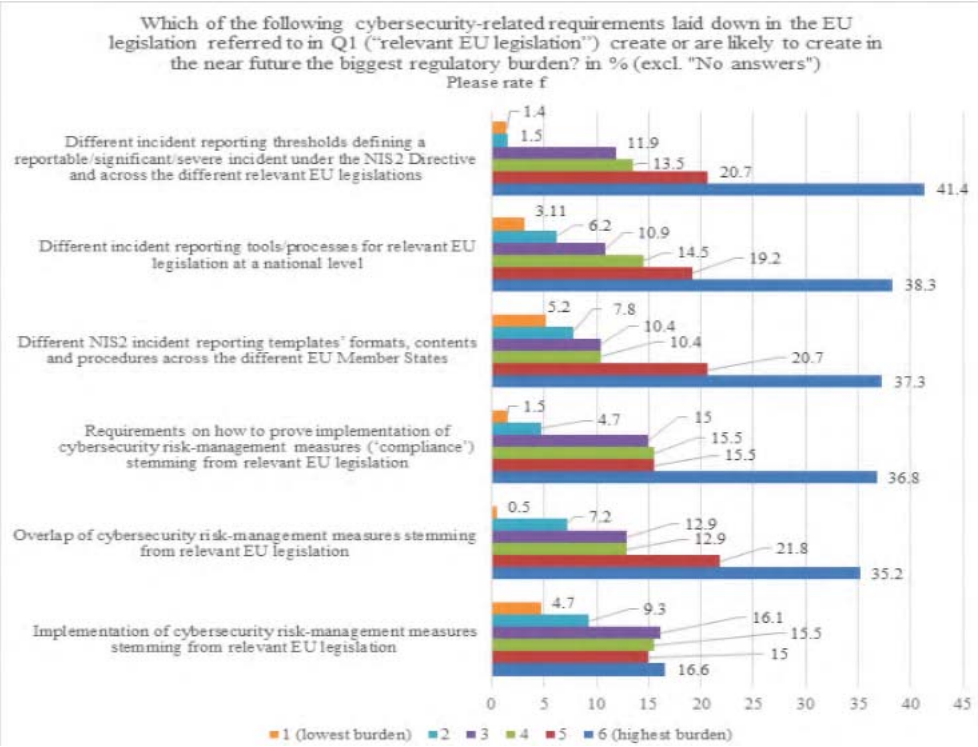



*Figure 10 Stakeholder's view on regulatory burden regarding EU legislation*

The analysis shows that NIS2 was the most frequently cited applicable EU legislation, with many respondents indicating multiple frameworks (GDPR, DORA, CER, AI Act) apply to their entities. Cross-sectoral associations and digital service providers highlighted the growing complexity and called for a more integrated legislative approach.

Stakeholders expressed strong concern about the diversity of incident reporting tools and processes at the national level, with medium-sized, small, and micro enterprises reporting the highest difficulty. The lack of harmonised reporting thresholds across EU legislations was a major challenge, especially for SMEs and business associations.

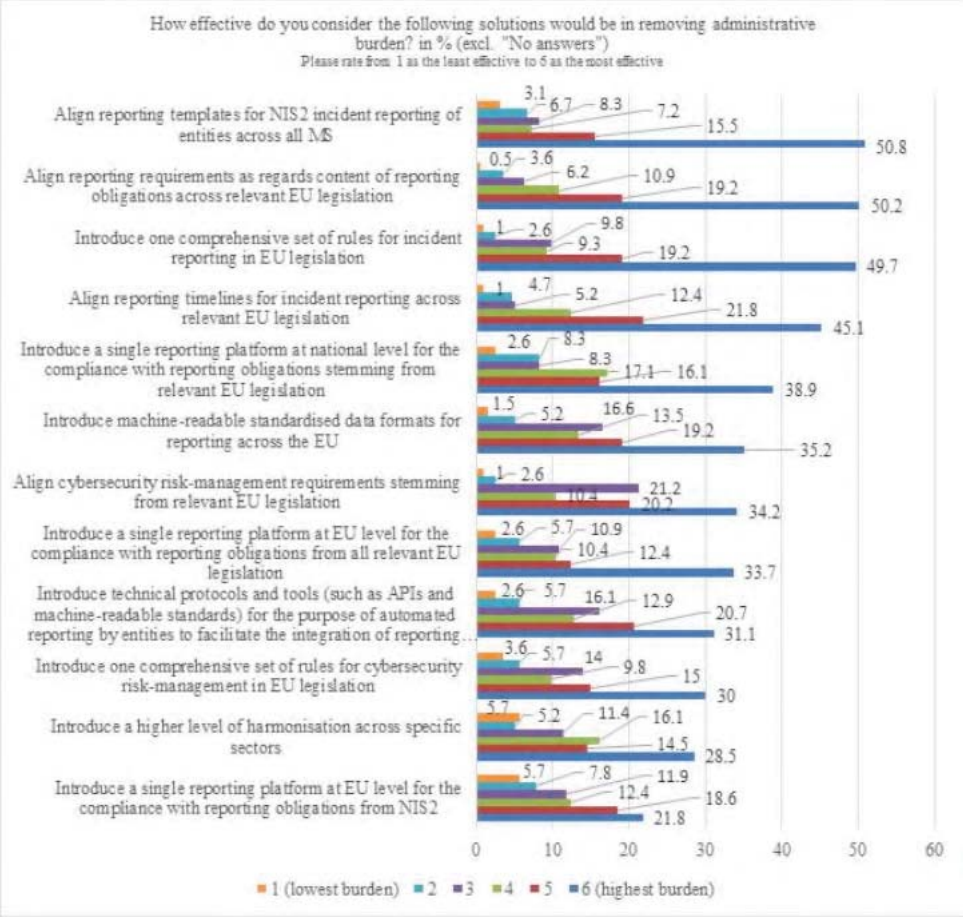



*Figure 11 Stakeholder's view on effectiveness of solutions to remove administrative burden*

Implementation of cybersecurity risk-management measures showed varied responses, reflecting differences in organisational capacity. Overlap of requirements and the burden of proving compliance were significant issues, particularly for medium-sized, small, and micro enterprises, as well as trade unions. Calls for clearer guidance and streamlined processes were frequent.

Open-ended responses emphasised the need for simplified regulations, standardised templates, and centralised platforms. Stakeholders described the current system as fragmented and resource-intensive, with overlapping obligations diverting resources from operational cybersecurity efforts. There was strong support for cross-sector harmonisation, especially in banking, energy, transport, and public administration.

Overall, the analysis reveals a consistent call for simplification, harmonisation, and clarity in EU cybersecurity legislation. Medium-sized companies report the highest concern, particularly regarding reporting thresholds, tool diversity, and compliance burdens. Small and micro enterprises also express significant concern, while large companies tend to be more moderate. Business associations advocate strongly for harmonisation, and public authorities, EU citizens, and other stakeholders highlight the need for coordination and sector-specific guidance. These findings underscore the importance of a coordinated and

inclusive approach to cybersecurity governance that balances regulatory ambition with practical feasibility for all entities.

### 4.4 *Stakeholders' position papers and additional submissions*

This section examines stakeholder submissions from the public consultation EU Survey for the revision of the Cybersecurity Act.

A central theme is the call for a clearer and more empowered mandate for ENISA. Stakeholders advocate for greater technical authority, enabling ENISA to lead in certification, threat analysis, incident coordination, and capacity building, while maintaining its neutrality and independence. ENISA's role in harmonising cybersecurity legislation across Member States, especially regarding NIS2 and the Cyber Resilience Act, is strongly emphasised, along with proposals for EU-wide training and strategic foresight.

On the ECCF, stakeholders strongly support modernisation and expansion, calling for broader applicability across sectors and technologies, including cloud services, telecoms, and critical infrastructure. Supply chain risk management is a priority, with requests for clearer guidance, harmonisation across Member States, and alignment with international standards to reduce fragmentation and foster trust in cross-border digital services. Stakeholders also call for more flexibility, transparency, and risk-based certification models.

Regulatory complexity is a major concern, especially the cumulative burden of overlapping obligations from multiple EU regulations. Respondents support a unified digital reporting platform to streamline compliance and reduce administrative overhead, and advocate for principle-based, risk-oriented frameworks for greater flexibility. Tailored support for SMEs is a recurring theme, with suggestions for tiered obligations and clearer guidance.

Overall, the feedback reveals a strong appetite for reforming the Cybersecurity Act. Stakeholders envision a future framework that is more coherent, technically robust, forward-looking, and easier to navigate. The proposed changes to ENISA's mandate, the ECCF, and reporting obligations reflect a shared commitment to enhancing cybersecurity across the EU while reducing complexity and fostering innovation.

## 5. **Conclusion**

The stakeholder consultation activities provided relevant evidence for the impact assessment and a nuanced understanding of stakeholder views.

The Call for Evidence yielded 184 written contributions from industry associations, cybersecurity firms, SMEs, academic institutions, and public interest organisations. Stakeholders broadly supported strengthening ENISA's role, with calls for increased resources, but some cautioned against overextension and advocated for clarifying the existing mandate. There was strong support for modernising the ECCF, including risk-based certification models and harmonised standards. SMEs emphasised the need for simplified compliance and centralised reporting.

The public consultation received 193 responses and addressed similar themes. There was consistent support for ENISA's core tasks, especially certification, operational cooperation, and policy implementation. Larger organisations and public authorities were more supportive of expanding ENISA's technical mandate than SMEs and micro-enterprises. Citizens valued ENISA's role in transparency and awareness, while public authorities focused on regulatory and harmonisation functions. Many respondents called for harmonisation of reporting obligations across EU legislation.

Targeted interviews added qualitative depth to these findings. ENISA's representatives and national authorities stressed the need for stronger crisis coordination, support for certification development, and stakeholder engagement. They emphasised ENISA's role as a facilitator, supporting Member States and industry through guidance, capacity building, and technical leadership. Some proposed new responsibilities for ENISA, such as vulnerability disclosure, threat intelligence sharing, and unified incident reporting.

Across all consultation activities, stakeholders consistently called for simplification and harmonisation. Complexity and fragmentation of cybersecurity obligations were seen as major barriers, especially for SMEs. There was broad support for streamlined reporting, clearer guidance, and better coordination across legislative instruments. Integrating privacy and data protection into certification schemes was widely supported, though views on mandatory and tailored schemes were mixed.

Some contradictions emerged: large companies and public authorities generally supported expanding ENISA's technical mandate, while SMEs and micro-enterprises were more sceptical. Concerns about duplication and over-centralisation were also noted.

Interdependencies were evident: calls for modernising the ECCF were linked to supply chain security, regulatory clarity, and market access. Support for ENISA's strategic role was often tied to demands for improved governance and stakeholder engagement. The need for proportionality in regulatory requirements was consistently linked to SME challenges.

In summary, the consultation revealed broad alignment on strengthening ENISA's mandate, modernising certification frameworks, and simplifying obligations, but also highlighted differences by organisational size, sector, and role.

# ANNEX 3: WHO IS AFFECTED AND HOW?

## PRACTICAL IMPLICATIONS OF THE INITIATIVE

The preferred package of policy options (A2, B2, C2, D3) is expected to have practical implications for the following categories of stakeholders:

- **Businesses** (large, SMEs and micro) including vendors of ICT products, services, processes, managed security services; essential and important entities covered by NIS2; businesses using ICT solutions and relying on critical infrastructure; conformity assessment bodies, testing laboratories and providers of individual skills attestations.
- **Public authorities** including National cybersecurity authorities; national cybersecurity certification authorities; national accreditation bodies; surveillance authorities and ICT users. Please note that public administrations as NIS2 entities are covered under "economic operators".
- **Consumers and citizens** as actual and potential cybersecurity professionals, ICT users and users of public services relying on critical infrastructure.
- EU institutions and agencies, in particular **ENISA.**

### 1. ECONOMIC OPERATORS (INCLUDING LARGE ENTERPRISES, SMES, AND CROSS-BORDER OPERATORS)

***NIS2 entities, including important and essential entities***

First, the simplification of the NIS2 Directive through targeted amendments to clarify its scope and definitions and to reduce the scope as regard micro- and small-sized DNS service providers, will reduce the number of SMEs covered by the directive. Likewise, by amending the NIS2 Directive to introduce the category of small-mid caps and designating small-mid cap-sized entities as important entities, compliance costs of the approximately 22 500 economic operators will be reduced. Collecting data on ransomware reporting in a streamlined manner will directly benefit economic operators by reducing the number of successful ransomware attacks. Moreover, ENISA's role in assisting competent authorities in mutual assistance and supervision of entities operating in several Member States will facilitate compliance and reduce burden on entities.

In addition, guidelines on supply chain security will provide legal certainty and streamline the implementation of the supply chain security requirements of the NIS2 Directive, facilitating compliance and preventing the undue pass of obligations on entities not in scope of the NIS2 Directive. Beyond indirectly benefiting from the harmonisation of cybersecurity in the ECCF, the NIS2 entities will also benefit from the future organisational cybersecurity certification schemes paired with the introduction of the possibility to demonstrate conformity with the NIS2 Directive, which will facilitate the compliance efforts for cross-border entities.

***SMEs and other economic operators***

The table below provides an overview of ICT security maturity across small, medium and large enterprises in the EU, based on key indicators such as incident occurrence, adoption

of security measures, and internal governance practices. The data highlights persistent gaps between small and larger firms, with smaller enterprises showing significantly lower rates of documentation, regular review, and employee awareness initiatives. These discrepancies are relevant in the context of EU cybersecurity reforms, as they underscore the need for proportionate support and simplified compliance mechanisms to ensure that all businesses, regardless of size, can meet evolving cybersecurity requirements effectively.

*Table 51: ICT maturity indicators in the EU for small, medium and large enterprises*

| Enterprise size (employees) | Enterprises that experienced any ICT security related incidents leading to unavailability of ICT services, destruction or corruption of data or disclosure of confidential data (2024)[1] | Enterprises using any ICT security measure (2024)[2] | Enterprises that have documents on measures, practices or procedures on ICT security in place (2024)[3] | Enterprises that reviewed their ICT security documentation in the last 12 months (2024)[4] | Enterprises that make employees aware of their obligations in ICT security related issues[5] |
|---|---|---|---|---|---|
| **Small (10-49)** | 19,85% | 91,79% | 30,31% | 17,98% | 55,99% |
| **Medium enterprises (50-249)** | 27,97% | 97,15% | 56,25% | 35,72% | 96,45 |
| **Large enterprises (<250)** | 38,29% | 99,11% | 81,84% | 57,87% | 92,34% |

In terms of operational benefits, economic operators will capitalise on ENISA's enhanced support role under Option A.2. ENISA would be equipped to provide sector-specific guidance, incident trends and technical alerts. Businesses would also be able to more effectively prepare, detect and respond to threats thanks to ENISA's operational support for cybersecurity. Cross-border economic operators, in particular, could benefit from interoperability gains provided by the harmonised legislative and certification framework. The same evaluation methodology and security requirements would apply across the internal market, supported by more streamlined cross-border supervision, improving consistency and reducing reliance on national consultants or legal interpretations. This supports a more levelled playing field, especially for SMEs aiming to scale their digital services across borders.

Option B.2 introduces a more efficient and effective ECCF which would enable businesses to certify their ICT solutions under EU-wide cybersecurity certification scheme once and provide services and products across the EU which being protected against emerging cyber threats. Clear development is expected to help businesses prepare for the upcoming certification, making it a viable and justifiable business cost contributing to scaling of business without undue administrative costs. The streamlining of certification governance and the broader synergies with other relevant act addressing cybersecurity are also expected to reduce legal uncertainty and could enable the use of certification framework

for demonstration and presumption of conformity with Union legal acts (the changes envisaged under option B.2 and C.2).

***Conformity assessment bodies***

Europe has a strong footprint of testing laboratories and conformity assessment bodies[184], especially for what pertains to product security. For conformity assessment bodies (CABs), the changes envisaged under option B.2 and C.2 (demonstration of conformity for NIS2 entities), especially more schemes with improved uptake, would provide them with more business opportunity. Furthermore, alignment of requirements for CABs between different legal frameworks (CSA, CRA based on NLF) will contribute to lowering of administrative costs.

***Providers of European individual cybersecurity skills attestations***

With option A2, the development of European individual attestation schemes would first affect economic operators by leading to the rise of providers authorised to deliver such attestations, who would gain visibility in a market which is today widely occupied by non-European providers. More widely and beyond authorised providers themselves, the development of European individual attestation schemes would support economic operators across the board in their training and hiring practices by providing visibility and portability of skills. Additionally, a low uptake of the attestation mechanism by individuals could result in providers engaging costs to be authorised but not benefitting from an immediate return on investment in case the workforce expresses low interest in holding such an attestation. This risk could nevertheless be offset by a market study to be conducted for each scheme – i.e. each profile – and by ensuring that the fees associated to each authorisation are tailored to the actual costs of developing a scheme as well as by a recommendation by the agency on the actual cost of an attestation, providing guidance to providers.

***Mobile network operators and other critical supply chain sectors***

Option D.3 entails adjustment costs on economic operators. Specifically, one-off adjustment costs for mobile network providers for replacing 5G equipment coming from high-risk suppliers or entities originating or controlled from countries of concern. This option would also bring substantial cross-sectorial security benefits by harmonising the level of security and resilience of telecommunications networks throughout the entire Union while decreasing the reliance on high-risk suppliers, as well as by stimulating investments in a trusted 5G offering. Sectorial benefits of securing 5G networks would depend on the degree of which a particular sector leverages them, with digital infrastructure being prime example of the most benefiting sector followed by transport or public sector. It is expected that trusted 5G equipment providers would largely benefit from the obligation of removing untrusted equipment from supply chains.

---

[184] ENISA, *Conformity assessments*, https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity%20Certification%20Statistics%20Report.pdf.

Beyond 5G networks, as explained in the Impact Assessment *(see Section 5)*, each application of the framework to a particular ICT supply chain would be based on a dedicated risk and impact assessment — including market and economic analysis of factors such as the availability of alternative suppliers and the potential impact on industry. Sectors that would likely be benefiting are those currently exhibiting high degree of non-technical risks and could include scanning equipment, submarine cables, and electricity supply.

### 2. NATIONAL AUTHORITIES

National authorities would experience both positive impacts and one-off adjustment costs as a result of the preferred policy option. The reduction of numbers of entities in scope of the NIS2 Directive, clarifying certain definitions of NIS2, the designation of small-mid cap-sized entities as important entities and the possibly of demonstrating compliance based on organisational cybersecurity schemes would reduce the burden incurred by fragmentation. This measure would facilitate the monitoring of entities' compliance with the relevant regulatory instruments, thereby resulting in savings for competent authorities. Likewise, receiving support from ENISA in supervising cross-border entities would reduce the supervisory burden on competent authorities.

The reform of ENISA's mandate under Option A.2 would strengthen its role in supporting policy implementation and operational coordination. While some national authorities may need to allocate staff to these enhanced coordination mechanisms, many structures are already in place. The expected benefits in terms of faster response, better guidance, and improved crisis coordination are likely to outweigh the associated costs.

Entrusting the elaboration and maintenance of European individual attestation schemes to ENISA and the delivery of such attestations to authorised providers, including **national authorities**, could ultimately lead to savings in terms of human resources for national authorities who develop today such attestations of people. Additionally, national authorities would not be constrained to develop or maintain in-house schemes as they could rely on the European individual attestations, notably to check the competence of individuals working for managed security service providers or for hiring purposes. A rationalised and centralised EU individual attestation scheme would further rationalise the costs, avoiding proliferation of national schemes which aim at a similar objective across Member States but are developed independently across the EU. Developing European individual attestation schemes could have potential effects on national authorities insofar as they decide to take an active part in the development of such schemes, therefore involving human resources efforts in the development thereof. However, such participation in the development of schemes would remain voluntary.

The governance of the ECCF would be clarified and improved based on lessons learnt in the past 5 years. National representatives in the European Cybersecurity Certification Group (ECCG) would have a more structured role with more predictable development cycles for the certification schemes. This would contribute to more efficient use of resources and avoid fragmentation of national certification initiatives. The increased uptake of schemes entails costs for National Cybersecurity Certification Authorities (NCCAs**)**, which may need to allocate additional resources to oversee a larger number of certifications. However, in certain cases, this can be offset by the resources that Member States already dedicate to supervising national certification schemes.

Option D.3 would entail a need for additional resources for national authorities as it would require sufficient staff to enforce the restrictions on high-risk suppliers or entities originating or controlled from countries of concern adopted at EU-level. Identifying high-risk suppliers and entities controlled by or originating from countries of concern, the framework will build on existing registries and mechanisms between the Commission and Member States that support unravelling corporate ownership structures of such entities. On the other hand, this option establishing a comprehensive and horizontal ICT supply chain framework would also bring more legal clarity and certainty for national authorities. The framework would be future-proof and common to all Member States, which makes the process of mitigating non-technical risks more efficient at EU level.

### 3. CONSUMERS AND CITIZENS

No direct adjustment or compliance costs are foreseen for citizens or consumers. Enforcement activities related to these reforms are covered within the overall administrative costs of national authorities and ENISA. Consumers are expected to benefit from a strengthened cybersecurity ecosystem. The reforms aim to improve the security and reliability of digital services and products across the Union, which directly impact users' safety and trust.

For **actual or potential cybersecurity professionals**, holding an individual cybersecurity certification not only enhances an individual's appeal in the job market but also leads to wage increase (*see Annex 4*), hence confirming the impact of holding a cybersecurity attestation on skills portability, career advancement with positive impact salary levels, reflecting the recognised value of their expertise. Moreover, defining the costs of a European cybersecurity individual attestation at EU level could lead to potential cost savings, considering that the foreseen cost of the European individual cybersecurity attestation would be potentially closer to those delivered by public organisations and lower than the current average cost of cybersecurity certifications delivered by private certification bodies.

Costs on individuals would materialise in the level of risks they bear by deciding to attempt at holding a European individual attestation instead of choosing an already market-recognised certification delivered by an established certification provider.

It is expected that more digital products and services would receive an EU cybersecurity certificate in the coming years. For consumers, this would serve as an assurance of basic cyber hygiene and raise level of risk awareness, particularly for connected products such as smart home devices or health apps. Improved product security reduces the risk of privacy violations, identity theft and unauthorised access. Furthermore, certification of ICT solutions intended for exercising rights online, such as the EUDI Wallet, would have further positive impact on citizens' rights.

From a legal perspective, citizens would gain from greater consistency in the enforcement of cybersecurity obligations. By facilitating the compliance of entities with different regulatory instruments including NIS2 and in particular by reducing the number of successful ransomware attacks, Option C.2 strengthens the continuity of services vital to society and the protection of personal data, including by supporting the enforcement of relevant obligations.

Option D.3 strengthens security and protection of personal data for consumers and citizens. It would contribute to the security of personal data by restricting provision of products by high-risk suppliers or entities originating or controlled from countries of concern and thus protecting the confidentiality, integrity and availability of information for all telecommunications networks.

All in all, consumers would experience a safer digital environment without the need to take action themselves. The long-term societal benefit is an increase in public trust and confidence in digital services, which supports digital inclusion and uptake.

### 4. EU INSTITUTIONS & ENISA

The implementation of the preferred policy option would entail important changes for ENISA. ENISA's mandate would be expanded to include operational support functions., including situational awareness. In parallel, ENISA's role would be expanded in cybersecurity certification and standardisation, as well as the development and maintenance of European individual attestation schemes. These tasks are expected to continue to strengthen ENISA's reputation in the cybersecurity ecosystem and towards industrial players.

Despite the significant financial outlay, the anticipated benefits of Option A.2 and B.2 such as improved governance, enhanced operational capabilities, and a more robust certification and standardisation framework justify the investment. By equipping ENISA with the necessary tools and authority, this policy option aims to strengthen the EU's cybersecurity posture and ensure a more resilient digital environment. Furthermore, more efficient development of certification schemes will help prevent the proliferation of national-level schemes, reducing compliance costs for businesses operating across the Single Market. These investments, borne at the EU level, are justified by the economies of scale achieved through the avoidance of 27 parallel national systems. At the same time, the more focused mandate and prioritised tasks will lead to a more efficient use of resources.

Moreover, to counterweight some of the costs occurring to ENISA some activities (development and maintenance of European attestation schemes and maintenance of certification schemes) activity could be funded through fees. Fees would have to reflect the real costs of the related activity and these revenues will not lead to a profit. It would lead to avoid relying on the medium run, on EU budget to fund this activity.

The main impact of developing **European individual attestations schemes** would be on the immediate budget of ENISA for the first 5 years (see *section 6.1.1.1 (a)* of the impact assessment). For the development of the attestation of skills schemes, taking into account that there are 12 different roles under the European Cybersecurity Skills Framework and that the development of schemes for all of those roles would be gradual, this action would incur the costs of human resources. However, to be in a position to deliver European individual attestations, implementing the European individual attestation schemes, providers would need to be authorised. Such authorisations, delivered by the agency, would entail paying a fee to ENISA ((see *section 6.1.1.1 (a)*). Such a cost could have a prohibitive effect for providers who, in the first years of the schemes, might not clearly identify the added value of holding such an authorisation. Therefore, even if a fee mechanism is established, the self-financing of this activity depends highly on EU market uptake by providers and by individuals.

The implementation of Option B.2 entails economic impact on ENISA, reflecting the broader and more **structured governance model of the ECCF**. These costs are driven by the new task of maintaining adopted certification schemes, the perspective of adopting new schemes (EUCS and EU5G) and the broadened scope of the framework (B2 + C2). Next to additional FTEs, where the maintenance of a scheme requires more complex work, this could be financed by a fee mechanism, ensuring a sustainable and future-proof model.

Option D.3 would entail a need for additional resources need for the EU institutions as it would require sufficient staff to coordinate with Member States on **enforcement of the restrictions on high-risk suppliers** or entities originating or controlled from countries of concern adopted at EU-level. Identifying high-risk suppliers and entities controlled by or originating from countries of concern, the framework will build on registries and mechanisms between the Commission and Member States that support unravelling corporate ownership structures and establish the list of subsidiaries of such entities. On the other hand, by decreasing the dependency on high-risk suppliers and entities controlled from countries of concern at Union level, would in turn also have a positive direct and indirect impact on the cybersecurity of EU institutions and agencies.

In summary, the EU institutions would incur upfront and recurring investment costs to launch and coordinate the reformed framework. These would be offset by the long-term efficiency and security gains delivered across the Union.

## 5. SUMMARY OF COSTS AND BENEFITS (INCL. "ONE IN, ONE OUT" APPROACH)

*Table 62: Overview of Benefits (total for all provisions) – Preferred Option (incl. "OUTs" of the OIOO approach)*

| **II. Overview of Benefits (total for all provisions) – Preferred Option** | | |
|---|---|---|
| ***Description*** | ***Amount*** | ***Comments*** |
| ***Direct benefits*** | | |
| Compliance cost reductions for businesses | **EUR 14.6 bn over five years** | **Main beneficiaries:** SMEs and economic operators. Savings arise from simplified compliance (C.2), reduced scope, and fewer legal interpretations needed, and lower administrative costs. |
| Enforcement cost reduction for public authorities | **EUR 7.5 M over five years** | **Main beneficiaries:** national supervisory authorities due to reduced scope. |
| Reduced cost caused by cybersecurity incidents, including ransomware attacks | Not monetised (at aggregated level) | **Main beneficiaries:** Economic operators in the first place, including SMEs as well as public authorities and citizens. This is driven by enhanced operational support by ENISA, including on situational awareness; more certification schemes covering key ICT technologies; mandatory ransomware reporting under NIS2; (A2, B2, C2)<br>See *Annex 7* for quantitative estimates of the costs factors linked to cybersecurity incidents. |
| Support to incident detection and response | **EUR 3.7 to 4.4 bn over five years** (broad estimate) | **Main beneficiaries:** EU institutions, national authorities, economic operators, SMEs, users. Support to incident detection and response (by analysing threats and cybersecurity events) (A.2) making use of the single-entry point proposed under the Digital Omnibus and other simplification measures (C.2) enable quicker identification and coordination. |
| Procedural efficiencies | Not monetised | **Main beneficiaries**: Public authorities, ENISA, economic operators (A2, B2) |
| Improved cross-border interoperability | Not monetised | **Main beneficiaries:** National authorities, economic operators.<br>ENISA's enhanced role (A.2), common reporting/certification practices improve EU-wide operational and data flows (B.2, C.2 ). |
| Increased uptake of certification | Not monetised | **Main beneficiaries:** SMEs, economic operators, EU Citizens.<br>Improved legal clarity (B.2) reduces uncertainty, encouraging more voluntary certification and trust-building. |
| Long-term efficiency gains | Not monetised | **Main beneficiaries:** SMEs.<br>Harmonised obligations (C.2) lower compliance costs over time by reducing reliance on legal consultants and internal admin capacity. |
| ***Indirect benefits*** | | |
| Cyber resilience and technological sovereignty | Not monetised | **Main beneficiaries**: EU institutions, economic operators, citizens, public authorities. |
| | | |
| Enhanced trust in digital services | Not monetised | **Main beneficiaries:** Consumers and businesses. Increased certification uptake (B.2) and improved |

| | | |
|---|---|---|
| | | incident handling (A.2) build digital trust and market confidence |
| Internal Market | Not monetised | **Main beneficiaries:** Cross-border operators, consumers.<br>Harmonised certification, cybersecurity risk managements requirements and reporting frameworks and […] reduce fragmentation and ease access to new markets. Enhancing the EU Single Market. |
| Better alignment with EU policy goals | Not monetised | **Main beneficiaries:** EU institutions and Member States.<br>Supports the EU's "green oath" and REFIT principles of simplification and digital readiness. More agile and integrated certification supports EU policy goals. |
| ***Administrative cost savings related to the "One in, one out approach"*** | | |
| Compliance cost reductions for businesses | **14.6 billion EUR** over five years, of which **2.4** bn EUR (EUR 1.35bn + EUR 1.06bn + EUR 30 million) in administrative costs | **Main beneficiaries:** SMEs and economic operators covered by NIS2. Savings arise from simplified compliance (C.2) and fewer legal interpretations needed, and lower administrative costs.<br>• NIS2 scope removals for DNS service providers and other entities: EUR 2.7 bn per year (EUR 94 355 per entity for 28 700 entities). Of the reduced compliance costs, EUR 270 million are categorised as administrative costs.<br>• NIS2 new mid-cap category: EUR 212 million per year (EUR 94 355 per entity for 22 500 entities)<br>• NIS2 compliance through cyberposture scheme: EUR 30 million per year (counting 1000 companies as of 2032– EUR 30 000 per year per entity) |
| Enforcement cost reduction for public authorities | **EUR 7.5 million over five years** | **Main beneficiaries:** national supervisory authorities due to reduced scope. |

*Tables 7 and 8 3: Overview of costs – Preferred option (incl. "INs" of the OIOO approach) over five years*

Aggregated estimates are provided over five years, unless specified otherwise.

| **III. Overview of costs – Preferred option** | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | **Citizens/Consumers** | | **Businesses** | | **Administrations** (MS and ENISA) | |
| | | **One-off** | **Recurrent** | **One-off** | **Recurrent** | **One-off** | **Recurrent** |
| Action (a) | Direct adjustment costs | N.A. | | Adapting to requirements and security testing in view of certification, on voluntary basis (B.2).<br><br>Adapting requirements | | For **Member States** (A2), **EUR 11.3M** for 40 national liaison officers.<br><br>Adjustment costs (on-off) for the Member States which have not | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | for implementing regulation on cybersecurity risk management measures, depending on risk-based approach (C2)<br><br>Adapting to requirements for the cyber posture scheme, on voluntary basis (C2, B2) | | implemented the 5G Toolbox, and as applicable for future sectors (D3).<br><br>For **ENISA** (A2), overall: **EUR 148.12 million** over five years (EUR 138M recurring. i.e. EUR26.7 in the first year and EUR 27.8M yearly over 4 years and EUR 10.1 M one-off costs), including **142 new FTEs** as well as operational costs related to platforms and tools, such as the operation of the CRA of the single reporting platform, the single repository of CTI, CVD database and a skills attestation website.<br><br>In addition, **up to 14 FTEs** linked to ECCF (B2+D3), amounting to EUR **7,9 million over five years,** and **5.2 M operational costs**, totalling adjustment costs of **EUR 13.1 M**<br><br>In total for ENISA, this leads to **EUR 161.3 M, including 156 FTEs** | |
| | Direct administrative costs | N.A. | Certification (on voluntary basis): costs related to documentation and obtaining certificate (one-off and recurrent), as well as maintenance (e.g. audits). For cyberposture scheme**, 30 000 EUR** (one-off and recurrent) (B2)<br><br>European skills attestation (on voluntary basis): costs for skills attestation vendor to obtain authorisation (one-off and recurrent) and to maintain it. (A2)<br><br>Minor (on-off) costs related to adapting notification procedures for ransomware attacks (C2) | | | |
| | Direct regulatory fees and charges | | Fees to be paid by conformity assessment bodies to ENISA for the maintenance of schemes: **EUR 1.3 M to 1.7 M** | N.A | | |

| | | | | | |
|---|---|---|---|---|---|
| | Direct enforcement costs | | | | For certification, up to **EUR 74.7 M** (one-off and recurrent) **for all 27 MS** (B2 +D3, C2) for the implementation of new schemes, including cyber posture scheme (3 FTEs in average) |
| | Indirect costs | | Costs related to cybersecurity incidents for NIS2 entities excluded from the scope (e.g. DNS providers) | | |
| | | | | | |

| **III. Application of the 'one in, one out' approach – Preferred option(s)** | | | |
|---|---|---|---|
| **[M€]** | **One-off**<br><br>(annualised total net present value over the relevant period) | **Recurrent**<br><br>(nominal values per year) | **Total** |
| **Businesses** | | | |
| New administrative burdens (INs) | N.A. | Certification (on voluntary basis): costs related to documentation and obtaining certificate (one-off and recurrent), as well as maintenance (e.g. audits). For cyberposture scheme, 30 000 EUR (recurrent) (B2)<br><br>European skills attestation (on voluntary basis): costs for skills attestation vendor to obtain authorisation (one-off and recurrent) and to maintain it. (A2)<br><br>Minor (one-off) costs related to adapting notification procedures for ransomware attacks (C2) | |

| | | | |
|---|---|---|---|
| Removed administrative burdens (OUTs) | **Over 5 years: EUR 2.4 billion** | NIS2 scope removals for DNS providers and other entities: EUR 270 million bn per year (EUR 94 355 per entity for 28 700 entities)<br><br>NIS2 new mid-cap category: EUR 212 million per year (EUR 94 355 per entity for 22 500 entities)<br><br>NIS2 compliance through cyberposture scheme: EUR 30 million per year (for 1000 companies as of 2032– EUR 30 000 per year per entity) | |
| ***Net administrative burdens**** | **Over 5 years: - EUR 2.4 billion** | **Average per year: EUR 488 million** | |
| Adjustment costs** | | | |
| **Citizens** | | | |
| New administrative burdens (INs) | N.A. | | |
| Removed administrative burdens (OUTs) | N.A. | | |
| ***Net administrative burdens**** | N.A. | | |
| Adjustment costs** | N.A | | |
| **Total administrative burdens***** | **- EUR 2.4 billion over 5 years** | **Average per year: EUR 488 million** | |

*(*) Net administrative burdens = INs – OUTs;*
*(**) Adjustment costs falling under the scope of the OIOO approach are the same as reported in Table 7 above. Non-annualised values;*
*(***) Total administrative burdens = Net administrative burdens for businesses + net administrative burdens for citizens.*

## 3. RELEVANT SUSTAINABLE DEVELOPMENT GOALS

*Table 94: Overview of relevant sustainable development goals*

| **IV. Overview of relevant Sustainable Development Goals – Preferred Option(s)** | | |
|---|---|---|
| **Relevant SDG** | **Expected progress towards the Goal** | **Comments** |
| SDG 8: Decent work and economic growth | Indirect contribution through improving certification helps increase competitiveness and economic efficiency, improving cybersecurity skills and workforce development through attestation. | Beneficiaries include SMEs and regulated entities, as it may foster secure digital trade |
| SDG 9: Industry, innovation | Strengthens EU cybersecurity posture through | Supports digital resilience and secure |

| | | |
|---|---|---|
| and infrastructure | ENISA's enhanced coordination role and ECCF reform | innovation ecosystems; primarily relevant for public administrations, critical infrastructure operators, SMEs, and service providers |
| SDG 12: Responsible consumption and production | Potential positive effect through certification frameworks and improved cybersecurity skills attestation. | – |
| SDG 13: Climate action | Neutral impact. | Dependent on ENISA's operational practices |
| SDG 16: Peace, justice and strong institutions | Improves trust in digital services and increased situational awareness also enhances the fight against cybercrime and skilled professionals contribute to securing institutions. | Reinforces transparency, rule of law, data privacy, security of institutions and institutional coordination through harmonised certification and cybersecurity skilled workforce |
| SDG 17: Partnerships for the goals | Reinforces cross-border cooperation among Member States and public-private partnerships in cybersecurity governance, as well as ENISA's cooperation with other European agencies. | Particularly relevant under ENISA's strengthened mandate and through shared governance models in the ECCF reform |

# ANNEX 4: ANALYTICAL METHODS

This annex describes the analytical methods used for the purposes of this impact assessment. It presents general assumptions, and the overview of impacts assesses. More detailed explanations regarding the methodologies are explained for each family of policy options.

## 1. GENERAL APPROACH

The assessment of the impact of the proposed policy options combines quantitative and qualitative analysis. The following methods were used to carry out this impact assessment:

- **Literature review:** A thorough desk research and documentary review provided foundational insights relevant to this impact assessment. The selected publications offer relevant information and data on the key aspects assessed as part of the present impact assessment.

- **Stakeholder consultation**: Semi-structured interviews were conducted with key stakeholders, including ENISA staff members, owners of national cybersecurity platforms, and experts involved in certification processes. Each interview utilised a tailored questionnaire. Targeted discussions with the representatives of Member States in various fora, based on a list of questions to organise the discussion were conducted. This was also complemented with the bilateral consultations. Furthermore, the outcomes from the public consultation and the call for evidence associated with this impact assessment supported the integration of diverse stakeholder perspectives and the triangulation of findings. In addition, findings from other stakeholder consultations conducted as part of the 2024 Evaluation report were considered to further substantiate the analysis.

- **Economic and statistical analysis:** To the extent possible and given the available data, the consequences and impacts of the policy options were monetised based on quantified cost-analysis, as described in Section 2 below. Benefits are largely analysed in qualitative terms, for the reasons explained in Sections 2 and 3 below. For estimates related to general business and economic indicators, Eurostat served as the primary source of statistical information. Additionally, more specific insights were derived from ENISA's thematic and annual reports, as well as its Single Programming Document 2025-2027. To verify assumptions and refine estimates, specific unpublished datasets were requested from ENISA. These datasets also served as a baseline for understanding ENISA's current activities and effort volumes, particularly concerning human resources.

## 2. KEY ASSUMPTIONS FOR THE QUANTIFICATION OF ECONOMIC IMPACTS

To quantify the economic impacts associated with the proposed measures, following assumptions were made:

- **The costs are aggregated over the next five years (2028-2032)** assuming that the legislation would start applying the 1st of January 2028. This is to take into account long-term impacts of certain measures.

- **Cost estimates for ENISA FTE**

The cost estimation per FTE across this impact assessment is based on previous evaluations, estimates from similar activities conducted in comparable EU agencies, and the CSA impact assessment, where the average cost of one FTE, adjusted for inflation, is calculated at **EUR 128 277**[185]. This estimated average cost of one full-time equivalent (FTE) is derived from two principal approaches:

(i) internal ENISA data on personnel costs for 2025, provided directly by the agency and reflecting average annual salary costs across staff profiles, resulting in an average cost of EUR 130 667/FTE; and

(ii) an analysis and actualisation of several estimates from previous ENISA evaluation report of 2017 and the Cybersecurity Act impact assessment, updated to 2025 values, resulting in an average cost of 125 887/FTE.

An additional estimate was calculated based on ENISA's reported staff expenditure in the Single Programming Document 2025-27 and Consolidated Annual Activity Report 2024, using figures for 2023 updated to 2025 values; however, as this figure closely aligns with the latest ENISA data (EUR 130 968/FTE), it is reported for transparency but not used in the final average.

Calculation: EUR 128 277 = (EUR 130 667 + EUR 125 887)/2

- **FTE for Member States**: Based on Eurostat data and OECD[186][187], the European average salary for ICT roles is approximately **EUR 56 500,** derived from data adjustments factoring in regional wage disparities and purchasing power variances.
- **Benchmarking against similar activities:** Regarding ENISA, the effort and resources required for setting up specific functions were benchmarked against analogous exercises conducted by other agencies, or for similar tools. These benchmarks provided guidance on expected human resource allocations, which were then adjusted to align with ENISA's average FTE costs, ensuring a tailored and context-appropriate financial projection.

---

[185] European Commission (2017). *Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA),* https://digital-strategy.ec.europa.eu/en/library/final-report-evaluation-european-union-agency-network-and-information-security-enisa.

[186] OECD (2024), *Building a Skilled Cyber Security Workforce in Europe*. Last accessed on 23/06/2025 and available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf

[187] particular the 'nama_10_fte' dataset, which provides average full-time equivalent salaries by country. Last accessed on 23/06/2025 and available at: https://ec.europa.eu/eurostat/databrowser/view/nama_10_fte__custom_13597179/bookmark/table?lang=en&bookmarkId=c29eed24-377e-4763-aaf0-0419906d2ecd

## 3. OVERVIEW OF IMPACTS BEING ASSESSED BY STAKEHOLDER

*Table 10: Overview of impacts by stakeholder*

| **Businesses**<br>NIS entities; conformity assessment bodies; ICT providers (applying to certification); ICT professional; businesses as users | **Citizens / consumers**<br>ICT users as consumers and citizens , ICT professional | **Public authorities**<br>National authorities doing supervisions of NIS 2; incident response teams /CSIRTs/Cyber agencies. | **EU institutions / ENISA** |
|---|---|---|---|
| **Costs**<br>*Direct: adjustment & administrative costs*<br>• Meeting new cyber requirements (adjustments costs – NIS2, certification)<br>• Accreditation fees for CABs<br>• Paying third party assessment (administrative costs – certification)<br>• Fee to be authorised provider of individual skills attestations<br>• | **Costs**<br>*Direct*<br>• Fees for obtaining a skills attestation | **Costs**<br>*Direct*<br>• Enforcement costs<br>• Adjustment costs: Transfer of national liaison officers and seconded national experts to ENISA | **Costs**<br>*Direct*<br>• Increased resources to ENISA (adjustment costs) |
| *Indirect*<br><u>As ICT provider</u><br>• Replacing ICT supply (retraining staff; interoperability with legacy systems)<br>• Impact on non-EU high risk businesses (market access restrictions)<br><u>As ICT user</u><br>• Increased prices due to supply chain restrictions (as ICT user) | *Indirect*<br><u>As ICT user, ICT professional</u><br>• Increased prices due to supply chain restrictions (as ICT user) | *Indirect*<br><u>As ICT user</u><br>• Renegotiating contracts in the context of public procurement procedures (restriction of suppliers)<br>• Increased prices due to supply chain restrictions (as ICT user) | *Indirect*<br><u>As trade partner</u><br>• Trade negotiations – market restrictions/retaliations<br><u>As ICT user</u><br>• Increased prices due to supply chain restrictions (as ICT user) |
| **Benefits**<br>*Direct*<br>• Trust & Uptake of ICT technologies<br>• Cost savings due to greater harmonisation<br>• Cost savings due to incident response/detection<br>• Costs savings due to less cyber incidents<br>• Fees from certification for CABs<br>*Indirect*<br>• Enhanced reputation & market opportunities due to certification and attestation<br>• Less dependencies & legal uncertainties (digital sovereignty; third countries)<br>• Market opportunities, competitiveness and innovation for EU and trusted providers | **Benefits**<br>*Direct*<br>• More certainty regarding trusted ICT solutions (certification)<br>*Indirect*<br>• Trust & Uptake of ICT technologies<br>• Enhanced privacy<br>• More job opportunities | **Benefits**<br>*Direct*<br>• Costs savings related to supervision<br>• Reduction of hassle costs due to greater harmonisation (certification; incident response coordination; NIS2)<br>*Indirect*<br>• Trust & Uptake of ICT technologies | **Benefits**<br>*Direct*<br>*Indirect*<br>• Trust & Uptake of ICT technologies (use of cloud and 5G by the Commission; ENISA)<br>• Increased reputation of ENISA towards MS and international partners |

## 4. METHODOLOGICAL EXPLANATIONS BY POLICY OPTION

### 4.1. Options related to ENISA mandate

#### 4.1.1. *Benefits and costs savings (Options A2 and A3)*

##### 4.1.1.1. Cost savings related to cybersecurity incidents

The quantitative benefits detailed below represent an estimate of the **possible impact in terms of cost savings of the measures included in options A2 and A3 in relations to cybersecurity incidents**. This is particularly relevant for enhanced operational coordination and situational awareness, such as the single repository or ENISA becoming a root authority within the international vulnerability identification systems. To estimate and show the possible impacts of the proposed measures on the EU's cyberposture, several assumptions have been made to quantify the benefits in a most representative way. The data limitations are further explained in section 6 of the report and *Annex 7*.

Based on the available data, this report measures the impact that proposed measures will have on reducing recovery costs from incidents. It is expected that the measures proposed will decrease the *mean-time-to-identify* and the *mean-time-to-detect*. As explained in *Annex 7*, both are drivers of the recovery costs from an incident.

To estimate the average cost of an incident, based on available data, it is assumed that the average cost of an incident is EUR 4.4 M which is the average cost of a data breach in Europe according to the data presented in *Annex 7 table 17*. This can be a very large underestimation depending on the type of incident. While data breaches represent one of the most widely spread incidents, there are other widely spread types of incidents, such as ransomware attacks or DDoS attacks as presented in *Annex 7 figure 12*.

The average recovery time for a data breach is currently at 241 days *Table 22*. It is assumed that the measures will lead to decreasing the recovery time from 241 to 200 days, reducing the recovery costs from EUR 4.4 M (BaU) to EUR 3.9 M (after the adoption of the measures proposed in A2/A3). The cost savings by number of incidents would be (4.4 – 3.9 =) EUR 0.5 million.

In order to aggregate the possible cost savings, an estimation needs to be made regarding the number of incidents per year. Incidents can be distinguished between their malicious and non-malicious intent (for instance human error). ENISA[188] observed 11,079 incidents (only malicious incidents), including 322 incidents specifically targeting two or more EU Member States. These are incidents that particularly affect NIS2 entities. Those entities are also expected to be the most impacted by the proposed policy measures. Considering that the gains would be fully reaped after some implementation time, we assume that they would intervene in year five. Over five years, the gains would be of 0.5 M x 11,079 = EUR 5.5 bn.

[188] *ENISA Threat Landscape 2024*

In order to take into account the business-as-usual scenario, we assume that some of these gains would be related to legislation in place, such as the CRA (20 to 33% of cost reduction, see below), this would lead to a range of benefits that might be related to measures improving detection and response under options A/A3 of **EUR 3.7 to 4.4 bn over five years** (applying the BaU factor to EUR 5.5 bn lead to 0.67 x 5.5 and 0.8 x 5.5).

Under the business-as-usual scenario, it is assumed that the number of recovery days would not decrease over time (or not as fast) staying at 241 days in the next five years (2028-2032). This might not be entirely accurate, considering that other factors, such as the existing legislation in place (NIS2, CRA) can also impact the recovery time thanks to better cybersecurity risk management measures in place and security by design approaches. At the same time, as presented in *section 2*, cybersecurity attacks are also gaining in complexity and are constantly evolving, hence the important of better situation awareness and response coordination. To make an estimate for the **BaU scenario**, we take the estimation of the reduction of cyber incidents made for the CRA (applicable by end of 2027) that could lead to a reduction of cybersecurity incidents by between **20 % and 33 %** and reduce incident-related costs by a similar percentage[189]. Following data limitations need to stressed:

- The proposed measures could also reduce the number of incidents as such. However, based on the data available, no reasonable assumption could be made on the extent to which the measures would affect the number of incidents.
- The average cost of an incident can be considerably higher, especially considering material and non-material damages as presented in *Annex 7*.

The number of incidents considered could be higher. A conservative assumption has been made that the measures would be particularly relevant for NIS2 entities as CSIRTs are already cooperating closely with ENISA on their protection. A higher estimate could be based on a Eurostat analysis[190] considers that according to Eurostat, 21.54 % of EU enterprises with 10+ employees experienced ICT-related security incidents in 2023. Taking the total number of enterprises 1.54 million, the number of enterprises that suffered incidents would amount to 331 100 enterprises experienced incidents (malicious and malicious). Assuming that these incidents would be data breaches and that according to ENISA, 68% of data breaches are of non-malicious intent, this would lead to 105 952 malicious incidents in Europe.

#### *4.1.1.2.* Benefits and costs savings related to European individual cybersecurity skills attestation schemes

Regarding ***economic operators***, the development of European individual attestation schemes would support the development of the Single Market by leading to the rise of providers authorised to deliver such attestations, who would gain visibility in a market which is today widely occupied by non-European providers, whether dedicated certification companies or larger tech companies.

---

[189] SWD(2022) 282 final, page 53
[190] https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf

More widely and beyond authorised providers, the development of European individual attestation schemes would support training and hiring practices by providing visibility and recognition of certifications, while at the same time ensuring quality assurance, thereby saving hiring departments difficulties

Regarding ***national authorities***, entrusting the elaboration and maintenance of European individual attestation schemes to ENISA and the delivery of such attestations to authorised providers, including national authorities, could ultimately lead to savings in terms of human resources for national authorities who develop today such attestations (or certifications) of people.

Additionally, national authorities would not be constrained to develop or maintain in-house schemes as they could rely on the European individual attestations, notably to check the competence of individuals working for managed security service providers or for hiring purposes. A rationalised and centralised EU individual attestation scheme would further rationalise the costs, avoiding proliferation of national schemes which aim at a similar objective across Member States but are developed independently across the EU.

Regarding ***benefits for citizens***, holding a cybersecurity attestation or certification enhances job market appeal and leads to wage increases. According to recent studies, 59 % of employees report a salary increase of 6–20 % within a year after being certified[191]. Attestations also support external career mobility[192] and skills portability, which is particularly valuable for entry-level professionals, young graduates, SMEs, and workers seeking mobility. This has a positive impact on salary levels, reflecting the recognised value of their expertise[193].

***Regarding the potential cost savings***, citizens would bear the cost of acquiring individual skills attestations. The cost of European individual cybersecurity attestations is expected to be closer to those delivered by public organisations and lower than the average cost of certifications from private bodies, potentially leading to cost savings. For example, attestations issued by public bodies in Europe cost around EUR 300-350, while the average cost for private certifications is around EUR 677 (excluding training). ENISA would advise on the price of European individual attestations, aiming for costs closer to those set by public authorities, which would benefit entry-level professionals, young graduates, SMEs, and workers seeking mobility.

[191] Pearson VUE 2025 Value of Certification Report - Candidate Report

[192] Agence nationale de la sécurité des systèmes d'information (ANSSI) (2025), Etude 2025: Les professionnels de la cybersécurité, https://cyber.gouv.fr/sites/default/files/document/Etude_des_professionnels_de_la_cybers%C3%A9curit%C3%A9_VF2.pdf

[193] Fortinet. (2023). 2023 Cybersecurity Skills Gap Report, https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf

Examples from European countries indicate that attestations issued by public bodies at national or regional level present a cost around EUR 300[194] and EUR 350[195]. In contrast, the average cost for obtaining a certification from private bodies is around EUR 677 per certification (training excluded)[196]. ENISA would advise on the price of a European individual attestation to be delivered by authorised providers, providing estimations of the cost of the attestations to offset the costs incurred. It can therefore reasonably be inferred that such costs would be closer to those set by public authorities. Although a European individual cybersecurity skills attestation scheme would not represent the only channel to obtain cybersecurity attestations or certifications, these estimates already show the potential positive impact of an EU-led skills attestation, especially for entry-level professionals, young graduates or SMEs, and workers looking for external mobility.

#### 4.1.2. *Costs related to ENISA mandate*

##### 4.1.2.1.FTEs costs on EU budget (all options)

The table below provides an aggregated overview of the costs related to Options A.1, A.2 and A.3 by stakeholder. Detailed explanations are included further below.

*Table 11: Allocation and costs of FTEs for Options A.1, A.2 and A.3*

| Option/ Stakeholder/ Purpose | Details | 2028 FTEs | 2029 FTEs | 2030 FTEs | 2031 FTEs | 2032 FTEs | Costs per year (EUR) | Total costs over 5 years (EUR) |
|---|---|---|---|---|---|---|---|---|
| **Option A.1** | | | | | | | | |
| **ENISA** | | - | - | - | - | - | - | - |
| **Member States** | | - | - | - | - | - | - | - |
| **Businesses** | | - | - | - | - | - | - | - |
| **Citizens** | | - | - | - | - | - | - | - |

[194] According to German law, the cost of a re-certification at EUR 221, which is expected to be slightly higher for first certification of individuals requiring entry-level certifications, therefore the cost of a first certification of this kind was assumed to be around EUR 300, while noting that costs can vary significantly depending on the process Source: Special Fee Regulation of the Federal Ministry of the Interior, for Building and Community for Individually Attributable Public Services within Its Area of Responsibility (Besondere Gebührenverordnung BMI – BMIBGebV), https://www.gesetze-im-internet.de/bmibgebv/BJNR135900019.html

[195] An analysis of professional designations in the UK indicating that and individual is operating at a recognized level of competence in the cyber profession indicate an average cost of GPB 300 for Associate Cyber Security Professional (ACSP) and Practitioner Cyber Security Professional (PraCSP). These are provided through the Cyber Security Professional curricula identified by the UK CSC. Sources: UK CSC, https://www.ukcybersecuritycouncil.org.uk/professional-registration/.

[196] This figure is calculated based on the examination fees for certifications provided by ISC2 (CISSP, ISSAP, ISSEP, ISSMP, CSSLP, CGRC, SSCP, and CCSP, https://www.isc2.org/register-for-exam/isc2-exam-pricing), ISACA (Source: https://www.isacaprep.com/how-much-is-the-cism-exam/) and SANS-GIAC, https://www.giac.org/pricing/, converted from USD to EUR using a 0.94 exchange rate, when needed. This average cost reflects the financial commitment required to achieve a certification in the field of cybersecurity.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Option A.2** | | | | | | | | |
| **ENISA** | | | | | | | | |
| **Reserve** | | 10 | 10 | 10 | 10 | 10 | 1 282 770 | 6 413 850 |
| CVD | | 15 | 15 | 15 | 15 | 15 | 1 924 155 | 9 620 775 |
| Mutual Assistance | | 4 | 4 | 4 | 4 | 4 | 513 108 | 2 565 540 |
| Support for critical sectors resilience | | 5 | 5 | 5 | 5 | 5 | 641 385 | 3 206 925 |
| Skills scheme development | | 2 | 2 | 2 | 2 | 2 | 256 554 | 1 282 770 |
| Skills scheme maintenance | | 6 | 6 | 6 | 6 | 6 | 763 662 | 3 848 310 |
| CRA platform | Day-to-day mgmt. | 10 | 10 | 10 | 10 | 10 | 1 282 770 | 6 413 850 |
| CRA platform | Vulnerability analysis | 5 | 5 | 5 | 5 | 5 | 641 385 | 3 206 925 |
| CRA platform extension | Single entry point | 8 | 8 | 8 | 8 | 8 | 1 026 216 | 5 131 080 |
| CRA implementation | Technical guidance, market analysis etc. | 8 | 8 | 8 | 8 | 8 | 1 026 216 | 5 131 080 |
| CRA implementation | Standardisation | 5 | 5 | 5 | 5 | 5 | 641 385 | 3 206 925 |
| CRA implementation | Market surveillance | 5 | 5 | 5 | 5 | 5 | 641 385 | 3 206 925 |
| CRA implementation | Testing and security evaluations | 4 | 4 | 4 | 4 | 4 | 513 108 | 2 565 540 |
| Operational cooperation | | 5 | 5 | 5 | 5 | 5 | 641 385 | 3 206 925 |
| Admin | | 10 | 10 | 10 | 10 | 10 | 1 282 770 | 6 413 850 |
| **TOTAL FTEs under Option A.2 for ENISA** | | **102** | **102** | **102** | **102** | **102** | **13 084 254** | **65 421 270** |
| NLOs Option A.2 (budget split bw ENISA and MS) | Daily allowances (EU budget) | 40 | 40 | 40 | 40 | 40 | 1 440 000 | 7 200 000 |
| **TOTAL Option A.2 for ENISA (FTEs + NLOs)** | | **142** | **142** | **142** | **142** | **142** | **14 524 254** | **72 621 270** |
| Setting up and operating the | | | | | | | 1 000 000 | 5 000 000 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CVD database | | | | | | | | |
| Skills scheme development, maintenance, and oversight | | | | | | | 212 920 | 1 064 600 |
| Skills website (one-off costs) | | | | | | | | 1 000 000 |
| CRA platform maintenance | | | | | | | 2 000 000 | 10 000 000 |
| CRA implementation | | | | | | | 2 000 000 | 10 000 000 |
| CTI services | | | | | | | 4 000 000 | 20 000 000 |
| Single entry point – one-off costs | Design, equipment, legislations | | | | | | | 8 000 000 |
| Secure communications set-up (one-off costs) | | | | | | | | 1 100 000 |
| Secure communications maintenance | | | | | | | 1 083 250 | 4 333 000 |
| Cyber maturity | | | | | | | 3 000 000 | 15 000 000 |
| **Total costs for ENISA** | | | | | | | | **148 118 870** |
| **Member States** | | | | | | | | |
| NLOs seconded to ENISA (budget split bw ENISA and MS) | MS budget | *(40)* | *(40)* | *(40)* | *(40)* | *(40)* | 2 260 000 | 11 300 000 |
| **TOTAL Option A.2 for Member States** | | *(40)* | *(40)* | *(40)* | *(40)* | *(40)* | **2 260 000** | **11 300 000** |
| **Businesses** | **Potential cost of paying a fee to ENISA to get authorised to deliver European individual attestations** | | | | | | | |
| **Citizens** | **Potential cost of acquiring the individual skills attestation** | | | | | | | |
| **Option A.3**<br><br>(building on | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| option A2) | | | | | | | | |
| **ENISA** | | | | | | | | |
| FTEs covering areas under Option A.2 (FTEs + NLOs) | | **142** | **142** | **142** | **142** | **142** | **14 524 254** | **72 621 270** |
| Other costs for ENISA under Option A.2 | | | | | | | | **75 497 600** |
| Operational team | Providing direct support under the NIS 2 Directive | 15 | 25 | 25 | 25 | 25 | 2 950 371 | 14 851 855 |
| EU Cybersecurity Umbrella | | 2.5 | 2.5 | 2.5 | 2.5 | 2.5 | 320 693 | 1 603 463 |
| Additional SNEs Option A.3 (budget split bw. ENISA and MS) | Daily allowances (EU budget) | *5* | *5* | *5* | *5* | *5* | 180 000 | 900 000 |
| **Total costs related to FTEs, NLOs and SNE for ENISA** | | **164.5** | **174.5** | **174.5** | **174.5** | **174.5** | **17 975 318** | **89 876 590** |
| **TOTAL Option A.3 for ENISA** | | | | | | | | **165 374 188** |
| **Member States** | | | | | | | | |
| NLOs seconded to ENISA under Option A.2 (budget split bw ENISA and MS) | MS budget | *(40)* | *(40)* | *(40)* | *(40)* | *(40)* | 2 260 000 | 11 300 000 |
| Additional SNEs Option A.3 (budget split bw ENISA and MS) | MS budget | *(5)* | *(5)* | *(5)* | *(5)* | *(5)* | 282 500 | 1 412 500 |
| **TOTAL costs for Member States under Option A.3 (Option A.2 + additional SNEs under Option A.3)** | **MS budget** | ***(45)*** | ***(45)*** | ***(45)*** | ***(45)*** | ***(45)*** | **2 542 500** | **12 712 500** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Businesses** | The same as Option A.2 (No additional costs under Option A.3.) | | | | | | | |
| **Citizens** | The same as Option A.2 (No additional costs under Option A.3.) | | | | | | | |

4.1.2.2.Costs on EU budget (Option A.2)

For implementing ***Option A.2,*** ENISA requires a total of **EUR 148 118 870 additional cost over 5 years (recurring cost of 138 million (M) over 5 years (EUR 26.7 in 2028 and EUR 27.8 yearly from 2029 to 2032) and a one-off cost of EUR 10.1M)**, which is an incremental cost compared to the baseline (i.e. it does not include current ongoing activities). See details below.

(a) Costs of FTEs and NLOs for the preferred option (Option A.2)

For implementing Option A.2 the total recurring costs related to 102 FTEs and 40 NLOs are EUR 14 524 254 per year, which amounts to EUR 72 621 270 over 5 years.

Around 102 additional FTEs will be needed to deliver the additional tasks, with an estimated total annual recurring cost of EUR 13.08M for the Agency (EUR 65.42M over 5 years) and 40 National Liaison Officer (NLOs) seconded by the Member States to ENISA, with an estimated recurring cost of EUR 1.44M yearly, i.e. EUR 7.2M over 5 years.

The **cost estimation per FTE** across this impact assessment is based on previous evaluations, estimates from similar activities conducted in comparable EU agencies, and the CSA impact assessment, where the average cost of one FTE, adjusted for inflation, is calculated at **EUR 128 277**[197]. This estimated average cost of one full-time equivalent (FTE) is derived from two principal approaches:

1) internal ENISA data on personnel costs for 2025, provided directly by the agency and reflecting average annual salary costs across staff profiles, resulting in an average cost of EUR 130 667/FTE; and
2) an analysis and actualisation of several estimates from previous ENISA evaluation report of 2017 and the Cybersecurity Act impact assessment, updated to 2025 values, resulting in an average cost of 125 887/FTE.

An additional estimate was calculated based on ENISA's reported staff expenditure in the Single Programming Document 2025-27 and Consolidated Annual Activity Report 2024,

[197] European Commission (2017). *Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA),* https://digital-strategy.ec.europa.eu/en/library/final-report-evaluation-european-union-agency-network-and-information-security-enisa.

using figures for 2023 updated to 2025 values; however, as this figure closely aligns with the latest ENISA data (EUR 130 968/FTE), it is reported for transparency but not used in the final average.

Calculation: EUR 128 277 = (EUR 130 667 + EUR 125 887)/2

Firstly, the administration and operation of the ***EU Cybersecurity Reserve*** requires around **10 FTEs**, resulting in a total cost of **EUR 1.28M per year**; to be complemented by procured services from trusted managed security service providers[198].

Secondly, ENISA should further enhance its activities around the creation of a ***European vulnerability database*** and support Member States in activities related to the coordinated vulnerability disclosure (CVD). To provide Member States with added value information stemming from advanced analysis of vulnerabilities, ENISA would require **15 additional FTEs**, which results in a total cost of approximately **EUR 1.924 million per year**.

Thirdly, for ENISA support to Member States in the ***mutual assistance and supervision NIS 2 Directive entities***, subject to the jurisdiction of several Member States (link with option C). This would result in costs for human resources with minimum **4 additional FTEs**, equal to EUR **513 108 per year**.

Fourthly, for the support of critical sectors resilience (including healthcare cybersecurity Action Plan implementation) 5 FTEs are needed, which amounts to a yearly recurring cost of EUR 641 385, i.e. EUR 3.2M over 5 years.

Fifthly, for the development of ***European individual attestation schemes***, considering that there are 12 different roles under the European Cybersecurity Skills Framework and that the development of schemes for all of those roles would be gradual, this action would require minimum **2 additional FTEs**, amounting to **EUR 256 554** for schemes development.

In addition, **6 FTEs** would be required for ***maintenance and auditing tasks for the providers*** that would be granted the role of entities issuing attestations, costing **EUR 769 662 per year**. These FTEs would be **recurrent for the first five years,** covering the preparation and roll-out of the first European individual attestation scheme and starting the second scheme[199]. To meet the market demand most effectively and ensure budgetary efficiency, **fees collected from providers would gradually complement and fully replace the EU budget after five years.**

In more details, based on ENISA's experience in running pilot projects, the first scheme would take five years to set up, test and roll-out[200]. During the first five years, EU budget

[198] The cost of the procurement of services from trusted MSSP are to be financed from the EU funding programme (currently Digital Europe Programme) via contribution agreement, as provided by the Cyber Solidarity Act.

[199] There are 12 ECSF cybersecurity profiles in total which can be divided into subsets. Therefore, there could be 12 European individual cybersecurity skills attestation schemes and potentially new ones in the future.

[200] Estimations are provided by analogy based on ENISA's experience in running pilots on a European individual attestation scheme, implementing the communication on the Cybersecurity Skills Academy.

would allow to cover the development, testing and rolling out of the first European individual attestation scheme. This period would be divided into two phases: (1) after an initial three-year period, during which EU budget would be necessary to nurture and test the model, (2) the activity would gradually become self-financed while still being supported by EU budget over the two following years. During this two-year transition period, both fee-based revenues and EU budget would support the model until it reaches sufficient maturity. In parallel, during the years four and five, ENISA would start developing a second scheme justifying to keep the same level of financing from EU budget for all five years Before the model would become fully independent financially.

It is taken into due account that as the schemes and the demand for authorisation from providers grows, this could lead to numerous applications of candidate attestation providers to be assessed by ENISA and ultimately, a growing number of providers for ENISA to supervise to ensure consistency in implementing the schemes. Consequently, ENISA would likely need additional resources to deliver on its tasks (authorisation and supervision). After year five, these additional **costs would no longer be funded by the EU budget but by the fees collected from providers.** The fees could also be used to cover the cost of training a pool of auditors in each Member State to perform the supervision tasks and to set up an internal governance ensuring uniform implementation of the schemes.

Sixthly, in the context of the Cyber Resilience Act (CRA) **23 FTEs** are needed, out of which 10 FTEs for the day-to-day ***management of the single reporting platform for CRA***, 5 FTEs for platform services (vulnerability analysis) and 8 FTEs for managing the single entry point (in connection with the Digital Omnibus). This amounts to a total of **EUR 2 950 371 per year**.

Seventhly, for supporting the ***implementation of the Cyber Resilience Act***, **22 FTEs** are needed. 8 FTEs are needed for the work on technical guidance, product security expertise and market analysis, 5 FTEs on standardisation to support CRA implementation, 5 FTEs for supporting the market surveillance activities and 4 FTEs for conformity/testing and security evaluations. This amounts to a recurring cost of **EUR 2 822 094 per year (i.e. EUR 14.11M over 5 years)**.

Eighthly, for ***operational cooperation*** including situational awareness and additional **5 FTEs** are needed, amounting to **EUR 641 385 yearly.**

Additionally, in the context of ***operational cooperation***, an additional cost stems from the daily allowance of National Liaison Officers seconded by each Member State to ENISA, **40 NLOs in total**, which amounts to **EUR 1 440 000 yearly** (see below further details under costs for National Authorities and Economic Operators).

Finally, given the overall increased headcount of ENISA an additional **10 FTEs** are needed for ***admin/support functions*** (such as accounting, HR, IT etc.), amounting to **EUR 1 282 770 per year.**

**Summary of calculations related to FTEs and NLOs for ENISA under Option A.2:**

- **EU Cybersecurity Reserve:** 10 FTEs × EUR 128 277 = EUR 1 282 770

- **Vulnerability database and CVD:** 15 FTEs × EUR 128 277 = EUR 1 924 155
- **Mutual assistance and supervision:** 4 FTEs × EUR 128 277 = EUR 513 108
- Support for critical sectors resilience (including healthcare cybersecurity Action Plan implementation): 5 FTEs × EUR 128 277 = EUR 641 385
- **European individual attestation schemes (development + maintenance):**
  - Development: 2 FTEs × EUR 128 277 = EUR 256 554
  - Maintenance and auditing: 6 FTEs × EUR 128 277 = EUR 769 662
  - **Total: 8FTEs => EUR 1 026 216**
- **CRA platform :**
  - day-to-day management of the platform: 10 FTEs x 128 277 = EUR 1 282 770
  - vulnerability analysis: 5 FTEs x 128 277 = EUR 641 385
  - single entry point: 8 FTEs x 128 277 = EUR 1 026 216
  - **Total: 23 FTEs => EUR 2 950 371**
- **Supporting the implementation of the CRA:**
  - technical guidance, product security expertise, market analysis: 8 FTEs x 128 277 = EUR 1 026 616
  - standardisation: 5 FTEs x 128 277 = 641 385
  - supporting market surveillance activities: 5 FTEs x 128 277 = EUR 641 385
  - conformity assessment/testing and security evaluations: 4 FTEs x 128 277 = EUR 513 108
  - **Total: 22 FTEs => EUR 2 822 094**
- **Operational cooperation, situational awareness:**
  - 5 FTEs x 128 277 = EUR 641 385
  - 40 national liaison officers x EUR 150 daily allowance x 20 days x 12 months = EUR 1 440 000
- **Support/admin functions:** 10 FTEs x 128 277 = EUR 1 282 770

**TOTAL costs related to 102 FTEs and 40 NLOs: EUR 14 524 254 per year (recurring costs), which amounts to EUR 72 621 270 over 5 years**

(b) Other costs under preferred option (A.2) – not related to FTEs and NLOs

***CVD database***

For setting up and operating the CVD database an annual EUR 1 000 000 recurring costs are estimated (i.e. 5 000 000 over 5 years).

***CRA platform***

For the CRA single reporting platform and depending on the final architecture of the CRA platform (including possible extensions with the single entry point), maintenance costs could amount yearly for up to EUR 2M recurring costs (**total of EUR 10M over 5 years**). The

current procurements for the establishment is of EUR 12 million[201]. The estimates consider that additional values are covered by contribution agreements to cover the operation and maintenance of the platform, that will need to be replaced by FTEs.

***CRA implementation***

The CRA implementation requires as well a yearly recurring cost of EUR 2M (i.e. EUR 10M over 5 years).

***Extension of single reporting platform with the single entry point***

The following costs would be covered by a **one-off cost of 6 million EUR**, which would be used for studying specific requirements related to the legislative act and translation of specific requirements into architectural design, evaluation of system integration with existing platform, development of specific workflows and templates, acquisition of necessary hardware, software and licenses, user interface design, deployment and testing, security assurance, mission and outreach costs.

In addition, operational expenses are estimated to be around EUR 500 000 per newly added legislation (one-off costs) for the extension. The assumption is that at least four legislations would be added in the next five years, amounting to a total of **EUR 2 million (one-off costs).**

***Procuring CTI services***

The costs related to procuring cyber threat intelligence would amount to approximately EUR 4 000 000 per year, i.e. to **EUR 20 million over 5 years**. See for reference: Service to Support the Cyber Situation and Analysis Centre for the European Commission https://ted.europa.eu/en/notice/-/detail/18139-2023.

***European individual cybersecurity skills attestation schemes***

Operational costs would need to support ENISA's activities related to the European skills attestation schemes. First, there would be a **one-off cost of EUR 1 million to design, develop, and penetration-test a secure website for running the mechanism[202].**

Second, further compliance costs would exist and need to be borne by EU budget during the first three years and shared between EU budget and fees during the two-year transition period. Such costs would cover activities related to the **development and maintenance of schemes,** including expenses of members of an ad hoc working group that would support ENISA in developing the schemes (reimbursement of expenses and payment of rapporteurs),

---

[201] *EU funding and Tenders Portal :* https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/46439658-5635-4465-ae7d-0a40e6e8e546-CN?order=DESC&pageNumber=1&pageSize=50&sortBy=startDate&isExactMatch=true&cftPartyLegalEntityId=47352382; *ENISA website:* https://enisa.europa.eu/procurement/implementation-of-the-single-reporting-platform

[202] Estimation provided by ENISA.

missions to audit on-site providers, and training of assessors to ensure homogenous application of the schemes. It can be estimated that the total compliance costs would amount to costs of **EUR 1,064,600 over 5 years, i.e. EUR 212 920 per year (recurring costs)**, by applying the following estimations: the ad hoc working group would cost EUR 800,000, training of two assessors per Member State would amount to EUR 129,600 and auditing one entity per Member State would amount to EUR 135,000.

In more details:

1) **Costs of training assessors** (on top of FTEs already included): it can be estimated that an additional EUR 129,600 would be needed. This estimation is based on analogy with UK courses to train Cyber Essentials Assessor, IASME Cyber Assurance Assessor or Cyber Essentials PLUS Assessor, for which we could estimate that the costs would be similar, amount to GBP 500 + VAT.

Calculations:

- 500 + (0.2x500) = 600 (Course Details and Certification Body Requirements v6). To implement the first scheme, we could estimate 2 assessors per Member State.
- 600x27x2 = 32,400
- 32,400x3 (first three years being fully EU budget) (97200) + (32,400/2)x2 (two year transition period being co-funded with the fees)= 129,600

2) **Cost of an onsite audit**: Using as a point of reference audits for ISO/IEC 17024 accreditation – for providers that want to conduct exams and certify individuals – , such accreditation can vary depending on the accrediting body, scope of certification, and location. Organisations such as the International Accreditation Service or ANAB (US), COFRAC (FR), DakkS (DE) do not publicly list their prices. The cost therefore needs to be derived with supposition based on available information: considering that an on-site audit for ISO/IEC 17024 could be considerably cheaper than an organisational audit under ISO 27001 (estimated EUR 30,000, see section 4.2) and that, in this case, the audit would not cover all elements of the accreditation package, it could be estimated that on-site audits would represent a **one-off cost of EUR 5,000** (covering the review of documentation, on-site audit and post audit report). Should ENISA audit **one entity per Member State during the first five years**, this would amount to 5,000x27= EUR 135,000

3) **Cost of ad hoc working group:** ENISA estimates the yearly cost of the AHWG to amount to EUR 200,000.

Calculations:

- AHWG: 200,000x3 (first three years being fully EU budget) + (200,000/2) x2 (two year transition period being co-funded with the fees)= 800,000

***Secure communications***

The setting up of secure communications entails a one-off cost of EUR 1.1M in the first year (2028) and a yearly recurring maintenance cost of EUR 1 083 250 over the next 4 consecutive years (2029-2032).

***Cyber maturity***

To strengthen the cybersecurity posture of ENISA by reaching the required cyber maturity level the recurring cost amounts to EUR 3M per year (i.e. EUR 15M over 5 years), including the migration to secure European Data Centre. It is of paramount importance that the EU Cybersecurity Agency has the highest levels of cybersecurity and is recognised as a trust partner and lead by example in Europe.

(c) Total annual costs (FTEs and other costs) under preferred option (A.2)

**Total annual cost for ENISA under Option A2 => EUR 148 118 870 over 5 years, broken down as follows in recurring and one-off costs:**

- **Total annual recurring costs for FTEs and NLOs for ENISA:**

  EUR 1 282 770 (Reserve)
  + EUR 1 539 324 (Vulnerability database and CVD)
  + EUR 513 108 (Mutual assistance and supervision)
  + EUR 641 385 (Support for critical sectors resilience (including healthcare cybersecurity Action Plan implementation)
  + EUR 1 026 216 (Attestation schemes)
  + EUR 3 335 202 (CRA platform)
  + EUR 2 822 094 (Implementation of CRA)
  + EUR 641 385 (Operational cooperation)
  + EUR 1 440 000 (Daily allowances for 27 NLOs)
  + EUR 1 252 770 (Admin)
  = **EUR 14 524 254 (rounded to EUR 14.5M), i.e. EUR 72 621 270 over 5 years.**
- **Other annual recurring costs:**

  EUR 4 000 000 (Costs related to procuring cyber threat intelligence (CTI))
  + EUR 2 000 000 (CRA platform maintenance)
  + EUR 2 000 000 (CRA platform implementation)
  + EUR 1 000 000 (Setting up and operating the CVD database)
  + EUR 212 920 (Skills scheme development and maintenance)
  **+** EUR 1 083 250 (Secure communications maintenance – over 4 years after set-up)
  + EUR 3 000 000 (Cyber maturity)
  = EUR 12.21M in the first year and EUR 13.3 over 4 years, i.e. **EUR 65 397 600 over 5 years**
- **Other one-off costs:**

  EUR 6 000 000 (Single entry point - one-off adjustment costs for various activities ranging from design to equipment)
  + EUR 2 000 000 (Single entry point – four newly added legislations)
  + EUR 1 000 000 (Skills website)
  + EUR 1 100 000 (Secure communications set-up)
  = **EUR 10 100 000**

4.1.2.3. Costs for national authorities and economic operators

***National liaison officers***

In addition to ENISA's staff, each Member State would designate at least one national liaison officer (NLO) as part of this operational team, in total 40 NLOs from the 27 MS. For cost estimation, we assume the average cost of EUR 56 500[203] applies to NLOs, as actual costs can vary across EU Member States. This assumption is justified because national liaison officers would retain their national salary and receive an allowance from ENISA, which may vary depending on multiple factors. Taking this information into account, the total cost of 40 NLOs would result in EUR 2.26M, to be borne by Member States' National Authorities.

**Calculations:**

**Total annual recurrent cost from MS budget:** 40 national liaison officers × EUR 56 500 = **EUR 2 260 000**

***European individual cybersecurity skills attestation schemes***

National authorities and economic operators may incur costs if they choose to **participate in developing European individual attestation schemes**, but such involvement is voluntary.

Similarly, both national authorities and economic operators may **pay a fee to ENISA** to become authorised to deliver European individual attestations. This cost is only borne by those who choose to become authorised and is offset by income from applicants seeking attestations.

To provide an indication of the costs of becoming an authorised provider to deliver EU individual cybersecurity skills attestations and maintaining this authorisation, information publicly available as well as information gathered by ENISA directly from countries in the framework of the pilot project on an individual cybersecurity skills attestation scheme has been used.

In particular, three countries which have established an attestation system for specific cybersecurity profiles have been explored (UK, SK and CY):

- The ***UK*** Cyber Security Council does not publicly list the cost for an organisation to become a Licensed Body under its Standard for Professional Competence and Commitment (SPCC). The process involves: a formal application and vetting process, demonstrating capability to assess professionals against the SPCC, ongoing compliance and reporting and licensing fees.

[203] See assumptions above based on OECD figures.

- In ***Cyprus***, the Digital Security Authority (DSA) has developed the Cybersecurity Maturity Assessors scheme and commissioned a public university to design a databank of 350 questions covering the required skills and knowledge. The DSA further defined a set of requirements to become an examination centre. Two examination centres have been approved. However, the cost of applying to become an examination centre is not publicly disclosed on the DSA website.
- ***Slovakia*** has developed two individual certifications for the profiles of Cybersecurity Manager and Cybersecurity Auditor. The model involves the National Cybersecurity Authority (NBU) in charge of certification requirements, including content and assessment methods, the **National Accreditation Authority (SNAS)**, who oversees the accreditation of providers, and certification accreditation bodies, the only entities allowed to issue certificates. Only the National Competence and Certification Centre (KCCB) for cyber the role profile Cybersecurity Auditor, and KCCB and a private accredited certification body for the profile Cybersecurity Manager have been allowed to issue certificates as of September 2025.

The SNAS has published the rates below[204], which were used in this impact assessment as an indication of the cost (fees) of an initial authorisation and renewal:

*Tables 12 and 13: Rates for accreditation of bodies certifying persons in Slovakia in 2025 (in EUR)*

| **sector-specific scheme** | **rate for accreditation** | **rate for reaccreditation** | **rate for surveillance** | **rate for annual fee for maintaining accreditation** |
|---|---|---|---|---|
| in the field of cyber security, information systems | 5,368 | 4,880 | 3,904 | 800 |

In case of assessment of certification body certifying persons as well as persons according to sector-specific schemes (in the field of cyber security, information systems) the resulting rate shall be calculated as the sum of rates for all activity types/categories and sector-specific scheme decreased by EUR 1,464 for accreditation / reaccreditation and by EUR 976 for surveillance.

| **Duration of the test *** | **rate for witness assessment** |
|---|---|

[204] Decision RR-02: Price list of SNAS services : https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf,

| | |
|---|---|
| up to 0,5 day | 1,220 |
| up to 1,5 day | 1,708 |
| 2 and more days | 2,440 |

*Note: The audit day is considered one day of verification by one verifier.

Calculations (estimations, using SK figures):

**Cost of an initial authorisation, maintenance of the authorisation and surveillance**:

- rate for accreditation + rate for surveillance + rate for witness assessment (taking "up to 1,5 day" rate in the absence of indicate as to the duration of the witness assessments for existing certifications) – decrease for accreditation – decrease for surveillance
- 5 368 + 3 904 + 1 708 - 1 464 – 976 = **EUR 8 540 (fixed costs)**
- An **additional EUR 800 would need to be paid covering the annual fee** of maintaining the accreditation.

4.1.2.4.Additional costs on EU budget for O***ption A.3***

Option A.3 proposes a significant reform of ENISA's mandate, placing a strong emphasis on operational support. This approach builds on the reforms proposed in Option A.2 and aims to transform ENISA into a central actor for incident response, policy advice, and direct operational intervention at the EU level. The financial implications of implementing Option A.3 are higher than Option A.2, with an estimated total cost of approximately EUR 165.37M over 5 years for ENISA and EUR 12.7M over 5 years for MS. The recurring yearly costs for ENISA in top of Option A.2. amount to EUR 3.45M (i.e. EUR 17.26M over 5 years) and for MS EUR 282 500, i.e. EUR 1 412 500 over 5 years. This expenditure reflects the investment required to extend ENISA's mandate, establish an EU-level cybersecurity umbrella, and create a dedicated operational team with NLOs to support entities under the NIS 2 Directive across all Member States.

Option A.3. builds on option A.2., thus all the costs considered under option A.2. have to be considered under this option as well.

Additionally, there are two key components under Option A.3:

A) the EU-level cybersecurity umbrella and
B) the establishment of an operational team to provide direct support to entities under the NIS 2 Directive.

Furthermore, EUR 180 000 for the daily allowances of 5 Seconded National Experts (SNEs) should be counted (see more details under the costs of Member States below)**.**

The costs for this component are estimated at EUR 13.53 million yearly:

- EUR 10.1 million - costs of Option A.2. and
- EUR 3.27 million average yearly costs stemming from the two key components mentioned above
- EUR 180 000 for the daily allowances of 5 Seconded National Experts (SNEs).

See further details below.

A) The first key component is the creation of an EU-level cybersecurity umbrella, which includes policy advice, serving as a centre for information, and functioning as a Computer Emergency Response Team (CERT). Based on actualised human resources cost estimates from the European Commission's 2017 evaluation of ENISA[205], a total of 2.5 FTEs would need to be added to the reforms proposed in Option A.2.

Calculations:

- **Additional 2.5 FTEs for the Cybersecurity Umbrella:**
  2.5FTEs x EUR 128 277 = EUR 320 692 average costs yearly.
  This amounts to EUR 1 603 460 over 5 years.

B) The other key component is the **establishment of an operational team to provide direct support to entities under the NIS 2 Directive**. This team, composed of ENISA staff and national liaison officers, would operate upon request from Member States. According to the same evaluation, the initial setup would cost around EUR 1.92 million, requiring 15 FTEs. Once fully operational, management and maintenance costs would reach around EUR 3.2 million, assuming the team grows to 25 FTEs by the 2nd year. The total cost for this component is estimated at EUR 5.13 million for the first 1–2 years, including both initial setup and operational costs.

Calculations:

- **Initial setup:** 15 FTEs × EUR 128 277 = EUR 1 924 155
- **Management and maintenance (fully operational):** 25 FTEs × EUR 128 277 = EUR 3 206 925

**Total cost for the first 2 years (setup + operational):** EUR 1 924 155 (setup) + EUR 3 206 925 (maintenance) = **EUR 5 131 080.**

Calculated over the assessment period of 5 years the total costs amount to EUR 14.75 million: (15 FTEs + 4 x 25 FTEs) x 128 277 = EUR 14 751 855 (calculating with 25 FTEs from the 2nd year).

This means a yearly average cost of:

[205] European Commission (2017). Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA), https://digital-strategy.ec.europa.eu/en/library/final-report-evaluation-european-union-agency-network-and-information-security-enisa

EUR 14 751 855 / 5 years = EUR 2 950 371.

Additionally to component A) and B), the daily allowances of 5 seconded national experts (SNEs) (=5 x EUR 150 daily allowance x 20 days x 12 months) EUR 180 000 should be added (see further details under costs of Member States below).

**Calculations of the total costs of Option A.3 for ENISA**:

*Recurring costs related to FTEs and NLOs:*

EUR 14 524 254 (from Option A2)

**+** EUR 320 692 (EU Cybersecurity Umbrella additional 2.5 FTEs)

+ EUR 2 950 371 (operational team for NIS2)

+ EUR 180 000 (daily allowances for 5 SNEs)

= EUR 17 975 318 yearly recurring costs, i.e. **EUR 89.88M** over 5 years.

*Other costs (only from Option A2):*

**EUR 75.5M**

**In total:** EUR 89.88M+EUR 75.5M = **EUR 165.38M over 5 years**

4.1.2.5. Additional costs for national authorities for Option A.3

In addition to the 40 NLOs designated under Option A.2, some Member States would designate additional seconded national experts (SNEs) as part of this operational team, which would be about 5 SNEs (from all MS). For cost estimation, we assume the average cost of EUR 56 500 applies to SNEs, as actual costs can vary across EU Member States. This assumption is justified because SNEs would retain their national salary and receive an allowance from ENISA, which may vary depending on multiple factors. Taking this information into account, the total cost of 5 SNEs would result in EUR 282 500 yearly, i.e. EUR 1 412 500 over 5 years, to be borne by Member States' National Authorities.

Calculations:

**Total annual recurrent cost:** 5 SNEs × EUR 56 500 = **EUR 282 500**

**In total:** EUR 11.3M (from Option A.2) + EUR 1.41M **= EUR 12.71M for Option A.3 over 5 years for MS**

### 4.2. Options related to the certification framework (B)

The following scenarios and combinations of policy options have been considered for the cost calculations of FTEs for ENISA and MS:

*Table 14: Scenarios for development of schemes under ECCF, and percentage of maintenance costs covered by fees*

| Policy options | 2024 | 2025 | 2026 | **2027** | 2028 | 2029 | 2030 | 2031 | 2032 |
|---|---|---|---|---|---|---|---|---|---|
| **BaU** | **EUCC adopted** | | | | 0% | 50% | 100% | 100% | 100% |
| **BaU** | | | **ID Wallet** candidate scheme | Scheme adopted<br><br>0% | 0% | 0% | 50% | 50% | 100% |
| **BaU** | | | **MSS** candidate scheme + 1st vertical *Gradually additional layers (tbc)* | *Scheme adopted*<br><br>0% | 0% | 0% | 50% | 50% | 100% |
| B+ D3 | | | | | **EUCS** candidate scheme (tbc) | Scheme adopted 0% | 0% | 0% | 50% |
| B2 + B3 | | | | | | **New candidate scheme (entities)** | Scheme adopted 0% | 0% | 0% |

The assumptions **of 2 FTEs for the maintenance of schemes** (included in B1/B2) take into account the following activities:

- the preparation, update and endorsement of technical specifications and guidelines, to support the harmonised operation of the schemes;
- interactions and, where relevant, establishment of liaisons with relevant stakeholders, including for the purpose of receiving technical contributions;
- advice on the necessary improvements and updates to the schemes;
- exchange of information related to the implementation of the schemes; and
- contribution to peer review and peer assessment mechanisms and analysis of their outcome with a view of improving the operation of the schemes.

The estimates related to the FTEs for ENISA and for Member States are based on the assumptions presented in the general parts of this document. The FTE increase for ENISA has been estimated on the basis of the *BaU scenario* in which ENISA has 9 FTEs covering following activities:

- Development of schemes

- Horizontal - Supporting ECCF governance ECCG, SCCG; horizontal issues: accreditation & notification of CABs; ECCG sub-group related to horizontal activities such as evaluation of encryption mechanisms
- Horizontal - Outreach & uptake of certificates - Website of certificates, CEF CSP, capacity building with MS

The **operational costs** related to maintenance consider the following assumptions:

- **The cost of ad hoc working group/ECCG sub-group & other related activities for the maintenance work** has been estimated at the yearly cost of EUR 200,000 based on figures from ENISA. Specifically, the maintenance considers two in person meetings with experts per year (EUR 100 000), costs of contractors supporting the development and review of supporting documentation for the scheme, the uptake of certification schemes, support the peer assessments and the implementation of conformity assessments (4 x 15 000 = EUR 60 000). The cost also includes operational part of the CEF platform and the ENISA certification website (EUR 40 000).

- **Fees related to maintenance of certification schemes**

Under B2, the expectations are that the revenues from fees to raise in progression with the adoption of every new scheme, according to the pattern described in the table above. The first three years of maintenance (starting the year of adoption), no significant revenues would be expected, with a gradual progression from 50% (year 4 and 5) to 100%. The pattern for the first adopted EU scheme (EUCC) would be slightly different with a faster progression towards full coverage of costs by fees considering the that the scheme is already operational.

As a result, under B2 + D3, the following revenues would be gathered.

Year Fees

2028 0

2029 100 000 (revenue) – one scheme (EUCC – 50%)

2030 400 000 (revenue) – three schemes (EUCC – 100%, ID Wallet – 50% , MSS – 50%)

2031 400 000 (revenue) – three schemes (EUCC – 100%, ID Wallet – 50%, MSS – 50%)

2032 800 000 (revenue) – five schemes (EUCC - 100%, ID Wallet - 100%, MSS - 100%, EUCS - 50%, 5G -50%)

- **Total operational costs taking into account the fee revenues** (under B2)

In order to estimate the total operational costs considering the revenues made by ENISA through the collection of fees, we deduct the revenues from the total operational costs, as follows (over five years).

The **estimates related to the costs of a certification scheme** are based on the below:

The picture illustrates the typical steps and hence costs for businesses when going through a certification process.[206]


**Average cost of security audit**

In the EU in 2025 typically ranges from EUR 3.000 to over EUR 50.000, depending on the organization's size, complexity, audit scope, and regulatory requirements, with compliance-focused audits such as ISO 27001 costing between EUR 10.000 and EUR 50.000[207] .

**Average costs of a qualification/certification process**

The following publicly available sources have been looked at to estimate the the range of costs for a certification process of cloud services, from EUR 5 000 to 160 000:

---

[206] ENISA, *CONFORMITY ASSESSMENT OF Qualified Trusted Service Providers - Technical guidelines for conformity assessment of qualified trust service providers*, March 2020, available at (30.09.2025): https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Conformity%20Assessment%20of%20Qualified%20Trust%20Service%20Providers.pdf

[207] See the following articles: https://qualysec.com/it-security-audit-cost/; https://atlantsecurity.com/blog/cost-of-cybersecurity-due-diligence/#elementor-toc__heading-anchor-21; https://cyberupgrade.net/blog/compliance-regulations/iso-27001-cost-understanding-certification-audit-and-implementation-expenses-in-2025.

*Table 15: Overview of existing national cloud certifications & qualifications*

| Scheme | Purpose | Target Cloud Level | Based on | Recognition | Base Standard | Auditing Requirements | Source |
|---|---|---|---|---|---|---|---|
| SecNumCloud *France* | Ensure high cybersecurity for cloud services | High | ANSSI controls (ISO+more) | National | ISO 27001 + extras | Annual, in-depth | • https://blog.avangarde-consulting.com/secnumcloud<br>• https://www.bpifrance.fr/nos-appels-a-projets-concours/guichet-dacces-au-dispositif-daccompagnement-a-la-qualification-secnumcloud<br>• https://cyber.gouv.fr/ |
| C5 (Cloud Computing Compliance Criteria Catalogue) *Germany* | Auditing framework for cloud services | Medium-High | BSI (based on ISO/IEC 27001) | National | ISO 27001 | Annual, risk-based | • https://www.chino.io/post/c5-certification-digital-health-compliance-guide?utm<br>• https://simpliant.eu/insights/neues-digital-gesetz-pflicht-zu-c5-testierung-fuer-saas-anbieter-im-gesundheitswesen<br>• https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf?__blob=publicationFile&v=3 |
| Esquema Nacional de Seguridad *Spain* | Qualification of cloud services for PA | Basic to High | ENS (Royal Decree) | National | ENS + ISO 27001 | Annual or periodic (per level) | • https://www.audidat.com/blog/esquema-nacional-de-seguridad/certificacion-ens-precio/<br>• https://doiser.com/que-precio-tiene-la-certificacion-del-esquema-nacional-de-seguridad |
| Italian AGID Qualification *Italy* | Qualification of cloud services for PA | Entry to Mid | AGID controls, partly ISO-based | National | ISO 27001 (partly) | Entry-level + documentation | • https://consulenza.isgroup.it/kb/migliori-normative-acn-agid-italia-2025/?utm_source=chatgpt.com<br>• https://www.acn.gov.it/portale/cloud/qualificazione-e-adeguamento |

## 4.3. Options related to simplification

### 4.3.1. *Average cost of compliance with NIS2 (adjustment and administrative costs)*

Article 21(2) of the NIS 2 Directive requires essential and important entities to implement cybersecurity risk-management measures.

Organizations typically spend between 1 000 and 4 999 hours per year on proving compliance with such requirements (Source: https://drata.com/blog/introducing-2023-compliance-trends-report). In terms of staffing, this range corresponds to roughly 0.56 to 2.78 FTE employees (assuming 1 800 working hours per FTE per year). Using an average fully loaded FTE cost of 56 500 per year (see above), this equates to an internal compliance demonstration cost ranging from approximately EUR 31.640 to EUR 157.070 annually per organisation. Taking the midpoint – around 3 000 hours or 1.67 FTE – the estimated average cost is about **EUR 94 355 per year**. This estimate includes administrative and adjustment costs. The assumption is taken that 10% of these costs would stem from administrative costs.

### 4.3.2. *Calculations for the number of entities impacted by scope changes*

The calculations are made under the assumption that there are 188 000 entities in the scope of NIS2.

The clarification of the NIS2 scope would reduce it by approximately 6.200 DNS service providers. Moreover, by providing clarification on definitions and the types of entities referred to in Annex I and II, the NIS2 Directive would no longer apply to an estimated number of 22.500 entities. This estimation is based on an extrapolation of the number of essential and important entities that 6 Member States notified to the Commission of pursuant to their obligation under Article 3(5) of the NIS 2 Directive so far. Therefore, following the clarification and reduction of NIS2 scope, the Directive would apply to 28 700 fewer entities, bringing down the NIS2 scope to 159 700 NIS2 entities.

### 4.3.3. *Cost savings under C2*

With respect to the **scope clarification and reduction,** if 28 700 companies are no longer required to comply with the NIS2 requirements, reducing their average costs of EUR 94355 per year, this amounts to EUR 2.7 billion annual savings considering all compliance costs.

Regarding the **introduction of the SMC category**, the following calculations have been applied. Based on SMC Omnibus data, there are approximately 38.000 small mid-cap (SMC) companies in the EU—defined as having 250–749 employees and up to EUR150 million in turnover or EUR 129 million in assets (see SWD(2025) 501 final). A sector-by-sector mapping against the 18 sectors covered by the NIS 2 Directive suggests that around 16.000 of these SMCs (approximately 42%) are likely to fall within its scope. This includes sectors such as energy, transport, digital infrastructure, healthcare, food production, chemicals, and key manufacturing sub-sectors. The estimate reflects companies operating in fully or predominantly covered sectors and may vary slightly depending on national implementation and company-specific activities.

An extrapolation of the number of essential entities that six Member States have notified the Commission of pursuant to Article 3(5) of the NIS 2 Directive thus far suggests that there will be around 51.000 essential entities in the Union. Based on the JRC study (https://op.europa.eu/en/publication-detail/-/publication/7860ea6e-f003-11ef-981b-01aa75ed71a1/language-en ) according to which enterprises with more than 250 employees are composed of 57% SMC defined as 250 to 499 employees, and that the simplification package defines SMCs as 250-749 employees (that is enlarging the notion of SMC), the number of essential entities that would be designated as important introducing the small-mid cap category in NIS2 would be more than 57% of 51.000, i.e. 29.070. Therefore, taking the midpoint of these two approaches, it is estimated that around 20.000 entities would be considered SMCs.

The NIS2 Directive distinguishes between the categories of important and essential entities, whereas as a rule, large-size entities from the Annex I sectors are considered as essential and medium-sized and smaller entities from Annex I as well as all entities from Annex II are considered important. Important and essential entities are subject to different supervision and enforcement regimes (essential are supervised ex ante and ex post, whereas important – only ex post). Therefore, the number of essential entities would likely bring cost savings (administrative costs savings) for both the entities that become important (less compliance documentation) as well as for the Member States that would reduce their supervisory costs (enforcement cost savings).

The estimated reduction for entities is 22 500 entities times 10% of EUR 94 355, amounting to a total of over EUR 212 million.

For Member States one FTE less per year with an average salary of EUR 56 500 times 27 Member States, amounts to savings of EUR 1 525 500 million per year.

With respect to savings linked to the use of a certification scheme to prove compliance with NIS2 requirements, the methodology of the calculations is as follows:
The average costs for a security audit is explained under the previous section (30 000 EUR). Under NIS2, if an entity needs to be compliant in two Member States and assuming one audit per year, this would amount to 60 000 EUR. Hence, the cyber posture scheme could reduce the audit cost by half.

#### 4.3.4. *Estimates related to adjustment costs for option C3*

According to available estimations, 22 000 entities are in scope of the DORA Regulation (see: https://www.pwc.com/mt/en/services/pwc-digital-services/cyber-security-and-privacy/cyber-security-services/dora.html). Therefore, in the case of Option C.3, if all NIS2 and DORA entities (159 700 + 22 000=181 700 in total) are to bear one-off adjustment costs of 0.5 FTE (taken 56.000/2= 28 250), this would amount to a total one-off cost of EUR 5.2 billion.

The costs for Member states training of staff are calculated as an approximate EUR 600 training cost multiplied by average of 10 staff per Member States, times 27 Member States

(EUR 162 000 in total). While no training courses for such a codified framework currently exists, trainings and NIS2-specific accreditations exist. For example, a training and accreditation to become a NIS accredited expert costs EUR 590 in Austria (https://www.incite.at/de/unser-programm/accredited-nis-expert/). A training to become NIS2 Directive Lead Implementer in Belgium costs EUR 720 (https://www.practics.be/opleidingen/nis-2-directive-lead-implementer/). Based on these existing courses, it was estimated that trainings could cost EUR 600. https://www.practics.be/opleidingen/nis-2-directive-lead-implementer/).

#### 4.3.5. *Estimates for cost savings under option C.3*

The 159 300 NIS2 entities following the scope reduction would save 0.5 FTE annually (EUR 28 250) from compliance due to streamlining and removing regulatory obligations. This would amount to EUR 4.5 billion annual savings only for the NIS2 entities.

Member States would benefit by requiring 2 FTE less per Member State (2x EUR 56 500 annual salary x27 = over EUR 3 million saving per year.

### 4.4. Options related to ICT supply chain

#### 4.4.1. *Cost estimation for replacing high-risk equipment under D2/3*

Estimations of costs for replacing the 5G equipment from high-risk suppliers in the EU were derived by taking into account the investments that were made in the EU for 5G non-standalone and standalone deployment since 2019 and until the measures would come into place in 2028. The data is provided by the 5G Observatory[208]. The estimations assume that the replacement of 5G equipment from high-risk suppliers will need to be done by mobile network operators for a period over three years starting in 2028 (1st January 2028 to 31st December 2030).

To aggregate the total value of equipment that would be affected by the restrictions, the observation is made, that according to the 5G Observatory, Member States started to deploy 5G around 2019 for non-standalone 5G (RAN on the top of 4G core). Deployment for 5G as standalone (both RAN and Core are 5G) on average took off from 2023 onwards. Furthermore in 2024, investments in 5G RAN reached EUR 5.3 bn[209], and in 5G core network EUR 0.9 bn[210], totalling EUR 6.2 bn.

Considering the deployment scenarios, it is assumed that between **2019 and 2022**, only 5G RAN investment have been done, while between **2023 and 2027**, both 5G RAN and core investments have been done. Given that no data is available for the years before, for 5G RAN and core, it is assumed that the same amount as in 2024 has been invested on an annual basis

---

208 https://digital-strategy.ec.europa.eu/en/policies/5g-observatory ; see in particular *5G Observatory indicators data – as of 2024*, available at : https://ec.europa.eu/newsroom/dae/redirection/document/120289

209 EU27 5G RAN Network Investment in 2024, *5G Observatory indicators data – as of 2024*

210 EU27 5G Core Network Investment in 2024, Ibid.

for the years before. This is an overestimation given that investments in 5G are typically increasing over time.

The share of equipment from high-risk suppliers across Member States can be estimated between 40%[211] and 32%[212] based on the estimated found in secondary sources. This is also corroborated by trade data (as indicated in the table below).

To calculate the costs of replacement of 5G equipment from high-risk suppliers, we consider that the (estimated) market share of high-risk suppliers has slowly decreased following the adoption of the 5G toolbox in 2020 and its gradual implementation: it is estimated as 40% for initial phase (**2019-2022**) and then decrease to 32% (**2023-2027**). These shares are applied to the estimated yearly investments from 2019 to 2027.

2019 – 2022: 0.4 x 5.3 bn = 2.12 bn * 4 years = EUR 8.5 bn

2023 – 2027: 0.32 x 6.25 bn = 2 bn * 5 years = EUR 10 bn

Total 2019 – 2027 = 8.5 bn + 10 bn = 18.5 bn EUR is the total value of high-risk equipment to be phased out.

**Business as usual (BaU) factor**: looking at the three year transition period, it can be reasonably assumed that from **2028 to 2030**, 30 to 45 % of the equipment would have to be replaced over a period of three years, if the assumption is taken that the 10 to 15% of the equipment invested since 2019 would need to be replaced on yearly basis.

The value of the BaU (equipment that would be replaced without intervention) ranges from EUR 1.9 bn to EUR 2.8 bn per year, calculating respectively 15 % and 10% of the yearly value of high-risk equipment. The yearly value of the high-risk equipment is equal to the total value of high-risk equipment invested in the past years (2019 to 2027) divided by the number of transition years (3 years) leading to 6.2 bn EUR (without BaU).

Hence, per year the value of high-risk vendor equipment to be replaced would be equal to **EUR 3.4 bn - EUR 4.3 bn** (for three years) considering the BaU. These costs would be carried either by operator or transferred to subscribers resulting in higher prices (see next section).

**Following assumptions** are taken for the calculations:

Regarding the calculated cost for operators : data from EU investment in 5G for 2024 are likely higher than what was actually invested in prior years. At the same time, it is assumed that prices of new equipment from other 'trusted' suppliers replacing high-risk suppliers remain the same. In reality, prices may differ due to market circumstances and technological developments. Additional costs for operators might occur e.g. install equipment, train personnel, ensure interoperability within the network, as well as costs relating to the decommissioning of old equipment.

---

[211] Strand Consult, The Market for 5G RAN in Europe: Share of Chinese and non-Chinese vendors in 31 European countries, May 2023.
[212] source: https://www.lightreading.com/5g/huawei-has-hardly-been-weakened-in-european-5g-data-shows;

The market share for high-risk suppliers may be subject to change. Whereas Strand Consult estimated the market share 40% in 2015, a more recent prediction pointed to 32% relative market share. The decline in market share is also supported by trade statistics for EU import from China for mobile equipment (see table below).

The market share for high-risk suppliers and resulting replacement costs are calculated on an EU average basis. In reality, these shares and costs will differ between EU Member States.

Regarding the normal course of replacement of equipment ('business as usual'), mobile operators typically work with **replacement cycles for their equipment of 7-10 years**, taking into account amongst other things technology cycles with new standards (3G, 4G, 5G) becoming available. On that basis, it can be assumed that about **10-15% of equipment will be replaced on a yearly basis**, i.e. about 30% to 45% of equipment will be replaced in the normal course of business over the 3-year transition period, and 100% of equipment will already have been replaced in the normal course of business over 10 years.

#### 4.4.2. *Transfer of costs: Potential Price increase for EU citizens*

The mobile network operator might decide to transfer the costs to the consumers. According to GSMA ([213]), there were 520 million mobile subscribers in 2025. Taken the estimated cost of replacement at EUR 3.4 bn - EUR 4.3 bn per year over 3 years, this would amount to EUR 6.5 to EUR 8.3 per mobile subscriber per year over three years.

#### 4.4.3. *Revenue gains for trusted suppliers*

According to the 5G observatory indicators data, there are about EUR 18 bn investments in mobile network equipment in 2024, of which about 48% is invested in 5G equipment, which leads to EUR 8,6 bn of total 5G investment in Europe in 2024. More granular assessment based on the data from the 5G Observatory, to focus on the key assets that would be considered on 5G as presented above:

- Investments per year on 5G RAN: EUR 5.3 bn
- Investments per year on 5G 5G core network: EUR 0.9 bn

This leads to a total of EUR 6.25 bn of yearly investments in 5G RAN and core network in Europe based on data from 2024. The assumption is taken that 32 %[214] of these investments currently goes to equipment from high-risk suppliers (Huawei/ZTE). This share would likely gradually decrease through the implementation of the measures to restrict equipment from high-risk suppliers in key assets.

According to 2023 STRAND Consultancy figures quoted in secondary sources, equipment stemming from Chinese equipment is around 32%. Strand Consult predicts that, under current market conditions, they will still have a meaningful share of 5G networks toward the end of

---

[213] GSMA, the mobile economy Europe 2025.

[214] source: https://www.lightreading.com/5g/huawei-has-hardly-been-weakened-in-european-5g-data-shows; see also: https://www.lightreading.com/5g/huawei-defies-us-to-grow-market-share-as-ran-decline-ends-omdia

the decade. The same calculation described in the previous paragraph produces a figure of about 29% for 2028. This assumption of a decline in market share can be supported by the general trend visible in statistical data representing EU import from China of telecommunications equipment, including 5G equipment, which shows a considerable and steady decline of about 30-40% from 2022 to 2024 which may be the result of the adoption of the EU 5G Toolbox. However, for our calculations we keep the estimation that the market share is 32% as in 2024.This would lead to a total value of investments **per year going to high-risk suppliers' equipment of** EUR 6.25 * 32% = **EUR 2 bn per year**. Under the impact of the measures adopted, operators would need to replace equipment amounting to this value with equipment from other, trusted, providers. This investment would feed back into the wider economy, while transaction and substitution costs can be expected from changing suppliers (as indicated above).

The assumptions is that the investments would continue the same pace. This considers the drive for European operators to upgrade their infrastructure if they want to rollout 5G. GSMA report shows that Europe is lagging with only 30% of 5G connections compared to the rest of the world.

**EU27 Trade import from China**

The Harmonized System (HS) Code for 5G Radio Access Network (RAN) components isn't a single code but varies based on the specific equipment, with common codes including 8517.69 for other apparatus for the transmission or reception of voice, images, or other data and 8517.61 for base stations and other telecommunication equipment, as 5G RAN falls under the broader category of telecommunications equipment.

The Harmonized System (HS) Code for an Evolved Packet Core (EPC) is typically 85176290, which covers telecommunication equipment, including devices for network and packet transmission.

*Table 16: Decrease in imports from China from 2020 to 2024.*

| | **851769**<br>-<br>**apparatus for the transmission or reception of voice, images or other data, incl. apparatus for communication in a wired or wireless network [such as a local or wide area network] (excl. telephone sets, telephones for cellular networks or for other wireless networks, base stations, apparatus for the reception, conversion and transmission or regeneration of voice, images or other data, and transmission or reception apparatus of heading 8443, 8525, 8527 or 8528)** | **851761**<br>-<br>**base stations of apparatus for the transmission or reception of voice, images or other data** | **851762**<br>-<br>**machines for the reception, conversion and transmission or regeneration of voice, images or other data, incl. switching and routing apparatus (excl. telephone sets, telephones for cellular networks or for other wireless networks)** |
|---|---|---|---|
| 2020 | 570 982 | 101 071 | 15 651 992 |
| 2021 | 589 006 | 214 897 | 16 127 974 |
| 2022 | 771 210 | 219 651 | 18 025 455 |
| 2023 | 577 615 | 200 374 | 14 938 139 |
| 2024 | 609 043 | 114 293 | 12 141 236 |

Values in 1000 EUR
Source: ESTAT Comext

# ANNEX 5: COMPETITIVENESS CHECK

## 1. OVERVIEW OF IMPACTS ON COMPETITIVENESS

*Table 17: Overview of impacts on competitiveness*

| Dimensions of Competitiveness | Impact of the initiative (++ / + / 0 / - / -- / n.a.) | References to sub-sections of the main report or annexes |
|---|---|---|
| Cost and price competitiveness | 0 | Section 6 of the main report |
| International competitiveness | + | Section 6 of the main report |
| Capacity to innovate | 0 | Section 6 of the main report |
| SME competitiveness | + | Section 6 of the main report and Annex 6 |

## 2. SYNTHETIC ASSESSMENT

In summary, the preferred option exhibits the following impacts on EU business competitiveness:

- In terms of cost and price competitiveness the initiative is expected to have a neutral impact, indicating that significant changes in compliance or operational costs are not anticipated.
- When it comes to the impact on international competitiveness and trade, the proposed changes are expected to enhance EU businesses' global competitiveness, reducing financial losses and improving operational stability in case of crises. New mutual recognition agreements could facilitate cross-border trade, while new market dynamics in certification strengthen the international standing of EU Conformity Assessment Bodies (CABs), improving market access.
- In relation to the capacity to innovate, the initiative does not seem to influence the innovation dynamics directly, maintaining a neutral effect on research, development, and technological progress.
- In terms of SME competitiveness there are multiple aspects that could directly or indirectly generate a positive impact on SMEs. These are related to improved cybersecurity certification and cybersecurity skills attestation as well as changes to considerably simplify and streamline the current framework. All of this would enhance the competitive positioning of SMEs, in the context of an overall strengthened cybersecurity support from ENISA also in terms of awareness raising, incidents response and implementation of cybersecurity measures.

The preferred option could potentially favour the enhancement of the competitiveness landscape for SMEs and other economic operators throughout the EU, particularly by amplifying efficiency and operational coherence. Among the anticipated improvements is the simplification of compliance with cybersecurity requirements, a change that would reduce compliance costs for SMEs and public authorities by diminishing administrative overhead.

This administrative streamlining may lead to immediate cost savings, allowing resources to be redirected towards innovation and market expansion initiatives. Additionally, the simplification of certification procedures is expected to offer advantages to businesses and certification bodies, as the ECCF reforms under option B.2 look to provide consistent and harmonised level of cybersecurity through certification across Member States, which could lighten the associated compliance and administrative burden.

Furthermore, improving legal clarity and targeted guidance could be a critical benefit, couple with ENISA's expanded and more focused mandate can contribute to reducing uncertainties and providing harmonised technical instructions that would be advantageous for national authorities and economic operators. These strategic enhancements could foster smoother operational cooperation on cybersecurity and related data flows across the EU, potentially strengthening the capabilities of national authorities and economic operators and facilitating new opportunities for public and private collaboration and service provision across borders.

Coupled with an increased uptake of certification, these measures are anticipated to boost market confidence by establishing clearer legal frameworks. This could reduce uncertainties and encourage voluntary adherence from SMEs and economic operators, nurturing a culture of trust and reliability in digital exchanges. Additionally, the enhanced agility of the ECCF in responding to market needs is expected to positively impact this development. The long-term efficiency gains anticipated as a result of these changes could include decreased reliance on external legal consultants and strengthened internal administrative capacities, enabling businesses to focus more on their core activities and strategic development. In essence, the proposed market intervention, particularly through harmonised certification and reporting frameworks, could dismantle barriers and facilitate seamless access to emerging markets, potentially enriching the EU market and contributing to the competitive positioning of EU businesses globally. Enhanced trust in digital services, fostered by improved certification uptake and streamlined incident reporting requirements, might spur increased consumer and business confidence, encouraging greater digital service adoption. Ultimately, the alignment with EU policy goals, including the "green oath" and REFIT principles, suggests a dedication to sustainable, simplified, and future-ready regulatory measures that may bolster economic resilience and competitiveness.

Focusing on cost and price competitiveness in particular, the proposed measures present potential benefits and challenges for businesses. Compliance costs, notably in the realm of cybersecurity requirements, may show favourable impacts, while other areas - such as the costs associated with inputs, capital, labour, production, distribution, and after-sales services - appear less impacted, suggesting neutral outcomes. Streamlined certification procedures promise reduced administrative burdens; however, they also raise the prospect of increased compliance costs, especially if stringent requirements are enforced. The competitive environment among suppliers and producers could be influenced by these developments, although current assessments indicate minimal disruption to their ability to set prices or freely advertise. The manner in which certification schemes are applied may advantage those who fulfil them, thereby affecting relative production costs across different entities. Additionally, simplifying reporting and oversight processes, facilitated by centralised databases, might lower long-term administrative expenses, thereby enhancing operational coherence and efficiency for entities navigating the regulatory environment. While these factors hold the potential to improve efficiencies in certain sectors, adapting to intensified competition and

managing the costs associated with transitioning to new systems present financial challenges, particularly for SMEs. Thus, while cost and price competitiveness offer pathways to potential savings and efficiency gains, the broader impact remains reliant on the implementation of the proposed intervention across the market. Additionally, in the area of skills, the development of European individual attestation schemes would lead to increased visibility and recognition of European economic operators authorised to deliver such attestations in a market which is currently dominated by non-European providers while not excluding the latter, thereby ensuring fair competition amongst providers. Concerning the international competitiveness and impact on international trade resulting from changes introduced by the preferred option, there is the possibility of increase in European companies' market share, as certified products or services will likely increase their overall level of cybersecurity and resilience in case of international crises, and are thus likely to gain stronger international appeal. The development of mutual recognition agreements under new certification schemes could facilitate international trade, dampen disruptions and potentially even increasing EU exports. The EU's leadership in product certification and advances in services and process certification could further enhance the stature of EU-based Conformity Assessment Bodies resulting in new market dynamic and opportunities for EU companies. However, active monitoring of international market dynamics through risk assessments and market analyses remains crucial as these changes are implemented. Whilst the overall high-tech import and export for the EU remains balanced, this may evolve over time and be different for specific sectors and / or products or services.[215]

The capacity to innovate within the cybersecurity landscape, within the preferred option, appears to maintain a neutral trajectory. The proposed measures do not seem to directly influence innovation dynamics, preserving the status quo in terms of research, development, and technological progress. The assessment is that the immediate capacity for innovation would remain unchanged as compliance adjustments do not directly impact the core innovation processes such as product or process innovation, nor do they significantly alter the pathways for accessing risk capital within the sector.

In terms of competitiveness of SMEs, the proposed measures could significantly reduce compliance costs and streamline processes, allowing SMEs to reallocate precious resources from navigating intricate legal requirements to fuelling business growth and innovation. This reduction in administrative strain empowers SMEs to focus on their core activities, unlocking potential for expansion within and beyond Europe's borders. The emphasis on harmonisation of certification practices paves the way for greater cross-border interoperability, enabling SMEs to engage more readily in the European market whilst seizing new business prospects also in the global market. Enhanced legal clarity bolster SMEs' resilience against cybersecurity threats, safeguarding their operational continuity and reinforcing their credibility.

### 3. COMPETITIVE POSITION OF THE MOST AFFECTED SECTORS

The proposed measures as part of the preferred option are predominantly cross-sectoral, meaning they do not single out specific industries for direct impact. However, sectors

[215] Eurostat, *EU high-tech trade: exports up in 2023*, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20241004-1.

identified as highly critical or critical under the NIS 2 Directive, such as healthcare, digital infrastructure, ICT service management, digital providers or manufacturing as well as sectors historically relying strongly on ICT solutions may experience stronger influence. These sectors, being integral to the operational infrastructure and in some case to public welfare, stand to benefit from enhanced security measures and better alignment with certification standards. Such enhancements foster a more secure and reliable digital environment, potentially improving the competitive position of these sectors. Overall, the proposed measures aim to eliminate some of the sector-specific compliance hurdles and facilitate reporting and certification across sectors and therefore no specific impact on competitiveness in specific sectors can be identified in relation to the preferred option.

# ANNEX 6: SME CHECK

**OVERVIEW OF IMPACTS ON SMES**

| **Relevance for SMEs** |
|---|
| This initiative is relevant to highly relevant for SMEs[1]. The revised EU Cybersecurity Act significantly impacts SMEs by establishing facilitating compliance, providing guidance, clarifying and reducing scope of NIS2 Directive and streamlining incident reporting mechanisms and development of certification schemes. In a digital business environment, cybersecurity is crucial for SMEs, particularly in vulnerable sectors like technology, healthcare, and e-commerce. SMEs must uphold cybersecurity throughout their product lifecycle, often relying on external solutions. Cybersecurity certification, while mainly voluntary, is essential for cross-border operations, scalability of business solutions and access to certain national or sectoral markets. SMEs, with fewer resources than larger companies, need streamlined requirements and simplified compliance to protect their systems effectively and reduce their legal exposure. Improving certification processes and reducing reporting requirements can enhance cybersecurity and lower compliance costs for SMEs. |

| **(1) IDENTIFICATION OF AFFECTED BUSINESSES AND ASSESSMENT OF RELEVANCE** |
|---|
| **Are SMEs directly affected? In which sectors?** |
| SMEs are directly affected by the preferred policy option. The initiative, while cross-sectoral, is particularly relevant in sectors identified as highly critical, where SMEs are also active. The proposed actions aim to enhance certification and cybersecurity skills, streamline the cybersecurity obligations, and reduce compliance costs, thereby improving the competitive positioning of SMEs. The number of micro- and small-sized entities in scope of the NIS2 Directive as well as medium-sized entities subject to ex ante supervision under the NIS2 Directive will be reduced. By fostering a more secure digital environment through harmonised certification procedures and streamlined administrative processes, SMEs in these sectors are expected to benefit substantially. Improved legal clarity and centralised guidance could further bolster SMEs' resilience and operational coherence, thus strengthening their competitive stance within the EU Single Market and beyond. |
| **Estimated number of directly affected SMEs** |
| According to Eurostat (2022), the EU is home to approximately 1.2 million enterprises operating in directly relevant sectors such as ICT manufacturing and ICT services (according to NACE Rev. 2 activity). Since 99 % of all EU enterprises are micro and small enterprises[2] and 0.8 % are medium-sized enterprises, this implies that around 1.2 million SMEs could fall within the scope of the proposed policy options. The reduction of scope regarding the NIS2 Directive would affect 6.200 micro- and small-sized enterprises. |
| **Estimated number of employees in directly affected SMEs** |
| In terms of employment, SMEs are the backbone of the European economy. Micro and small enterprises (up to 49 employees) account for 48 % of all enterprise employment, while medium-sized enterprises (50–249 employees) account for 15 %. Applying these proportions |

| |
|---|
| to the ICT sector, we estimate that the preferred option could directly affect between 4 and 5 million workers employed by SMEs in the information and communication technology[216]. |
| **Are SMEs indirectly affected? In which sectors? What is the estimated number of indirectly affected SMEs and employees?** |
| Beyond the ICT realm, the anticipated solutions under the preferred policy option will have significant indirect effects on key EU sectors reliant on secure digital technologies, like smart manufacturing, healthcare, energy, transport and finance. This impact extends to the vast network of SMEs integrating, procuring, and distributing ICT products and services. Critical sectors such as manufacturing, retail trade, professional services, transportation, construction, and healthcare include around 6 to 7 million SMEs, employing approximately 36 million individuals who could be indirectly affected. The reduction of scope regarding the NIS2 Directive would affect 6.200 micro- and small-sized enterprises as DNS providers. |

| **(2) CONSULTATION OF SME STAKEHOLDERS** |
|---|
| **How has the input from the SME community been taken into consideration?** |
| A public consultation was launched from 11 April 2025 to 20 June 2025, also targeting SMEs. A share of 8.8% out of the total respondents identified themselves as SMEs, while the rest of respondents corresponded to large companies, academia, public authorities, business associations, trade unions and citizens. Focusing on business respondents, the share of SME respondents was 36.7 %, including micro enterprises (15.2 %), small enterprises (11.4 %) and medium sized enterprises (10.1 %).<br><br>Moreover, a call for evidence was launched from 11 April 2025 to 20 June 2025. The initiative was also presented and discussed at a dedicated session organised by the European DIGITAL SME Alliance on 17 June 2025. |
| **Are SMEs' views different from those of large businesses?** |
| SMEs' perspectives on cybersecurity differ significantly from those of larger businesses. SMEs often struggle with the administrative, financial burdens and legal exposure associated with cybersecurity compliance due to their limited resources and smaller compliance departments. While larger companies might adapt more readily to rigorous compliance measures, SMEs advocate for simplified certification processes and regulatory frameworks to reduce costs and foster innovation reducing costly compliance efforts. This was highlighted on one side by the European DIGITAL SME Alliance but it is also stemming from the results of the public consultation, where SMEs, in particular, underlined the need for more structured and transparent engagement mechanisms in the ECCF and warned against overregulation. |

| **(3) ASSESSMENT OF IMPACTS ON SMES[217]** |
|---|

[216] Eurostat, *NACE Rev. 2 activity*, https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-ra-07-015

| **What are the estimated direct costs for SMEs of the preferred policy option?** |
|---|
| The preferred policy option will result in direct costs for SMEs, which are categorised into one-off and recurrent expenses. SMEs might incur expenses for short-term resource reallocation to align with new reporting templates and procedures. Recurrent costs mostly encompass certificate management and continuous compliance. Initial (one-off) costs could also include, should SMEs choose to get certified, adapting internal procedures for certification compliance *(see Section 6.1 of the impact assessment)*. |
| **What are the estimated direct benefits/cost savings for SMEs of the preferred policy option[218]?** |
| The preferred policy option presents several estimated direct benefits and cost savings specifically for SMEs, with some applying broadly to all economic operators. First, the number of micro- and small-sized entities in scope of the NIS2 Directive will be reduced. Moreover, SMEs benefit from compliance cost reductions thanks to fewer legal interpretations, easier demonstration of compliance with supply chain and cybersecurity risk-management obligations, resulting in lower administrative expenses. This translates into higher efficiency, which contributes to reduced operational disruptions and potentially lowers associated costs. Improved legal clarity and simplified certification procedures, particularly the ECCF reform, further reduces administrative burdens, enhancing predictability and harmonisation across Member States. The increased uptake of certifications, driven by reinforced trust is expected to support cross-border business models. Furthermore, long-term efficiency gains are projected for SMEs as harmonised obligations lead to lower compliance costs over time, diminishing reliance on external consultants while strengthening internal capacities. The higher readability of cybersecurity roles thanks to the European Cybersecurity Skills Framework and industry-delivered individual certifications, which will lead to increased transparency on identifying relevant attestations and on better information on the cost of a European individual attestation, two reasons mentioned by companies as a reason for not providing cybersecurity training[219], will encourage SMEs to support employees in working towards such attestations. Whereas this will lead to direct immediate costs to support employees in their training, such immediate costs can be offset by longer employee retention and increased cybersecurity of SMEs thanks to trained staff, hence less costs in case of cybersecurity incidents. |
| **What are the indirect impacts of this initiative on SMEs?** |
| Positive impacts for economic operator, also pertinent to SMEs, include enhanced cross-border interoperability, which is facilitated by ENISA's expanded mandate, and also through standardised reporting practices. This leads to improved operations across the EU in terms of streamlined and more efficient business processes. In alignment to EU policy goals, enhanced trust in digital services and market integration, through harmonised certification frameworks can boost access to new markets, supporting SMEs both within the EU Single Market and globally. |

| **(4) MINIMISING NEGATIVE IMPACTS ON SMES** |
|---|

[217] The costs and benefits data in this annex are consistent with the data in annex 3. The preferred option includes the mitigating measures listed in section 4.
[218] The direct benefits for SMEs can also be cost savings.
[219] Eurobarometer (2024) on Cyberskills, https://europa.eu/eurobarometer/surveys/detail/3176.

| **Are SMEs disproportionately affected compared to large companies? If yes, are there any specific subgroups of SMEs more exposed than others?** |
|---|
| SMEs are not foreseen to be disproportionally subject to negative impacts, according to the measures proposed for the preferred options. |
| **Have mitigating measures been included in the preferred option/proposal?** (Yes/No) |
| Given the absence of specific negative impacts for SMEs, no mitigating measures have been included in the preferred option formulation. |

| **CONTRIBUTION TO THE 35% BURDEN REDUCTION TARGET FOR SMES** |
|---|
| **Are there any administrative cost savings relevant for the 35% burden reduction target for SMEs?** |
| Enhancing the cybersecurity framework supports the achievement of the 35 % burden reduction target for SMEs by streamlining certification processes and reducing administrative costs. Measures such as supply chain guidelines, organisational certification and harmonized obligations can considerably diminish the effort required for cybersecurity compliance. Reducing the number of micro- and small-sized enterprises in scope regarding the NIS2 Directive directly contributes to the 35% burden reduction target for SMEs. Moreover, as stronger involvement and support of ENISA in addressing cybersecurity incidents it is estimated to potentially reduce between 15% to 20% the cost of such incidents for affected entities. European individual attestation will further support talent retention and hiring practices by providing visibility of competences, quality assurance of candidates, and will indirectly lead to potential savings to prevent cybersecurity incident thanks to trained staff. Regarding certification, a stronger role of ENISA is estimated to potentially generate around 35% costs savings for each certification. Moreover, as a more indirect benefits, estimates suggest that companies (including SMEs) could benefit from cyber certification in terms of lower insurance premiums related to coverage of cyber incidents. Additionally, improved clarity, modularity, and streamlined certification processes benefit SMEs by easing compliance mechanism. These measures reduce reliance on external consultants and support SMEs across critical sectors, aligning with EU policy goals for a resilient digital economy. |

# ANNEX 7: MAGNITUDE AND COSTS OF CYBER INCIDENTS

To illustrate the political context, problem definition and economic impacts of the policy options explored in this impact assessment (sections 1, 2.1 and 6.1), this document presents **quantitative estimates related to direct and indirect costs of most common cybersecurity incidents** by threat type affecting businesses, public authorities and citizens in Europe (Part 1). Additionally, examples of cybersecurity incidents are provided to illustrate **societal and/or economic cross border impacts, with specific SMEs examples** (Part 2), followed by an illustrative overview of **cybersecurity problems chain reaction on real world problems** (quantified evidence of magnitude) (Part 3). A **mini-case study on real world effects** is presented (Part 4). The last table provides more granular **data on ransomware attacks**: financial, economic and human impacts, recovery and root causes across selected European countries (Part 5).

## 1. COSTS OF CYBER INCIDENTS

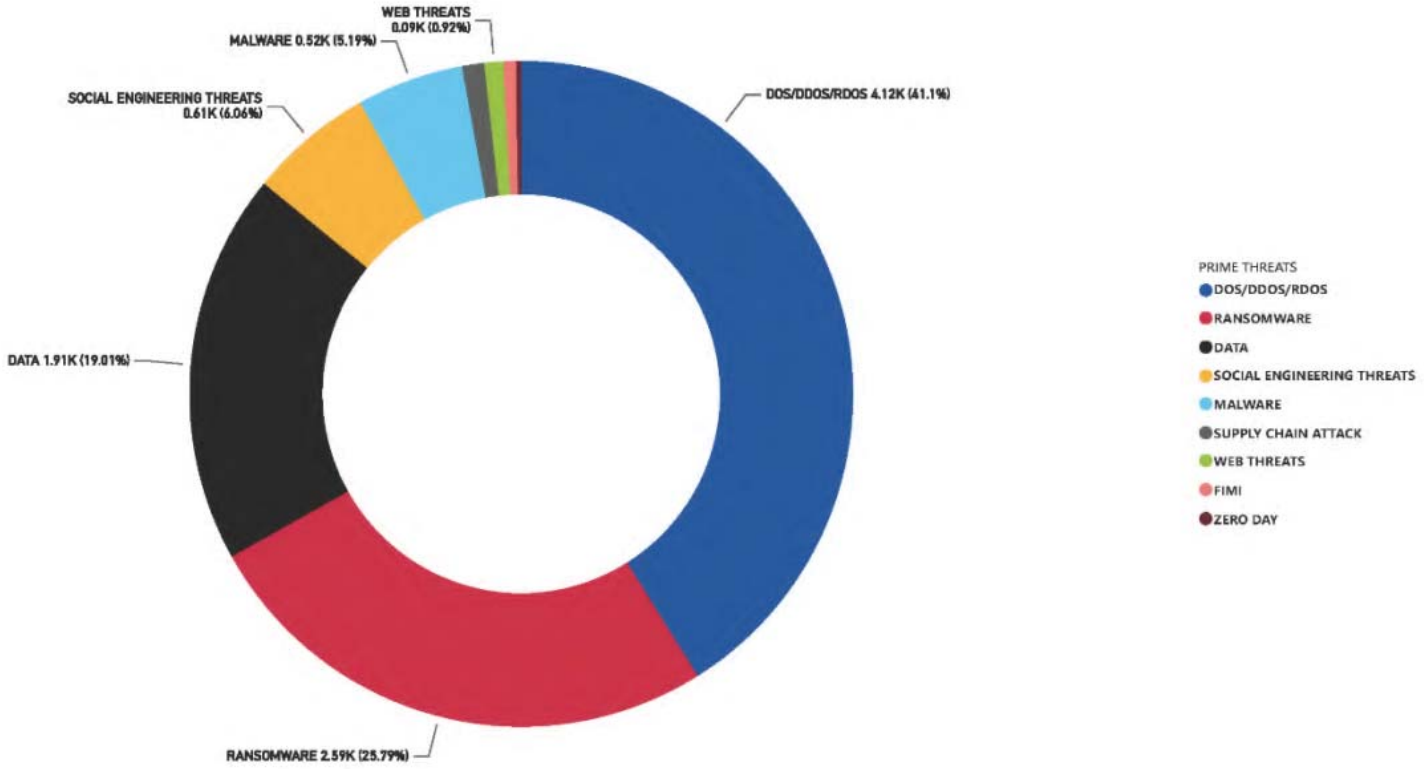


*Figure 12 Breakdown of incidents analysed by ENISA by threat type (July 2023-June 2024)*[220]

Building on available and reliable data sources (see section 1 below), **aggregated quantitative estimates of costs** of two of the most common incidents by threat type in the European Union, namely ransomware[221] attacks (25.79% of incidents) and data breaches[222] (19.01%), are further analysed (see figure 12). While distributed denial of services (DDoS) is the most frequent threat type (41.1%), no reliable aggregated estimates can be provided. Additionally, where relevant and available, information related to supply chain attacks, considered by ENISA as threat on a horizontal level touching multiple of other threats[223], was further included.

To the extent possible, the document provides granularity on various types of incidents (malicious vs. non-malicious), their **distribution** and **different costs for different types of stakeholders**. The document also includes examples to illustrate **direct and indirect (societal and economic) costs of cyber incidents** for which no aggregated estimates are available and that show the full magnitude of cyber incidents, including for SMEs.

The impact assessment (section 6.1) explains how the policy measures are likely to affect the costs related to cybersecurity incidents presented in this document. This Annex is complementary to *Annex 4* on the Methodological approach.

## 1. Methodological approach

### 1.1. Data limitations

As identified in other jurisdictions[224], **the costs of adversarial cyber activity are difficult to estimate in a reliable fashion in the absence of common and mandatory reporting mechanism** due to a series of factors which should be taken into consideration when exploring the said data:

---

[220] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[221] Ibid. Ransomware: a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability or in exchange for publicly exposing the target's data.

[222] Ibid. The definitions provided by ENISA allow to differentiate between malicious and non-malicious intent. The impact assessment report only refers to data breaches as defined by ENISA: ***"Data breach**: an intentional cyber-attack executed by a cybercriminal to gain unauthorised access to release sensitive, confidential or protected data. In other words, a data breach is a deliberate and forceful attack against a system or organisation to steal data. **Data leak**: an event (e.g. due to misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data. It does not consider intentional attacks and is sometimes called data exposure."*

[223] Ibid.

[224] CISA (U.S. Cybersecurity and Infrastructure Security Agency) (2021). Cost of Cyber Incidents Study, https://www.cisa.gov/sites/default/files/publications/CISA_OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf Cost of Cyber Incidents Study, https://www.cisa.gov/sites/default/files/publications/CISAOCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

- The **sensitive nature of cybersecurity incidents (underreporting)**: Economic actors often exhibit significant reluctance in disclosing the specifics and costs associated with such events. This reluctance stems from concerns over reputational damage, potential legal liabilities, and competitive disadvantages. Any available data or estimations must be viewed with these limitations in mind, recognizing that they may not fully capture the scope or scale of the potential impacts. Additionally, not all cybersecurity incidents are reported.
- **Overlaps between different types of threats (complexity of the cyberspace)**: An incident can be caused by different types of cybersecurity threats, leading to challenges in assessing the root cause of the damages. For instance, one of the techniques in ransomware is to encrypt data and ask a ransom to decrypt them. If the ransom is not paid, the data will be leaked, leading to a data breach.
- **Challenges related to cost quantification of cyber incidents (lack of sufficient data on costs and losses):** The unpredictable nature of the aftermath of significant cybersecurity disruptions makes it exceedingly difficult to quantify material and human costs in advance. While economic analyses can provide estimates of direct costs, the broader societal impacts — including potential loss of life linked to outages in critical infrastructure — are not easily quantifiable. These assessments are typically performed retrospectively. Extrapolating from a single incident would not lead to reliable data, the impacts of incidents differing widely depending on factors such as the type of attack, sector, supply chain dependencies, geographical dimension...
- **Comparability (lack of common reporting mechanism)**: While data from incidents occurring in the US are more easily accessible and reliable due to reporting mechanisms[225], such data cannot systematically be compared or used with the European market. For instance, cybersecurity incidents insurance models in the US and in Europe can hardly be compared. Hence, such comparisons or figures cannot be used nor considered reliable for comparison. Reporting across European countries may also vary. For the purpose of this impact assessment and in the absence of a unified reporting system, it is considered that the data can be compared.

The reliability of information presented in this document is further outlined in the following section.

### 1.2. Data sources for cost aggregation

Data presented are extracted from two different sources: IBM Cost of a Data Breach Report 2025[226] and 2024[227]; and Sophos "State of Ransomware" reports for 2025[228] (covering

[225] See for instance the federal Bureau of Investigation's Internet Crime Complaint Centre (IC3), https://www.ic3.gov/.
[226] IBM, Cost of a data breach report 2025, https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91; IBM, *Cost of data breach: financial industry 2024*, https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry.
[227] IBM, Cost of a data breach report 2025, https://www.ibm.com/reports/data-breach.
[228] Sophos, *The State of ransomware 2025*, https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2025.pdf;

globally and also on specific countries: Spain, France, Germany, Italy, Switzerland and the UK).

*About the IBM Cost of Data Breach Reports*

IBM reports are based on research that studied 600 organizations impacted by data breaches across 16 countries and regions, in partnership with the Ponemon Institute, which quantifies the financial impact and trends associated with data security incidents globally. IBM study is worldwide, and it includes specific European countries and regions (Belgium, the Netherlands, and Luxembourg together (Benelux), Germany, France, Italy and the UK).

The data breaches examined ranged in size **between 2,960 and 113,620 compromised records**. It excludes very small and very large breaches. Researchers collected in-depth qualitative data through **3,470 separate interviews**. Interviewees included CEOs, CISOs, heads of operations, controllers, IT practitioners, and risk management specialists.

Costs include **direct expenses** (engaging forensic experts, outsourcing hotline support, and providing free credit monitoring or product discounts) and **indirect costs** (in-house investigations and communications, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates).

*About Sophos report on "State of Ransomware"*

Sophos reports are based on an independent, vendor-agnostic **survey of 3,400 IT/cybersecurity leaders** who work in organizations that were affected by **ransomware** in 2025. All respondents work in organizations that employ **between 100 and 5,000 employees**.

Reports on specific countries are based on a survey of:

- Germany: 300 IT/cybersecurity leaders were surveyed
- Italy: 254 IT/cybersecurity leaders were surveyed
- Spain: 237 IT/cybersecurity leaders were surveyed
- UK: 201 IT/cybersecurity leaders were surveyed
- France: 185 IT/cybersecurity leaders were surveyed
- Switzerland: 74 IT/cybersecurity leaders were surveyed

### 2. Malicious vs. non-malicious intent of incidents and attack vectors

When analysing incidents, one consideration is whether these have been originated by malicious or non-malicious activities. In the IBM reports, "data breach" is used to cover all threats against data[229]. **Regarding data breaches, 51% of the incidents can be attributed to malicious activities[230]**; 26% attributed to human error and 23% to IT failures[231]. Hereafter,

---

Sophos, *State of ransomware – country reports*, https://www.sophos.com/en-us/content/state-of-ransomware#country-reports

[229] ENISA makes a distinction between "Data breach" and "Data leaks", see section 1 of this Annex.

[230] "Data breach" in ENISA terminology, see section 1 of this Annex.

[231] "Data leak" in ENISA terminology, see section 1 of this Annex.

the expression “data breach” will be used to cover threats against data resulting from malicious activity only, as understood by ENISA.

**Malicious activities** are those actions that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon[232]. These activities can be executed different initial attack vectors such as phishing campaigns, vulnerability exploitation, supply chain compromise (see table below).

**Non-malicious activities** are those without hostile intent, but that can still have serious consequences. They cover **human errors** (caused by accidental errors made by individuals while performing their regular responsibilities), **structural failures** (hardware, software, or support systems, such as environmental controls fail (e.g., air conditioning)**, and natural disasters**[233].

*Table 18: Overview of average cost of breach and prevalence by initial attack vector*

| Initial Attack Vector | Average Cost of Breach (USD millions) | Prevalence (% of all breaches) |
|---|---|---|
| **Malicious insider** | 4.92 | 7% |
| **Third-party vendor and supply chain compromise** | 4.91 | 15% (second most prevalent) |
| **Phishing** | 4.80 | 16% (most frequent) |
| **Compromised credentials** | 4.67 | 13% |
| **Denial-of-service attacks** | 4.41 | 7% |
| **Vulnerability exploitation** | 4.24 | 11% |
| **Physical theft or security issue** | 4.07 | 8% |
| **Insider error** | 3.62 | 14% |
| **System error** | 3.61 | 9% |
| **Total** | 4.44 | |

[232] NIST, *Computer Security Resource Centre Glossary*, malicious cyber activity - Glossary | CSRC. ENISA does not offer a single, formal definition of "malicious activity" but describes it through threat types and behaviours that compromise cybersecurity and are reflected in the NIST definition.
[233] FEMA, *Planning Considerations for Cyber Incidents*, https://www.fema.gov/sites/default/files/documents/fema_planning-considerations-cyber-incidents_2023.pdf.

In the case of attacks using **third-party vendor and supply chain** as their initial vector, the average breach cost rises to **USD 4.91 million**. Apart from the costs associated, this type of attacks is difficult to detect because it exploits trust between vendors and customers, and consequently, they took the longest combined time to detect and contain among the initial attack vectors studied, at **267 days**.

## 3. Overview costs for main types of incidents in Europe and globally

Aggregated estimates are provided for data breaches and ransomware attacks.

### 3.1 Data Breach

Average cost in 2025 (globally): **USD 4.44 million** (costs include detection, notification, post breach response and lost business).

*Table 19: Average cost of data breach by countries/regions in 2024-2025*

| Country/Region | 2025 Average Cost (USD) | 2024 Average Cost (USD) |
|---|---|---|
| Benelux | 6.24 million | 5.90 million |
| United Kingdom | 4.14 million | 4.53 million |
| Germany | 4.03 million | 5.31 million |
| France | 3.73 million | 4.17 million |
| Italy | 3.44 million | 4.73 million |

### 3.2 Ransomware

*Table 20: Average cost of a ransomware incident (globally) in 2025*

| Type | 2024 Average |
|---|---|
| Average Ransom Demand | USD 1,324,439 |
| Average Ransom Payment | USD 1,000,000 |
| Average Recovery Cost (Excluding Ransom) | USD 1,530,000 |
| Payment vs. Demand | 85% |

*Table 21: Average cost to recover, median ransom demand and median ransom payment by country/region in 2024*

| Country | Average Cost to Recover (Excluding Ransom) | Median Ransom Demand (2024) | Median Ransom Payment (2024) |
|---|---|---|---|

| | | | |
|---|---|---|---|
| France | $1.22 million | $643,125 | $231,525 |
| Germany | $1.56 million | $600,000 | $411,600 |
| Italy | $3.55 million | $4.12 million | $2.06 million |
| Spain | $1.15 million | $911,600 | $322,500 |
| Switzerland | $1.04 million | $328,748 | $1.1 million |
| UK | $2.58 million | $5.37 million | $5.20 million |

## 4. Costs parameters of data breaches

Among the cost drivers of cybersecurity incidents, an important parameter to be considered is the **time organizations took to identify (MTTI) and contain (MTTC)** a breach as well as the time to fully recover systems. **Recovery** means that business operations are back to normal, compliance obligations are met, confidence is restored, and controls are in place to avoid future breaches.

*Table 22: Mean-time-to-identify and mean-time-to-contain data breaches in 2021, 2024 and 2025 (in days)*

| Year | MTTI (Days) | MTTC (Days) | Total Days |
|---|---|---|---|
| 2025 | 60 | 181 | **241** |
| 2024 | 64 | 194 | 258 |
| 2021 (Peak) | 75 | 212 | 287 |

This time varies depending on how the incident was discovered, and recovery is typically longer when the incident was identified by disclosure of the attacker.

*Table 23: Mean-time-to-identify and mean-time-to-contain data breaches per identification method in 2025 (in days)*

| Identification Method | MTTI (Days) | MTTC (Days) | Total Days to Resolve |
|---|---|---|---|
| Organization's security teams and tools | 52 | 172 | **224** |
| Benign third party | 63 | 190 | 253 |
| Disclosure from the attacker | 75 | 183 | 258 |

Recovery time also depends on the use of emerging technologies in the security process.

*Table 24: Mean-time-to-identify and mean-time-to-contain data breaches per use of emerging technologies in 2025 (in days)*

| Security AI and Automation Usage | MTTI (Days) | MTTC (Days) | Total Days to Resolve |
|---|---|---|---|
| Extensive use | 51 | 153 | 204 |
| Limited use | 60 | 183 | 243 |
| No use | 72 | 212 | 284 |

This **time to recover** can be translate into **economic cost.** The longer it is, the more costly it will be for an organisation.

*Table 25: Economic cost of time to recover (in USD)*

| Breach Lifecycle Duration (MTTI + MTTC) | Average Cost (USD) |
|---|---|
| Less than 200 days | 3.87 million |
| Exceeding 200 days | 5.01 million |

## 2. EXAMPLES OF INCIDENTS AND SECTORAL TRENDS WITH SOCIETAL AND/OR ECONOMIC CROSS-BORDER IMPACT, INCLUDING SMES

The following table provides examples of cybersecurity incidents or sectoral trends and their cross-border impacts. The purpose of this table is not to quantify costs but to illustrate rippling effects onto the real world.

*Table 26: Examples of incidents and sectoral trends with societal and/or economic cross border impact (Source: Sophos[234])*

| No. | Incident or trends, date, source | Sector(s) and countries involved | What happened | Societal and/or economic cross border impacts |
|---|---|---|---|---|
| 1 | **NotPetya** (June 2017)<br>Major Cyber Incidents Archives - EuRepoC: European Repository of Cyber Incidents | Ukraine origin; heavy collateral damage in EU companies (e.g. manufacturing, shipping, health care, pharmaceuticals, global supply chain disruption, essential services disrupted in Ukraine) | Started as an attack against Ukraine on 27 June 2017, disguised as ransomware but in reality a wiper that irreversibly destroyed data. Spread globally within hours, bypassing borders and hitting multinational companies. | Shipping giant Maersk effectively paralyzed: 76 port terminals across the world were disrupted, leaving cargo ships stranded.<br>Essential goods like food, medicine, and energy shipments delayed, showing how a cyberattack in one region can cascade into global logistics.<br>Merck, one of the world's largest pharmaceutical companies, had its vaccine production disrupted.<br>Ripple effect on healthcare systems worldwide due to delayed medicine distribution.<br>Banks, government offices, and the Kyiv metro system were disabled.<br>Citizens couldn't withdraw money, pay bills, or use essential transport.<br>Ukrainian society faced a nationwide paralysis, |

[234] Sophos, *The State of ransomware 2025*, and Sophos, *State of ransomware – country reports (2025)*

| | | | | |
|---|---|---|---|---|
| | | | | highlighting the fragility of digital infrastructure during geopolitical conflict. |
| 2 | **WannaCry** (2017)<br>https://www.wired.com/story/how-wannacry-spread-around-the-world/ | Affected over 150 countries, hitting critical sectors including healthcare (notably the UK's NHS), telecommunications, transportation, manufacturing, government services, and finance | Launched on 12 May 2017, spreading via the EternalBlue exploit (a leaked NSA tool).<br>A ransomware attack, poorly coded with little chance of recovering files even if ransom was paid. | Over 200,000 computers across 150 countries affected.<br>Global cost estimated at $4 billion.<br>Healthcare:<br>- Over 80 NHS hospitals and 600 GP practices disrupted.<br>- Emergency departments forced to turn patients away.<br>- Operations and cancer treatments cancelled.<br>- Lives were put at risk — one of the clearest examples of a cyberattack impacting human safety directly.<br>Global Disruption Across Industries: Telecom (Spain's Telefónica), logistics (FedEx), railways (Germany's Deutsche Bahn), and manufacturing plants all impacted.<br>Employees sent home as systems locked up, productivity ground to a halt.<br>Takeaway: Showed how ransomware can directly endanger human lives by crippling hospitals and essential services. |
| 3 | **Colonial Pipeline Attack** (2021)<br>https://www.energy.gov/ceser/colonial-pipeline- | the U.S., disrupting the fuel sector, which in turn caused | On 7 May 2021, Colonial Pipeline — the largest refined oil pipeline in the U.S. — shut down operations after a | Ransom payment of $4.4 million (partially recovered by U.S. DOJ). Cleanup, recovery, and compliance costs added tens of millions.<br>Immediate Societal Impacts: |

| | | | | |
|---|---|---|---|---|
| | cyber-incident | widespread gasoline shortages, panic buying, and impacts on transportation and critical supply chains | ransomware attack.<br>The pipeline supplies 45% of the East Coast's fuel, moving 2.5 million barrels per day of gasoline, diesel, and jet fuel. | Fuel Shortages Across the U.S. East Coast. Shutdown lasted nearly a week: more than 11,000 gas stations ran dry across states like Georgia, North Carolina, Virginia, and Washington, D.C. In some areas, 70% of gas stations reported shortages.<br>Panic Buying & Public Anxiety: Fear of prolonged shortages led to panic buying and hoarding, worsening the crisis. Long queues at gas stations.<br>Transportation & Airline Disruptions: Airlines, including American Airlines and Delta, were forced to reschedule or add refuelling stops. Trucking and logistics companies saw higher fuel prices, raising delivery costs and slowing operations.<br>Economic Impact: National average gasoline prices rose to their highest level since 2014 (~$3 per gallon).<br>Takeaway: Highlighted the economic fragility of energy infrastructure under cyberattack. |
| 4 | **Jaguar Land Rover** (2025)<br>theguardian.com/business/2025/sep/16/jaguar-land-rover-production-shutdown-cyber-attack<br>https://www.bbc.com/news/articles/cgl15ykerlro | The UK, China, Slovakia, India, automotive manufacturing sector | In September 2025, a major cyberattack forced Jaguar Land Rover to halt production across its factories in the UK, China, Slovakia, and India, crippling the automotive manufacturing sector, disrupting global supply chains, and threatening thousands of jobs in the UK economy and beyond. | Jaguar Land Rover's (JLR) cyber-attack led to a shut-down of its UK factories (Solihull, Halewood, Wolverhampton), halting production entirely and costing about £72 million in lost sales per day.<br>Suppliers, especially small- and medium-sized firms in its supply chain (which supports over 100,000 UK jobs) are facing cash-flow crises, with some at risk of collapse without government support.<br>The wider UK economy is seeing a knock-on effect, as vehicle registrations are delayed, dealerships can't |

| | | | | |
|---|---|---|---|---|
| | | | | operate normally, and output lags during a key registration period.<br><br>The UK government will underwrite a £1.5bn loan guarantee to Jaguar Land Rover (JLR) to protect jobs and support the supply chain. It is believed to be the first time that a company has received government help as a result of a cyber-attack.<br><br>If the shutdown extends through to November, JLR could lose over £3.5 billion in revenue while suppliers' losses and job risks mount even higher. |
| 5 | **SolarWinds / "Sunburst"** (discovered late 2020)<br><br>https://cert.europa.eu/publications/security-advisories/2020-060/<br><br>Major Cyber Incidents Archives - EuRepoC: European Repository of Cyber Incidents<br><br>https://www.ironnet.com/hubfs/IronNet-2021-Cybersecurity-Impact-Report-June2021.pdf?hsLang=en&submissionGuid=39c8446a-6789-41e5-8652- | Global—including EU governmental & private organizations using SolarWinds Orion software | In December 2020, malicious activity that led to the compromise of the software of a major provider was exploited to access data of providers' customers.<br><br>According to CERT-EU, the attack was a very sophisticated supply chain attack | 85% of SolarWinds cyberattack victims said the attack had an impact ranging from 'small' to 'significant'.<br><br>Financial impact: On average globally, the attack cost companies 11% of their annual revenue. These financial costs include incident response and remediation, system upgrades, legal and regulatory fines, customer notification and support, operational disruption and downtime<br><br>Indirect and long-term costs: reputational damage and loss of trust, loss of intellectual property and sensitive data, insurance premium increases, litigation and legal fees, or loss of competitive advantage. |

| | | | | |
|---|---|---|---|---|
| | a7dd61b8af94. | | | |
| 6 | **Denmark Railway Transport Disruption** (November 2022)<br>Denmark's rail transport paralysed due to cyberattack \| INCIBE-CERT \| INCIBE | Denmark / Danish rail sector | Attack on a subcontractor's system used by Denmark's railway operator (DSB) forced a shutdown of services (servers shut down). | Daily life & mobility: Thousands of commuters, students, and workers were stranded, highlighting society's reliance on rail transport.<br>Safety risk: Train drivers lost access to safety-critical data, making continued operation unsafe.<br>Public trust: The sudden halt of the national rail network eroded confidence in digital resilience of essential services.<br>Vulnerability awareness: The incident exposed how attacks on third-party suppliers can paralyze critical infrastructure.<br>Social strain: Frustration, missed obligations, and unequal impact on vulnerable groups deepened the societal disruption. |
| 7 | **Transport Sector Trends** (2021-2022)<br>ENISA THREAT LANDSCAPE: transport sector | EU-wide transport sector (aviation, maritime, rail, road) | ENISA reports that ransomware attacks in transport nearly doubled in 2022 from 2021; other threats include data breaches, malware, DoS/DDoS. | Increased risk to movement of people/goods; potential disruptions in essential infrastructure; regulatory and insurance implications; growing need for OT/IT integration security. |
| 8 | **Health Sector Trend** (2021-2023)<br>ENISA Threat LANDSCAPE: HEALTH SECTOR | EU health, hospitals, health authorities | From reported incidents, ~ 215 publicly reported incidents over period; 54% of cybersecurity threats in health were ransomware; also many data breaches. | Impacts on patient care; cancelled or delayed operations; exposed sensitive personal data; pressure on policy to improve resilience of health systems. |

| | | | | |
|---|---|---|---|---|
| 9 | **Estonia GRU Attacks & Sanctions** (2020-2025)<br>Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia - Consilium | Estonia & EU | Series of cyberattacks by Russian GRU element U29155, infiltrating various government ministries, stealing documents including health, business data; led to EU sanctions against individuals. | Diplomatic consequences (sanctions), reinforcement of cyber norms and influence on policy (sanctions regime / cyber diplomacy toolbox); motivated other states to improve defensive posture. |
| 10 | **Airports software provider (Collins Aerospace) attack** (Sept 2025)<br>Cyberattack disrupts European airports including Heathrow, Brussels \| Reuters | Multiple major European airports (Heathrow, Brussels, Berlin etc.) | Attack/disruption affecting electronic check-in / baggage drop / boarding systems, due to cyber issue at a third party supplier. Forced manual procedures; flight delays / cancellations. | Travel & mobility disruptions; passenger inconvenience; economic cost; demonstrates dependencies on software providers; need for supply chain resilience. |
| 11 | **ENISA threat landscape on transport & OT** (2022)<br>ENISA THREAT LANDSCAPE: transport sector | EU transport sector | ENISA warned that operational technology (OT) infrastructure & industrial control systems are increasingly at risk, with more connected systems, more vulnerabilities. Ransomware increasing. | Potential for major disruption if safety-critical OT systems are directly attacked; underscores urgent need for OT security; drives regulatory / standards work. |

*Table 27: Examples of cyber incidents affecting SMEs*

| Company | Country | Year (incident / reporting) | Incident type | Reported impact | Direct quote (local source) | Source |
|---|---|---|---|---|---|---|
| **Einhaus Group (Hamm)** | Germany | 2023 attack, reported 2025 (insolvency proceedings) | Royal ransomware attack → downtime + ransom | Paid ≈ EUR 200,000 ransom; **total losses in mid seven-figure range**; insolvency for subsidiaries | *"Einhaus spricht von einem Schaden im mittleren siebenstelligen Bereich."* (WA.de, 31 Jul 2025) → "Einhaus speaks of a loss in the mid seven-figure range." | WA.de article |
| **Fasana (Stotzheim, paper-napkin manufacturer, ≈240 employees)** | Germany | May 2025 | Ransomware attack → production halted; ransom notes printed | **EUR 250,000 lost orders in one day**; **≈EUR 2 million losses in two weeks**; company filed insolvency | *"Allein am 20. Mai habe man Aufträge im Wert von mehr als 250.000 Euro nicht ausführen können…"* (Kölner Stadt-Anzeiger, 12 Jun 2025) → "On 20 May alone, orders worth more than EUR 250,000 could not be executed…" | Kölner Stadt-Anzeiger article |

- **Einhaus Group** was a significant player in the mobile phone insurance and repair industry, operating across Germany with a substantial workforce and revenue. The ransomware attack in 2023 led to severe operational disruptions, including the payment of a ransom and a drastic reduction in staff, ultimately resulting in the company's collapse. Previous to the attack, the company had around 170 employees and 70 million of annual revenues
- **Fasana GmbH**, a mid-sized manufacturer of paper napkins, experienced a ransomware attack in 2025 that halted production and caused significant financial losses. Despite efforts to recover, the company filed for insolvency due to the extensive impact of the cyberattack. Previous to the attack, the company had around 240 employees and 54 million of annual revenues in 2023.

### 3. CYBERSECURITY PROBLEMS CHAIN REACTION ON REAL WORLD PROBLEMS: QUANTIFIED EVIDENCE OF MAGNITUDE

*Table 28: Cybersecurity problems chain reaction*

| Cybersecurity problem | Evidence of the cybersecurity problem | Affected stakeholder(s) | Chain reaction on real world (societal problems) | Evidence of magnitude on real world (illustrative examples) |
|---|---|---|---|---|
| Fast-evolving cybersecurity threat: growing cybersecurity incidents | July 2023-June 2024: 11,079 incidents, including 322 incidents specifically targeting two or more Member States<br><br>Steep rise compared to July 2022-June 2023: 2,580 incidents, with an additional 220 incidents specifically targeting two or more Member | Private and public entities, including<br><br>public authorities | Need to recover from the costs of incidents | **Direct costs**<br><br>Total costs of cyber incidents are difficult to estimate, despite proliferating (non-scholarly) reports. Scholarly analysis of those reports estimates the range from USD 172 billion in 2017 to USD 8.0 trillion in 2021 [235].<br><br>Around 4,000 ransomware incidents per year[236] and the average cost of a ransomware attack in 2024-2025 was approximately EUR 1.59 million[237].<br><br>For a national example, Germany[238]: Record losses of around 267 billion euro (2024)<br><br>**Indirect costs:**<br><br>Large data breaches are associated with a loss of 5-9% reputational intangible capital or firm's brand value (Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018 \| Journal of Cybersecurity \| Oxford Academic)<br><br>Germany (2024):<br><br>• 8 out of 10 companies affected by data theft, espionage or sabotage in |

[235] Estefania Vergara Cobos , Selcen Cakir, *A Review of the Economic Costs of Cyber Incidents*, https://documents1.worldbank.org/curated/en/099092324164536687/pdf/P17876919ffee4079180e81701969ad0a18.pdf.
[236] ENISA, *ENISA Threat Landscape 2024*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[237] Astra, *100+ Ransomware Attack Statistics 2025: Trends & Cost*, 100+ Ransomware Attack Statistics 2025: Trends & Cost.
[238] Bitkom, *Vorstellung der Bitkom-Studie „Wirtschaftsschutz 2024*, Bundesamt für Verfassungsschutz - Bundesamt für Verfassungsschutz - Vorstellung der Bitkom-Studie „Wirtschaftsschutz 2024".

| | | | | |
|---|---|---|---|---|
| | States | | | • Cyberattacks: Two-thirds of companies feel their existence is threatened |
| | | | Increased need for cybersecurity professionals at a time of budget cuts | Cybersecurity incident responders are in the top 3 cybersecurity most needed roles (Summary-report_Cybersecurity-Skills-Needs-Analysis-1.pdf), identified by 34% of surveyed organisations[239]<br><br>Organisations in the EU have experienced cybersecurity cutbacks in the past 2024 with budget cuts on the rise (+3%), freezes on promotions (+6%), hiring freezes (+4%)[240] |
| | | | Increased need for spending on information security | Median spending for information security of an organisation in scope of the NIS2 Directive was EUR 1.4 million in 2023, while the average expenditure was EUR 6.7 million NIS INVESTMENTS 2024<br><br>"Even though more than 60% of CEOs and CISOs surveyed report that cyber risk management is integrated into enterprise risk management in their organizations, many still struggle to accurately assess the level of required investment". WEF_Global_Cybersecurity_Outlook_2025.pdf<br><br>Germany: The average share of IT security expenditure in companies' total IT budgets has risen to 17% (2024)[241] |
| | | Public authorities | Increased need for information exchange to allow more effective cross-border cooperation | Academic literature shows the added value of information exchange to ensure pro-active defence of organisations, while displaying the challenges in information sharing (lack of common language, complexity of information…) Overcoming information-sharing challenges in cyber defence exercises \| Journal of Cybersecurity \| Oxford Academic |

[239] ISC2, *First Look at the 2024 Cybersecurity Workforce Survey*, https://digital-skills-jobs.europa.eu/system/files/2024-12/ISC2_Workfoce-Study-Findings-EU.pdf.
[240] Ibid.
[241] Bitkom, *Vorstellung der Bitkom-Studie „Wirtschaftsschutz 2024*, Bundesamt für Verfassungsschutz - Bundesamt für Verfassungsschutz - Vorstellung der Bitkom-Studie „Wirtschaftsschutz 2024".

| | | | | |
|---|---|---|---|---|
| | | EU citizens | Increased societal instability<br>Safety and privacy<br>Financial | The societal impact (inability of the citizens to access important services) of cyber threats is the third biggest impact thereof, affecting primarily access to public administration and health sectors ENISA THREAT LANDSCAPE 2023<br>Global average cost of a data breach in 2025: USD 4.4 million (IBM. (2024) Data Breach Report). |
| Quickly evolving cybersecurity related technologies | Cybersecurity professional consider the biggest challenge industry faces will be emerging technology (48%)[242]<br>Annual growth rate of cloud security of approximately 25% projected through 2027 [243] | Companies and businesses<br>Public authorities<br>EU citizens | Need for a permanently skilled workforce | Cybersecurity professionals consider technical gaps on EU security teams to address Artificial intelligence (29%), Cloud computing security (27%), Zero Trust implementation (24%), Digital forensics and incident response (23%)[244]<br>Cybersecurity certifications are becoming key to showing credentials and demonstrating up-to-date knowledge, e.g. in France where 39% of professionals hold a certification (non-formal education) vs 36% holding a diploma in cybersecurity (formal education)[245]. |
| | | Companies and businesses<br>Public authorities | Need to keep up with technological evolution to ensure security of the systems | Bad actors are close to using AI to hijack other AI systems that companies rely on — like chatbots or agents — forcing them to go rogue, warns John Watters, a longtime cybersecurity leader and former top executive at Google's Mandiant[246]. He says security companies are now carving out a new vertical of products to respond[247]. Why it matters: The world is only months away from an untraceable cyberattack run entirely by an autonomous AI agent. But the attack won't be generic. It will be built uniquely for its victim, exploiting a zero-day vulnerability tailored to that |

[242] ISC2, *First Look at the 2024 Cybersecurity Workforce Survey*, https://digital-skills-jobs.europa.eu/system/files/2024-12/ISC2_Workfoce-Study-Findings-EU.pdf.
[243] ENISA, *NIS INVESTMENTS 2024*, https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf.
[244] ISC2, *First Look at the 2024 Cybersecurity Workforce Survey*, https://digital-skills-jobs.europa.eu/system/files/2024-12/ISC2_Workfoce-Study-Findings-EU.pdf.
[245] ANSSI, *Observatoire des métiers 2025*, https://cyber.gouv.fr/publications/observatoire-des-metiers-2025.
[246] Axios, *Axios AI+*, https://www.axios.com/newsletters/axios-ai-plus-eafb70c7-71fb-4dab-ba52-5006df10529e
[247] Ibid.

| | | | | |
|---|---|---|---|---|
| | | | | company's systems. The big picture: Security vendors need to adapt faster than ever to prepare customers for that new reality. Watters warns that AI tools will make it easier for malicious hackers to personalize their attacks and to do so at scale. |
| | | Academia | Need to keep up with updated curricula and training programmes | Academic literature demonstrates that "consistency across programs ensures that graduates enter the workforce with comparable skills, no matter where they were trained, enhancing their employability across the EU. As recognized by Stavrou & Piki (2024)[248], this is especially valuable for a mobile workforce, allowing professionals to transfer their skills easily across member states and filling gaps where shortages are acute.[249] |
| Lack of cybersecurity professionals | Estimated gap of 299,000 professionals missing in the EU in 2024 [250] | Companies and businesses<br>Public authorities | Difficulties to hire and adequately train professional; competition amongst employers | More than half of the companies that searched for adequate candidates experienced difficulties, such as finding qualified candidates (45%), because of lack of candidates (44%), lack of awareness (22%) and budget constraints (16%) [251]<br>57% of companies say their employees involved in cybersecurity absorbed this role into an existing non-cyber security related role. 34% of companies have recruited from a non-cyber security related previous role[252] |
| | | | Vulnerability to cybersecurity incidents / weakening of the security of | Nearly 50% of SMEs indicate that a lack of in-house cybersecurity expertise leaves them vulnerable to cyber incidents[253] |

[248] Comparative analysis of EU-based cybersecurity skills frameworks, https://doi.org/10.1016/j.cose.2025.104329.
[249] Ibid.
[250] ISC2, *First Look at the 2024 Cybersecurity Workforce Survey*, https://digital-skills-jobs.europa.eu/system/files/2024-12/ISC2_Workfoce-Study-Findings-EU.pdf.
[251] Eurobarometer (2024) on Cyberskills, https://europa.eu/eurobarometer/surveys/detail/3176.
[252] Eurobarometer (2024) on Cyberskills, https://europa.eu/eurobarometer/surveys/detail/3176..
[253] ENISA, *NIS INVESTMENTS 2024*, https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf.

| | | | | |
|---|---|---|---|---|
| | | | organisations | |
| | | | Incapacity to follow up on technological development / loss of competitiveness | The Draghi report explicitly identifies that competitiveness is less about relative labour costs and more about knowledge and skills embodied in the labour force[254]. |
| | | Academia | Difficulty in attracting academic knowledge and expertise to academia, with consequences on discrepancy between academic programmes/employers needs | There are not enough academic institutions achieving top levels of excellence and the pipeline from innovation into commercialisation is weak[255] |
| Proliferation of national cybersecurity certification schemes | The 2024 ENISA report on Market of Cybersecurity Assessments shows | National authorities<br>EU institutions | Fragmented cybersecurity across the EU creating strategic weaknesses | The 2024 Report on the State of the Cybersecurity in the Union[257] clearly shows uneven level of cybersecurity capability and maturity across member states creating strategic gaps and weaknesses in the Unions attack surface, which is interconnected through supply chains. |

[254] European Commission, *The Draghi report on EU competitiveness*, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.
[255] Ibid.
[257] ENISA, *The 2024 Report on the State of the Cybersecurity in the Union*, https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf.

| | | | | |
|---|---|---|---|---|
| | proliferation of certification schemes across different technologies and sectors, while at the same time there continues to be a strong market demand for security assurance based on certification schemes[256] | Companies and businesses<br><br>EU citizens | Lack of trust in security of ICT solutions limiting the Unions ability to adopt data-driven solutions at large | The 2025 Digital Trust Index[258] has shown that the global trust in digital services is declining. This has been impacting the use of cutting-edge technologies by customers[259] . The importance of trust in security of data has also been recognised in the G7 Leaders' Communiqué[260]. |
| | | Companies and businesses<br><br>EU citizens | Higher compliance costs for businesses resulting in higher prices, limited market access to the Single Market, fragmented reaction to emerging threats | The negative impacts of the lack of mutual recognition and harmonised security requirements has been also acknowledged in the Draghi report on EU competitiveness[261] and the Niinistö report[262]. The average cost of these certifications is around EUR 70 000 and can vary each can vary between EUR 28 750 for smaller systems to EUR 110 000 for larger and more complex systems to be assessed . This estimate would grow proportionally with the number of currently existing parallel/national schemas. |
| Complexity of cybersecurity policies | Results of the public consultation + | Companies and businesses | Reducing the burden on businesses to | A cybersecurity audit in the EU typically ranges from €3,000 to over €50,000, depending on the organization's size, complexity, audit scope, and regulatory requirements in 2025. While small businesses and basic |

[256] ENISA, *Conformity assessments*, https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity%20Certification%20Statistics%20Report.pdf.
[258] Thales, *2025 Digital Trust Index – Consumer Edition*, https://cpl.thalesgroup.com/about-us/newsroom/digital-trust-index-2025.
[259] See e.g. Euronews, Survey: Most Europeans are worried about their digital privacy - and it's impacting how they use AI, https://www.euronews.com/next/2025/06/12/survey-most-europeans-are-worried-about-their-digital-privacy-and-its-impacting-how-they-u?utm_source=chatgpt.com.
[260] G7 Leaders' Communiqué, https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1.
[261] European Commission, *The Draghi report on EU competitiveness*, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.
[262] European Commission, *Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness*, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf.

| | | | | |
|---|---|---|---|---|
| | stakeholder position papers + Implementation Dialogue on Cybersecurity Policy by EVP Virkkunen - stakeholders raised significant concerns about the cumulative burden of overlapping cybersecurity obligations[263] | Competent authorities | determine the applicable legal requirements and to support them in demonstrating compliance would free resources and allow entities to focus on the main goal – improving their resilience and Union's overall cyber posture. | vulnerability scans cost €3,000 – €10,000, compliance-focused audits (ISO 27001) can cost between €10,000 and €50,000 [264]. ISO 27001 is the most used international standard for information security in Europe. However, compliance with national cybersecurity frameworks can cost up to 100.000 EUR.<br><br>Therefore, entities which are subject to different national cybersecurity frameworks may have to obtain several certifications, increasing costs for compliance. The same holds true for entities subject to different legal frameworks. For instance, an entity which is subject to NIS2 and DORA and which is operating in two Member States with its activities in scope of NIS2 may have to carry three audits despite the existence of an internationally recognized standard for information security.<br><br>Focusing only on entities in scope of the NIS 2 Directive, it is estimated that around EUR 213 810 per entity per year are spent on demonstrating compliance[265]. Assuming that the new measure would lead to even a mere 10% reduction in time and effort, enabled by recognised certifications, this could save over EUR 3.40 billion annually across the EU. This highlights how adopting ECCF certifications can both strengthen security posture and |

[263] Many highlighted the challenges posed by the interplay of various EU regulations. In the implementation Dialogue, there was broad consensus among participants on the importance of simplifying regulatory compliance, reducing the documentation burden. Representatives from all sectors, including SMEs, also emphasised the need for clear, harmonised legislation and consistent implementation, highlighting that the existing framework is often too complex and fragmented.

[264] See the following articles, Qualysec, *How Much Does an IT Security Audit Cost*, https://qualysec.com/it-security-audit-cost/; Atlant, *The Real Cost of Cybersecurity Due Diligence: What You're Paying For and Why It Varies So Much,* https://atlantsecurity.com/blog/cost-of-cybersecurity-due-diligence/#elementor-toc__heading-anchor-21.

[265] Article 21(2) of the NIS 2 Directive requires entities to implement and demonstrate cybersecurity risk-management measures. Organizations typically spend between 1 000 and 4 999 hours per year on proving compliance with these requirements (Source: https://drata.com/blog/introducing-2023-compliance-trends-report) . To understand what this means in terms of staffing, this range corresponds to roughly 0.56 to 2.78 full-time equivalent (FTE) employees (assuming 1 800 working hours per FTE per year). Using an average fully loaded FTE cost of EUR 128 277 per year, this equates to an internal compliance demonstration cost ranging from approximately EUR 72 000 to EUR 356 000 annually per organisation. Taking the midpoint - around 3 000 hours or 1.67 FTE - the estimated average cost is about EUR 213 810 per year. A 1% reduction in the time spent proving compliance corresponds to saving about 30 hours or 0.017 FTE per year, corresponding to a cost save of approximately EUR 2 138 per organisation annually. Multiplied across the roughly 160 000 entities in scope of NIS 2, this efficiency gain could result in over EUR 340 million in collective annual savings across the EU.

| | | | | |
|---|---|---|---|---|
| | | | | materially reduce the administrative and financial burden of compliance with the NIS 2 Directive's risk-management requirements. |
| | | | | |

## 4. MINI-CASE STUDY

**The challenge of assessing societal impacts: the example of the Viasat Satellite Network Cyber-attack (2022)**

On February 24, 2022, coinciding with the start of Russia's invasion of Ukraine, a sophisticated cyberattack targeted the KA-SAT satellite network operated by Viasat Inc. This network provides broadband internet access to tens of thousands of users across Ukraine and much of Europe.

The attackers deployed a wiper malware known as "AcidRain" designed to remotely erase vulnerable modems and routers, effectively disabling them. The primary goal was to disrupt communications, not to steal data. The attack was publicly attributed by the European Union to Russia[266], as well as by the United Kingdom and by the United States.

**Quantifiable impact across Ukraine and Member States[267]**

- **Ukraine:** The attack severely disrupted internet access for both civilian and government users, hampering communications during a critical period of military conflict.
- **Germany:** A major German energy company lost remote monitoring access to over **5,800 wind turbines**, highlighting the risk to critical infrastructure.
- **France:** Nearly **9,000 subscribers** of a French satellite internet provider experienced outages.
- **Other EU Member States:** Around a third of **40,000 subscribers** of another satellite internet provider in Europe (including Germany, France, Hungary, Greece, Italy, and Poland) were affected.
- **Duration:** Some users were without internet for more than two weeks, demonstrating the prolonged operational impact.

**Unquantifiable societal and operational impacts**

- **Military and civilian impacts:** The outage affected not only government and military communications, but also civilian populations, who lost access to reliable information and essential services at a time of war for Ukraine. This disrupted daily business operations and potentially put at risk civilians in Ukraine, whose access to information was affected.

---

[266] Council of the EU, *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union*, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[267] ENISA, *ENISA Threat Landscape 2022*, https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf; Viasat, *Case Study*, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat; CERT FR, *Panorama de la cybermenace*, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf.

- **Critical Infrastructure:** The attack's spillover into the energy sector and widespread internet outages underscored the vulnerability of interconnected infrastructure across borders.
- **Recovery:** The recovery time varied, but the incident highlighted the challenges of restoring service after a coordinated, destructive cyberattack.

**Lessons Learned**

- **Cross-border vulnerability:** The attack demonstrated how a cyber incident in one country can rapidly impact multiple EU member states due to shared infrastructure.
- **Critical infrastructure risk:** Essential services are vulnerable to cyber disruptions and spillover effects.
- **Need for information sharing:** Better information sharing would have increased preparedness and resilience

## 5. STATE OF RANSOMWARE IN SELECTED EUROPEAN COUNTRIES

*Table 29: Ransomware attacks: financial, economic and human impacts, recovery and root causes in France, Germany, Italy, Spain, Switzerland and the United Kingdom (Q1 2025)*[268]

| Category | Finding | France (FR) | Germany (DE) | Italy (IT) | Spain (ES) | Switzerland (CH) | UK (UK) |
|---|---|---|---|---|---|---|---|
| **Survey scope** | Sample size (Organisations hit by ransomware) | **185** | **300** | **254** | **237** | **74** | **201** |
| | Employee Range | 100 to 5,000 | 100 to 5,000 | 100 to 5,000 | 100 to 5,000 | 100 to 5,000 | 100 to 5,000 |
| | Survey Period | Jan–Mar 2025 | Jan–Mar 2025 | Jan–Mar 2025 | Jan–Mar 2025 | Jan–Mar 2025 | Jan–Mar 2025 |
| **Attack Outcomes** | Percentage of attacks resulting in data encryption | **58%** (Above global 50%) | 51% (In line with global 50%) | 55% (Above global 50%) | 47% (Below global 50%) | 53% (Just above global 50%) | **70%** (Well above global 50%) |
| | Percentage of encrypted | 44% | 24% | **11%** | 36% | 10% | 26% |

[268] Sophos, *State of ransomware – country reports (2025)*

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | attacks that also resulted in data theft | | | | | | |
| **Financial impact (Ransom)** | Median Ransom Demand (Last year) | $643,125 | $600,000 | **$4.12 million** | $911,600 | **$328,748** | **$5.37 million** |
| | Demands of $1 million or more | 49% | 49% | 68% | 50% | 46% | **89%** |
| | Median Ransom Payment (Last year) | $231,525 | $411,600 | $2.06 million | $322,500 | $1.1 million (Shared by 22 respondents) | **$5.20 million** |
| | Typical percentage paid of the ransom demand (Global avg. is 85%) | 87% | 86% | **97%** | 80% | **76%** | **103%** |
| **Payment negotiation** | Paid LESS THAN the initial ransom | 38% | 47% | 62% | **72%** | 65% | 49% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | demand | | | | | | |
| | Paid THE SAME as the initial ransom demand | **50%** | 32% | 14% | 28% | 15% | 23% |
| **Recovery & Costs** | Average Cost to Recover (excluding ransom payments) | $1.22 million | $1.56 million | **$3.55 million** | $1.15 million | $1.04 million | $2.58 million |
| | Fully recovered in up to a week | 53% | **64%** | 46% | 49% | 58% | 59% |
| | Used backups to recover encrypted data | 60% | 59% | 58% | **70%** | 56% | **39%** |
| **Root Causes (Technical)** | Most common technical root cause | **Exploited vulnerabilities (30%)** | **Exploited vulnerabilities (42%)** | **Exploited vulnerabilities (35%)** | **Exploited vulnerabilities (30%)** | Compromised credentials (32%) | **Exploited vulnerabilities (36%)** |
| **Root Causes (Operational)** | Most common operational root cause | Known security gap (43%) | **Lack of people/capacity (47%)** | **Lack of expertise (45%)** | Known security gap (42%) | **Lack of people/capacity (55%)** | Lack of expertise (42%) |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Human Impact** | Reported increased anxiety or stress about future attacks | **50%** | 44% | 35% | 33% | 28% | 41% |
| | Staff absence due to stress/mental health issues | 22% | 44% | 32% | 25% | **64%** | 26% |

# ANNEX 8: COMMISSION STAFF WORKING DOCUMENT EVALUATION ACCOMPANYING THE DOCUMENT REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL ON THE EVALUATION OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA) AND THE EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

## GLOSSARY

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

| *Term or acronym* | *Meaning or definition* |
|---|---|
| AI | Artificial intelligence |
| BEREC | Body of European Regulators for Electronic Communications |
| CAB | Conformity Assessment Body |
| CERT-EU | Cybersecurity Service for the Union institutions, bodies, offices and agencies |
| cPPP | Contractual Public-Private Partnership on cybersecurity, signed by the European Commission and the European Cyber Security Organisation (ECSO) on 5 July 2016 |
| CRA | Cyber Resilience Act |
| CSoA | Cyber Solidarity Act |
| CSA | Cybersecurity Act |
| CSIRT | Computer Security Incident Response Team |
| DORA | Digital Operational Resilience Act |
| EC | European Commission |
| EC3 | European Cybercrime Centre |
| ECA | European Court of Auditors |
| ECCC | European Cybersecurity Competence Centre and Network |
| ECCF | European Cybersecurity Certification Framework |
| ECCG | European Cybersecurity Certification Group |
| EDA | European Defence Agency |
| eID | European Digital Identity |
| eIDAS | 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 Cybersecurity |
| EU Cyber Blueprint | Council Recommendation on an EU blueprint for cyber crisis management (COM/2025/66 final) |

| *Term or acronym* | *Meaning or definition* |
|---|---|
| EUCC | European Common Criteria |
| Europol | European Union Agency for Law Enforcement Cooperation |
| FTE | Full-time equivalent |
| GDPR | 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) |
| IA | Impact assessment |
| ICT | Information and communication technologies |
| IoT | Internet of things |
| ISAC | Information Sharing and Analysis Centre |
| MoU | Memorandum of Understanding |
| MS | Member State |
| NATO | North Atlantic Treaty Organization |
| NCC | National Coordination Centre |
| NGO | Non-governmental organisation |
| NIS | Network and information security |
| NIS2 Directive | Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 |
| OECD | Organisation for Economic Cooperation and Development |
| PART-IS | EU Regulation on Information Security (PART-IS, Regulation (EU) 2023/203) |
| SCCG | Stakeholder Cybersecurity Certification Group |
| SME | Small and medium-sized enterprise |
| SOG-IS MRA | Senior Officials Group Information Systems Security Mutual Recognition Agreement |
| TFEU | Treaty on the Functioning of the European Union |
| URWP | Union rolling work programme |

## 1. INTRODUCTION

The impact assessment (IA) report that accompanied the proposal for the Cybersecurity Act (CSA) in 2017[269] ('2017 IA') was developed by the European Commission to provide a comprehensive and evidence-based foundation for developing legislation on EU cybersecurity. The main purpose of the 2017 IA was twofold: (i) to assess whether the existing mandate and operations of the European Union Agency for Network and Information Security (ENISA) remained fit for purpose in a rapidly evolving threat and policy landscape, and (ii) to determine the need for an EU-wide cybersecurity certification framework for ICT products and services. The 2017 IA was not only a legal requirement under the then ENISA Regulation[270] but also a response to the growing recognition that cyber threats were increasing in scale and complexity and that fragmented national approaches to cybersecurity and certification risked undermining both the internal market and the EU's collective resilience.

### 1.1. Purpose and scope of the evaluation

Building on the 2017 IA, this evaluation report examines the performance of ENISA and the European cybersecurity certification framework (ECCF) since the adoption of the CSA. The evaluation was conducted in accordance with Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides the legal basis for EU action in this area, aiming to harmonise the laws of the Member States to ensure 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 ENISA Regulation setting out ENISA's current mandate. Activities aimed at increasing cooperation and coordination and EU-level capabilities to complement the action of Member States fall within the field of operational cooperation. This is specifically identified by the 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 (hereafter referred to as NIS Directive), for which Article 114 TFEU is the legal basis. The Directive identifies operational cooperation as an objective to be pursued by the Computer Security Incident Response Team Network (CSIRTs Network), with ENISA providing the secretariat and actively supporting cooperation (Article 12(1)). Article 12(f) further identifies the following as tasks of the CSIRT Network: identifying further forms of operational cooperation, including in relation to categories of risks and incidents, early warnings, mutual assistance and principles and modalities for coordination when

[269] Commission Staff Working Document Impact Assessment (2017) accompanying the 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').

[270] 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 (Text with EEA relevance) (http://data.europa.eu/eli/reg/2013/526/oj).

Member States respond to cross-border risks and incidents. Article 11(3) under the NIS2 Directive[271] also confirms this.

The 2017 IA covered the performance, governance and organisational structure of ENISA, focusing on the period from 2013 to 2016, also taking into account more recent developments and anticipated future needs. The 2017 IA examined ENISA's support to Member States, its role in policy development and capacity building, its contribution to operational cooperation and its visibility and added value at both national and EU levels. In parallel, the IA addressed the emerging challenge of cybersecurity certification. It analysed the proliferation of national schemes, the lack of mutual recognition and the resulting risks of market fragmentation and increased compliance costs for businesses, particularly SMEs. The 2017 IA thus considered not only the effectiveness of ENISA's existing mandate but also the potential benefits and design of an ECCF.

This evaluation assesses the extent to which the objectives of ENISA's mandate and of the ECCF have been achieved, the effectiveness and efficiency of the measures implemented, their continued relevance, coherence with other EU policies and the added value of EU action. The evaluation addresses the main issues arising from the evolving cybersecurity landscape, such as the increasing number and sophistication of cyberattacks, the need for a high common level of cybersecurity across the EU and the fragmentation of certification schemes for ICT products and services.

In line with the European Commission's Better Regulation Guidelines, the evaluation applies all five compulsory criteria:

- **Relevance:** Examining whether the action continues to address the needs of stakeholders in light of technological and threat developments.
- **Effectiveness:** Assessing the extent to which the objectives of the existing framework have been achieved.
- **Efficiency:** Evaluating whether the resources invested are justified by the results obtained.
- **Coherence:** Analysing both internal coherence across the various provisions of the CSA, including ENISA's mandate and the ECCF, and external coherence in relation to other EU legislation such as 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, later replaced by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS1 & NIS2 Directive), 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 (the General Data Protection Regulation or GDPR), Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic

[271] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (http://data.europa.eu/eli/dir/2022/2555/oj).

identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation), and sectoral rules.

- **EU added value:** Considering whether action at EU level provides benefits that could not be achieved by Member States acting alone, particularly in terms of reducing fragmentation and supporting the functioning of the internal market.

The methodology for this evaluation combines a review of legal and policy documents, ENISA's annual reports and technical studies, along with other grey literature, with both quantitative and qualitative data analysis. The evidence base is further strengthened by stakeholder consultation, a call for evidence, targeted surveys, interviews and workshops involving public authorities, EU institutions, industry, academia, civil society and individual citizens. Where possible, the assessment benchmarks EU approaches against international best practices and considers the coherence of measures with other relevant policies.

Despite its broad evidence base, the evaluation has several limitations. Data gaps persist in certain areas, particularly regarding the uptake and impact of certification schemes and the experiences of small and medium enterprises (SMEs) and end-users. The dynamic nature of the cybersecurity landscape and the concurrent evolution of related EU policies make it challenging to decide whether to attribute observed impacts solely to ENISA or to the certification framework. Furthermore, the representativeness of some stakeholder consultations is limited by the relatively low participation of certain groups.

The evaluation covers the period between 2019 and 2023. More recent developments, such as the Cyber Resilience Act (Regulation (EU) 2024/2847), could only partly be considered. The geographical scope includes all EU Member States, as well as countries participating in relevant EU cybersecurity initiatives, such as those in the European Economic Area and the European Free Trade Association and Horizon 2020-associated countries. The methodology and its limitations are described in detail in Annex II to the evaluation report.

## 2. WHAT WAS THE EXPECTED OUTCOME OF THE INTERVENTION?

This Chapter introduces the EU's action on cybersecurity as it falls within the scope of this evaluation, outlining its objectives, logic and the baseline conditions that shaped its design. The chapter explains how the CSA and the establishment of ENISA's mandate and the ECCF were intended to address persistent fragmentation, inconsistent protection and market barriers across Member States, based on the 2017 IA. By reconstructing the state of play prior to the CSA, this chapter provides the necessary context for evaluating the effectiveness and impact of the action in subsequent sections.

### 2.1 Description of the intervention and its objectives

The CSA, adopted in 2019, was designed to address persistent fragmentation and insufficient coordination in the EU's approach to cybersecurity. The preceding IA identified the need for a more coherent EU-wide approach, as existing legislation such as the NIS Directive, GDPR and eIDAS Regulation had resulted in a patchwork of national policies and certification schemes. This fragmentation undermined both the resilience of the internal market and the competitiveness of European industry.

The preferred options were a 'reformed ENISA' (Option 2) and the establishment of an EU general ICT security certification framework (Option 3). The explanatory memorandum confirms that these options were fully taken on board in the final CSA. ENISA was granted a permanent mandate and a central role in the EU cybersecurity ecosystem, with expanded responsibilities to support policy implementation, capacity building, support for operational cooperation and certification. The CSA also established the ECCF, aiming to harmonise certification schemes across the EU, reduce costs and administrative burdens and increase trust in ICT products, processes and services.

These actions were intended to address several interrelated problems. Fragmentation of cybersecurity policies and national certification schemes across Member States led to inconsistent levels of protection and market barriers. There were also dispersed resources and approaches among EU institutions, agencies and bodies, as well as insufficient awareness and information among citizens and businesses regarding cyber threats and the security properties of ICT products and services.

To tackle these problems, the following objectives were agreed upon:

- increase capabilities and preparedness of Member States and businesses,
- improve cooperation and coordination across Member States and EU institutions, agencies and bodies
- enhance EU-level operational capacity, particularly in the case of cross-border cyber crises
- raise awareness of cybersecurity issues among citizens and businesses,
- increase transparency of cybersecurity assurance for ICT products, services and processes and
- avoid further fragmentation of certification schemes and related requirements across the EU.

At the time of adoption, the expected achievements were clear. The CSA was expected to deliver a more harmonised and resilient cybersecurity landscape, with ENISA acting as a centre of expertise, supporting policy implementation, capacity building and operational

cooperation. The ECCF was expected to streamline certification processes and reduce costs by up to 80% for certain products. The intervention logic was that by empowering ENISA and establishing a harmonised certification framework, the EU would be better equipped to respond to cyber threats, support the digital single market and protect citizens and businesses. Success was expected to be reflected in a more harmonised and resilient cybersecurity landscape, with reduced costs and barriers for businesses and increased trust and awareness among users.

The strategic objective of the intervention logic for the EU cybersecurity certification scheme was 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 to reduce trade hindrances.

Quantitatively, according to the 2017 IA, before action was taken, certification costs for products like smart meters could exceed EUR 300 000 for two markets, with processes taking six to eighteen months. For cloud services, compliance costs were estimated at EUR 1.2 billion, representing up to 10% of annual expenditures and certification could take up to nine months. The CSA aimed to reduce these costs by up to 80% for smart meters and to achieve yearly savings of EUR 1.1 billion in the EU public sector for cloud services, with certification times reduced to four to six months.

### 2.2 Point(s) of comparison

This section reconstructs the state of play in the EU as of 2017, drawing on the 2017 IA and its supporting studies, stakeholders' consultations and economic analyses. The baseline scenario reflects the situation before the adoption of the CSA and serves as the main point of comparison for assessing subsequent developments. It covers ENISA's status and resources, the certification landscape, relevant market and economic data, as well as stakeholder perceptions and consultation data.

**ENISA's status and resources**

In 2017, ENISA was operating under a fixed-term mandate that was due to expire in 2020. Its annual EU contribution was EUR 10.3 million and it had an authorised establishment plan of 48 staff members, making it one of the smallest EU agencies in terms of both budget and personnel. Despite its broad mandate, which included support for policy development and implementation, capacity building, community building and support for operational cooperation, ENISA's resources were widely recognised as insufficient to meet the growing and evolving demands from Member States, EU institutions and the private sector.

When ENISA's performance was evaluated for the period 2013-2016, it was found to be relevant and efficient to a large extent, but its effectiveness, coherence and EU added value were only partially achieved. The fixed-term mandate was a significant limitation, as it prevented long-term planning and sustainable support for Member States and EU institutions. Furthermore, ENISA's ability to recruit and retain highly qualified experts was hampered by its location (split between Athens and Heraklion) and the predominance of fixed-term contracts, which made it less attractive compared to other agencies or the private sector.

Stakeholder consultations reinforced these findings. A majority of respondents considered ENISA's size insufficient for its workload. There was a broad consensus that both its resources and mandate needed to be adapted to enable it to support Member States in facing future cybersecurity challenges. While ENISA's activities were generally coherent with those of other organisations, there was a clear need for a more coordinated approach at EU level. The agency's main added value was seen in its ability to enhance cooperation between Member States and communities under the NIS Directive, but its impact was limited by its scale and temporary mandate.

**Certification landscape**

The certification landscape in the EU in 2017 was highly fragmented and complex. Multiple national and sectoral certification schemes existed. Manufacturers often had to certify the same product multiple times to access different national markets. For example, according to the 2017 IA[272], smart meter manufacturers faced costs of around EUR 1 million to certify products in three countries, a barrier particularly penalised SMEs.

The SOG-IS Mutual Recognition Agreement (MRA) was the main European mechanism for certification, but it only included 12 Member States plus Norway and was limited to a few protection profiles for certain digital products. Certification processes were lengthy and costly: a CC certificate for the lowest assurance level could take six months and cost EUR 20 000, while higher assurance levels could take up to two years and cost at least EUR 500 000. The lack of a harmonised approach led to significant market fragmentation, increased costs and barriers to entry, especially for smaller companies.

Surveys conducted as part of the 2017 IA showed that a majority of respondents were aware of multiple certification schemes for the same product or service and a large majority agreed that mutual recognition was desirable at European level. The absence of a common EU framework for certification was widely seen as a major obstacle to the development of the digital single market and the competitiveness of European industry.

**Relevant market and economic data**

According to the 2017 IA, the economic impact of cybercrime in the EU was substantial. It was estimated at 0.41% of GDP, or around EUR 55 billion in 2013, with Germany being the most affected Member State (1.6% of GDP)[273]. The cost of certification for smart meters was at least EUR 300 000 for two markets and for cloud services, compliance costs were estimated at EUR 1.2 billion, representing 2% to 10% of companies' annual expenditure. Certification processes for cloud services could take 7-9 months.

The EU's investment in cybersecurity was below the critical mass needed to protect the economy and institutions, especially when compared to international competitors. For example, the US government invested over EUR 19 billion in cybersecurity in 2017, a

[272] EUR-Lex - 52017SC0500 - EN - EUR-Lex

[273] McAfee & Center for Strategic and International Studies, 'Net Losses: Estimating the Global Cost of Cybercrime', 2014.

35% increase from 2016[274]. EU funding for cybersecurity projects under Horizon 2020 was about EUR 600 million for 2013-2020, with additional contributions from other programmes, but these were not sufficient to address the scale of the challenge[275]. The lack of sufficient investment and coordination at EU level was seen as a key barrier to building resilience and supporting the digital single market.

**Stakeholder perceptions and consultations data**

Stakeholder consultations for the 2017 IA included a call for evidence, targeted surveys, workshops and interviews with a wide range of actors, including public authorities, EU institutions, industry, academia, civil society and individual citizens. The main findings were as follows:

- A large majority of respondents positively assessed ENISA's performance for 2013-2016 and a significant proportion considered ENISA to be achieving its objectives.
- Many appreciated ENISA's products and services as coming from an EU-level body and valued their quality.
- A large majority considered current EU instruments and mechanisms insufficient or only partially adequate to address cybersecurity challenges and almost all saw a need for an EU body to respond, with most identifying ENISA as the right organisation.
- A significant proportion of respondents to the ENISA consultation saw a role for ENISA in establishing a harmonised framework for ICT security certification.
- Many respondents to the 2016 consultation for the preparation of the EU cybersecurity contractual public-private partnership (cPPP)[276][277], which devoted a section to the topic of certification, did not know whether national certification schemes were mutually recognised, with only a minority saying 'Yes'[278].
- A substantial proportion thought existing certification schemes did not support the needs of Europe's industry, and many said it was not easy to demonstrate equivalence between standards, certification schemes and labels.
- Many respondents experienced barriers to market access and export due to fragmentation and a significant number of SME respondents identified the cost of certification as a problem.

Stakeholders consistently identified the most urgent gaps to be in cooperation across Member States, capacity to prevent and resolve large-scale attacks and the need for

---

[274] As per CSA 2017 IA; Source: White House, Factsheet Cybersecurity National Action Plan.
[275] CSA 2017 IA.
[276] Contractual Public-Private Partnership on cybersecurity, signed by the European Commission and the European Cyber Security Organisation (ECSO) on 5 July 2016.
[277] Commission 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, accompanying the document 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, SWD(2016) 215 final.
[278] In this 2016 public consultation, a section was devoted to the topic of ICT security certification. 240 stakeholders from national public administrations, large businesses, SMEs, microbusinesses and research bodies responded to the section on certification.

harmonised standards and certification. The consultations also revealed that while ENISA was valued for its expertise and its role in community building, there was a strong call for a more permanent, better-resourced agency with a clearer mandate and greater operational capacity.

In summary, the baseline scenario in 2017 was a small, under-resourced ENISA with a fixed-term mandate, a fragmented and costly certification landscape, significant economic losses due to cybercrime and widespread stakeholder recognition of the need for greater EU-level coordination, harmonisation and investment. The lack of mutual recognition of certification schemes, high costs and long processes and insufficient EU-level operational capacity were seen as major barriers to a secure and competitive digital single market. These baseline conditions provide the foundation for assessing the effectiveness and impact of the CSA and the reformed ENISA. The evidence presented here is drawn directly from the 2017 CSA IA, including its executive summary, problem definition, baseline scenario, economic analysis and stakeholder consultation sections.

## 3. HOW HAS THE SITUATION EVOLVED OVER THE EVALUATION PERIOD?

This chapter reviews how the EU's cybersecurity landscape has evolved over the evaluation period, highlighting the transformative impact of major legislative acts such as the Cybersecurity Act, NIS2 Directive, Cyber Resilience Act and Cyber Solidarity Act (both under development at the time of the evaluation). These laws, together with sector-specific regulations, have reshaped the mandates and activities of ENISA and the ECCF. The chapter outlines how new threats, rapid digitalisation and geopolitical tensions have driven regulatory and operational changes, setting the context for assessing the effectiveness, coherence and added value of the EU's action on cybersecurity.

### Current state of play

Since the adoption of the CSA, the EU's cybersecurity environment has undergone profound changes. The world has seen a dramatic escalation in cyber threats, with attacks becoming more frequent, sophisticated and impactful. Geopolitical tensions, such as Russia's war of aggression against Ukraine, have brought cyber operations to the forefront of hybrid warfare. At the same time, the COVID-19 pandemic accelerated digitalisation, exposing new vulnerabilities as remote work and digital services expanded rapidly. These developments have fundamentally altered the risk landscape and prompted the EU to significantly strengthen its legal and policy framework for cybersecurity.

### Expansion of the EU cybersecurity legal and policy framework

In response to these evolving challenges, the EU adopted new legislative and policy instruments (of which some were under development during the evaluation period), building on the foundation laid by the CSA, and which have been central to the EU's cybersecurity strategy:

- **NIS2 Directive (Directive (EU) 2022/2555):** This Directive makes a broader range of entities subject to cybersecurity requirements, strengthens risk management and incident reporting obligations and develops cooperation among Member States.
- **Cyber Resilience Act (CRA, Regulation (EU) 2024/2487**, under development during the evaluation period**):** The CRA introduces horizontal cybersecurity requirements for products with digital elements, aiming to ensure that hardware and software placed on the EU market are secure by design and by default considering their lifecycle.
- **Cyber Solidarity Act (CSoA, Regulation (EU) 2025/38,** under development during the evaluation period**):** The CSoA focuses on building Union capacities for detection, preparedness and response to significant and large-scale cyber incidents, including the establishment of the EU Cybersecurity Reserve.
- **Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554):** DORA sets out comprehensive requirements for the financial sector to ensure operational resilience against ICT-related incidents.
- **Network Code on Cybersecurity for Electricity (NCCS, Delegated Regulation (EU) 2024/1366**, under development during the evaluation period**):** The NCCS introduces sector-specific cybersecurity rules for the electricity sector, particularly for cross-border flows.

- **EU Regulation on Information Security (PART-IS, Regulation (EU) 2023/203):** PART-IS establishes information security requirements for the air transport sector.
- **5G Cybersecurity Toolbox (Commission Recommendation (EU) 2019/534):** This provides guidance for securing 5G networks across the EU by recommending strategic and technical measures.
- **Cybersecurity Skills Academy (COM(2023) 207 final):** This initiative addresses the growing gap in cybersecurity skills by promoting training and capacity building.
- **EU Action Plan on the Cybersecurity of Hospitals and Healthcare Providers (COM(2025) 10 final):** This plan aims to strengthen the resilience of the healthcare sector.

Together with the CSA, these legal and policy instruments form a comprehensive and multi-layered framework that addresses both horizontal and sector-specific cybersecurity challenges. They reflect the EU's recognition that cybersecurity is not only a technical issue but also a matter of economic security, public safety and strategic autonomy.

**Implementation and operational developments**

The implementation of the new legal framework has required significant adaptation by Member States, EU institutions and businesses. ENISA's mandate has expanded accordingly. ENISA now supports Member States in developing and updating national cybersecurity strategies, implementing new legal requirements and building operational capacity. By virtue of other legislation proposed at the time of evaluation and subsequently through the contribution agreements, ENISA has also been tasked with managing the European Vulnerability Database and supporting the EU Cybersecurity Reserve.

The ECCF, established by the CSA, has continued to evolve. ENISA has coordinated the development of candidate certification schemes, such as the EU Common Criteria (EUCC) and the forthcoming European Cloud Certification Scheme (EUCS). However, the process has been slower than anticipated, with the first scheme taking nearly five years from initiation to adoption. The reasons for the delays include the complexity of technical, legal and political negotiations, as well as the need for consensus among a wide range of stakeholders.

Monitoring arrangements have included regular reporting, stakeholder consultations and the use of indicators such as the number of training courses delivered, publications produced, and stakeholder engagement events held. ENISA's outputs have increased in both volume and scope, reflecting the growing demands on it.

**Current situation and key developments**

The cybersecurity threat landscape has become more complex and interconnected. Ransomware attacks, supply chain compromises and hybrid threats are now commonplace, affecting critical infrastructure, public services and businesses of all sizes. The average cost of a major cyber incident has risen sharply, with global estimates of

overall cost exceeding EUR 5.5 trillion in 2020[279] and projected to reach EUR 9 trillion by 2025.

ENISA has responded by scaling up its activities, delivering a growing number of publications, technical guidelines and capacity-building events. ENISA has played a central role in supporting the implementation of new legislation, advising on incident response and facilitating information sharing among Member States. The ECCF has begun to deliver candidate certification schemes (with one scheme adopted), but the pace has been slower than originally envisaged and fragmentation persists due to differences in national approaches and resource allocation.

**Delays, challenges and external factors**

The implementation of the new legislative framework has not been without challenges. Delays in the adoption of certification schemes have limited the harmonisation of cybersecurity assurance across the EU. Both ENISA and national authorities are affected by resource constraints, including the shortage of skilled cybersecurity professionals. The regulatory landscape is complex, with overlapping horizontal and sector-specific requirements. This has created compliance challenges for businesses operating across multiple sectors.

External factors, such as the acceleration of digital transformation, the emergence of disruptive technologies like AI and quantum computing and intensifying geopolitical tensions, have all impacted the implementation of the EU's cybersecurity framework. Hybrid attacks, in which cyber operations are combined with other forms of aggression, have become a defining feature of the threat landscape.

**Monitoring, indicators and further information**

Throughout the evaluation period, ENISA's mandate and the ECCF have been monitored using a range of quantitative and qualitative indicators. These include the number of certification schemes adopted, the volume and reach of ENISA's outputs, the level of stakeholder engagement and feedback from stakeholder consultations. Further details and data can be found in the annexes to the evaluation report.

In summary, the evolution of the EU's cybersecurity landscape over the evaluation period has been shaped by a series of ambitious and far-reaching legislative initiatives. These new laws have been instrumental in driving change, expanding the regulatory framework and strengthening the capacity of Member States, EU institutions and businesses to address increasingly complex and dynamic cyber threats. Their implementation has also revealed important challenges, including delays, resource constraints and the ongoing need for harmonisation. The rapidly changing cyber threat landscape, technological advances and geopolitical developments increase the critical importance of these legislative measures and the need for continued adaptation and coordination at European level. This is the background to the subsequent analysis of the effectiveness, efficiency and added value of the CSA, ENISA's mandate and the ECCF.

[279] JOIN(2020) 18 final.

## 4. EVALUATION FINDINGS (ANALYTICAL PART)

This chapter presents an analytical assessment of the CSA, ENISA's mandate and the ECCF, drawing on the study to support the evaluation of ENISA and the ECCF from 2024[280]. This chapter summarises the findings around the five evaluation criteria: effectiveness, efficiency, coherence, EU added value and relevance. Drawing on qualitative and quantitative evidence, including stakeholder surveys, interviews and performance data, this chapter compares the expected outcomes of the action with the actual situation observed during the evaluation period. The analysis provides an evidence-based assessment on the extent to which the action achieved its objectives, the difference it made for various stakeholders and its ongoing suitability in the face of evolving cybersecurity challenges and policy needs. References to supporting data and further details are provided throughout, with additional evidence available in the annexes.

### 4.1. To what extent was the intervention successful and why?

**Effectiveness**

**ENISA**

ENISA has fulfilled its mandate by delivering nearly all planned outputs. During challenging times, such as the COVID-19 pandemic and Russian war of aggression on Ukraine, ENISA demonstrated flexibility and was evaluated positively by stakeholders. ENISA's effectiveness stems from a robust governance structure and a matrix-based organisational model that facilitates task delivery and cooperation. However, while stakeholders valued ENISA's capacity-building efforts, there were occasionally delays due to ongoing resource constraints and rigid strategic plans. In particular, ENISA planned 219 outputs between 2017 and 2022 and delivered 203, often exceeding initial targets per output due to a higher-than-expected number of stakeholders engaged in its activities. Eight outputs were delivered to some extent and in three cases, outputs were not delivered or only partially achieved, due particularly to the COVID-19 pandemic. The results of five outputs were not reported entirely. ENISA's support for policy implementation was generally well received, with 93% of stakeholders expressing satisfaction with ENISA's added value in this area in 2022. ENISA contributed to national and EU policies and legislative initiatives, supported the implementation of the NIS Directive and played a key role in the development of the ECCF. In 2021, ENISA made 193 relevant contributions to EU and national policies and legislative initiatives, which increased to 314 in 2022. However, over 80% of these contributions were through organising workshops and conferences. In 2022, ENISA's reports, analyses and studies were referred to 65 times at EU and national levels. Between 2017 and 2023, ENISA produced and issued a total of 286 publications. These covered a wide range of topics, with the most frequent being cybersecurity policy (72 publications), cyber threats (48), critical infrastructure (38), incident reporting (24) and emerging technologies (21).

[280] PPMI, Intellera Consulting and PwC (2024): Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report.

Among key outputs, ENISA's studies, such as the 2020 report on NIS investments[281], highlighted the challenges faced by organisations in implementing the NIS Directive, such as unclear expectations and limited support from national authorities. Moreover, the Agency's support to the NIS Cooperation Group Workstream on Digital infrastructure and service providers was crucial in analysing the security aspects of the digital infrastructure sector, which then fed into the NIS2 proposal to extend the scope of the sector. This analysis also assisted Member States in the development of guidelines by highlighting priorities and best practices within the industry.[282]

In 2023, ENISA's efforts in the implementation of the directive included the provision of technical advice to the Commission on the implementation of NIS2 security measures and the drafting of guidelines for national coordinated vulnerability disclosure policies.[283] The Agency supported the implementation of NIS2 by responding to 12 individual requests from Member States for advice on the transposition of the Directive into national legislation and by organising risk management training for national authorities to help build knowledge and expertise.

However, stakeholders also noted that ENISA's reports could be more concise, practical and better tailored to their needs, with improved visualisation and summaries. The lack of a more effective communication system and the complex structure of ENISA's website further complicated stakeholder interaction with ENISA's outputs. Some stakeholders called for more transparent processes, better tailored content and more detailed and pragmatic guidance, especially for sector-specific needs.

While ENISA has achieved many of its objectives, there is a clear opportunity for ENISA to enhance its efficiency through improved prioritisation, clear focus and more strategic resource allocation. ENISA's efficiency has been occasionally hampered by external factors and a need for more streamlined internal governance. Internally, ENISA has developed innovative solutions, such as a matrix-based organisational model, to coordinate between operational and administrative functions more effectively. However, ENISA's staff occupancy rate fluctuated between 74% and 90% from 2017 to 2023 and recruitment and retention of senior cybersecurity experts remained a persistent challenge. This impacted deliverables, with some outputs that were not delivered or only partially achieved.

There is also room to improve task prioritisation. By reassessing its operational focus, ENISA can leverage existing frameworks and stakeholder feedback to improve task delivery even further. This approach is particularly crucial for addressing emergent priorities without compromising on existing commitments. ENISA's ongoing commitment to stakeholder engagement and consultation has been a strength, yet its operational capacity shows insufficient resources. More dynamic reallocation of tasks and resources could help towards timely fulfilment of new requests and enhance ENISA's ability to respond to cybersecurity challenges to a certain extent.

ENISA's aim of maintaining and bolstering its reputation in the cybersecurity community could be further realised by ensuring that tasks are aligned not only with strategic goals but also with operational capacity. To this end, ENISA's mandate would

[281] NIS Investments Report 2020, https://www.enisa.europa.eu/publications/nis-investments
[282] ENISA, Annual Activity Report, 2020.
[283] ENISA, Annual Activity Report, 2023.

need to be revised, supported by a continual process of resource evaluation and strategic reprioritisation. This structured approach will assist ENISA in navigating its evolving role within the EU cybersecurity framework more effectively, ultimately increasing its impact and sustaining its status as a flagship institution for cybersecurity initiatives. Such prioritisation should be facilitated through collaborative efforts between ENISA, Member States, and EU policymakers to ensure alignment with strategic objectives and operational capacity.

**ECCF**

The ECCF was envisioned as a pillar for improving cybersecurity assurance across the EU internal market, aiming to harmonise the certification of ICT products, services, and processes. It sought to tackle persistent issues such as market fragmentation, the need for enhanced transparency, and raise public trust in digital solutions. Its structured governance model involving entities like ENISA and the European Cybersecurity Certification Group (ECCG), gathering National Cybersecurity Certification Authorities (NCCAs), has indeed laid a foundation for increased coordination among stakeholders, including Member States and private entities. However, the practical realisation of these goals has been met with numerous challenges that have restricted the ECCF's effectiveness. A significant shortcoming of the current ECCF is its inability to effectively address the fragmentation of certification schemes across the EU, mainly due to procedural limitations. This fragmentation has persisted even though the framework is intended to harmonise certification processes, leading to inconsistencies and inefficiencies in cybersecurity assurance. This can be observed in the substantial delay in operationalising the first certification scheme, the EUCC, which took 55 months from initiation to adoption. This delay points to inefficiencies, predominantly influenced by the complex and multifaceted approval procedures. Moreover, there is a certain lack of clarity about responsibilities and accountability among stakeholders. This has made achieving the framework objectives even more complex. External factors further complicated the ECCF's aims.

The evolving geopolitical landscape, characterised by increasing cyber threats and political tensions around data sovereignty and digital control, required adaptive measures that the ECCF struggled to implement swiftly. These external pressures resulted in delayed scheme adoptions, as seen with the EUCS, where discussions stalled over non-technical debates like data localisation requirements.

Despite these hurdles, there have been positive outcomes–particularly in raising awareness across Member States about the importance and intricacies of cybersecurity certification. The COVID-19 pandemic, while causing operational delays, also made the necessity for resilient digital infrastructure even clearer, thrusting cybersecurity into the policy spotlight. Additionally, the analysis identified key lessons, noting the uneven resource allocation across stakeholders, which hinders the uniform development and deployment of certification schemes. National authorities acknowledged the support of the ECCF in building national cybersecurity certification capabilities but noted significant resource imbalances between Member States. For example, the number of FTEs was seven times higher in one Member State compared to another one for similar activities of issuing certificates. Also, ENISA stated that due to the difficulty of retaining staff and the competitive job market for cybersecurity professionals, it could not maintain its full staff level (including for certification) at times. Addressing these disparities is vital for future efficiency and effectiveness, particularly through retaining expert staff within ENISA and fostering constant dialogue among all parties involved.

Despite these challenges, the ECCF did improve harmonisation among Member States and established better cooperation opportunities, particularly through the creation of stakeholder cooperation forums such as the ECCG. Most participants during the interview process agreed that the ECCF established better cooperation opportunities for Member States and the majority of Member State representatives interviewed agreed that the ECCF improved harmonisation among Member States. Statements gathered during interviews underlined the importance of the ECCF support to Member States when Member States developed their capabilities. For instance, one national authority reported how it benefited from cooperation among Member States by acquiring knowledge in areas where it lacked expertise, while others stressed the pedagogical value that cooperation among ECCG members can have. However, national experts stressed that the ECCF strengths remained 'potential' due to the lack of scheme implementation so far.

**Efficiency**

**ENISA**

During the evaluation period, which spanned from 2017 to 2023, ENISA demonstrated efficient operations under its existing governance structure. The matrix-based organisational framework helped ENISA prioritise tasks, optimised resource alignment, and fostered cooperation between various units. This approach, coupled with a balanced mix of operational and administrative staff, helped facilitate the execution of its mandated duties. Despite this, the evaluation highlighted several key areas where ENISA has room to improve its efficiency. Interviews with ENISA's staff, stakeholder surveys and internal documentation indicated that ENISA struggled to keep pace with increasing demands and fill specialised positions, exacerbated by a global shortage of IT and cybersecurity specialists. This has led to delays, reprioritisation of tasks, and periods of high stress and workload. Stakeholders gave a positive assessment of ENISA's performance during periods of high workload, with 63% of respondents stating that ENISA was successful or very successful in delivering its outputs. However, resource constraints, operational inefficiencies and challenges stemming from the political and regulatory environment were identified as the main obstacles to ENISA's performance during periods of high workload. In 2022, 64% of respondents experienced stress due to high workload and 43% due to high administrative burden. Only 32% gave a positive assessment of stress management.

Nevertheless, certain adjustments could alleviate these challenges. The recent strategic decisions to reallocate human resources demonstrate a capacity that can address priority shifts to a certain extent. For instance, the reallocation of approximately 10.5 FTEs planned in 2022 to accommodate the Cybersecurity Support Action suggests that ENISA is able to optimise current resources when necessary even though, on that occasion, the FTEs needed for the implementation of the Support Action were in fact obtained partially through procurement and partially through contract management staff.

Budget management also presents opportunities for improvement. Despite significant budget growth from 2017 to 2023, resource constraints persisted. ENISA's budget grew unevenly, with notable increases in 2019 (over 46%), 2020 (30.5%) and 2022 (72.4% compared to 2021, due to the Cybersecurity Support Action). ENISA was less able to balance approved and committed appropriations between 2019 and 2022 due to delays in actions like the Cybersecurity Support Action. By reversing this trend and making efforts

to manage administrative expenditure, including addressing procurement delays, internal efficiency could see certain further enhancement.

**ECCF**

The efficiency of the ECCF has been subject to scrutiny, given the extended timelines for the adoption of cybersecurity certification schemes and the myriad of complexities involved. Despite its strategic aim of streamlining the certification process across the EU, the ECCF's efficiency was notably hampered by drawn-out discussions and preparation phases that culminated in significant delays; the first scheme EUCC was only adopted in early 2024, nearly five years post-implementation. These protracted timelines can be attributed to multifaceted challenges encompassing both political and technical dimensions.

Given the recent adoption of the EUCC scheme, it is premature to identify costs borne or benefits experienced by stakeholders for compliance with ECCF requirements. Survey respondents indicated some costs and benefits related to preparatory activities. Benefits include enhanced cooperation, knowledge exchange, growing awareness and contribution to standard development. Costs include dissemination and awareness support, pilot implementations, legal consultations for aligning national requirements, setting up of web portals and reporting mechanisms and CAB accreditation. Stakeholders involved in preparing schemes bore costs related to scheme development, publication and communication efforts, including investment in staff allocation and upskilling.

Content and process-related issues had the greatest impact on the efficiency of the ECCF. Content issues included political factors and the technical complexity of schemes, which varied for each scheme depending on the stakeholders involved and products/services to be certified.

More generally, political challenges, including the politicisation of discussions around certification requirements, have hindered progress by creating an environment where transparency and communication suffered. For instance, the EUCS was impacted significantly by debates around data sovereignty requirements, attracting political pressure from non-EU countries and industry outside the EU, leading to shifts from technical to political discourse within the ECCG. Moreover, the scheme was impacted by a shift in EU policy priorities due to the concurrent proposal of the CRA in September 2022.

Technical complexities further contributed to inefficiencies, notably the difficulty in translating draft schemes into legal acts, given the diverse and demanding nature of the products/services slated for certification, such as 5G and cloud computing. The wide-ranging requests and lack of established standards in certain areas added layers of difficulty to the preparation and adoption processes, necessitating a multitude of stakeholders and phases to ensure alignment with existing policies and practices. Stakeholders confirmed the difficulty of converting an existing international certification mechanism (SOG-IS) into EU law and highlighted the need for more structured engagement in the framework through clear processes and realistic timelines. Despite these inefficiencies, several positive elements arose within the framework. The formation of dedicated groups and forums, including the ECCG, the Ad Hoc Working Group (AHWG) dedicated to specific schemes and the Stakeholder Cybersecurity Certification Group (SCCG), facilitated necessary stakeholder involvement. Nonetheless, there remains substantial room for improvement in ensuring these structures function optimally as, for example perceived lack of involvement of the SCCG members in the ECCF.

Refinement of internal governance is crucial to increase the active participation and strategic input of stakeholders.

## Coherence

### ENISA

In assessing ENISA's coherence, the evaluation highlights both strengths and areas for improvement. ENISA's commitment to fostering cybersecurity cooperation at the EU level is apparent, particularly through its facilitation and direct engagement with stakeholders. ENISA supported EU networks such as the CSIRTs network and EU-CyCLONe and facilitated the exchange of best practices through the NIS Cooperation Group and organised exercises such as CyberEurope. Despite some overlaps with national cybersecurity authorities and CERT-EU, ENISA's efforts were largely complementary, with effective exploitation of synergies and knowledge sharing. Survey data indicated that 74% of stakeholders overall agreed that ENISA sufficiently exploited synergies in expertise and knowledge sharing with other actors, with representatives of private bodies slightly less satisfied (65%).

This dual approach has enabled ENISA to significantly contribute to the cyber domain, aligning with recent legislative frameworks. However, while ENISA's role as a facilitator and coordinator is positive, several areas require improvement to enhance coherence. The evaluation identified the need to improve synergies between the responsibilities and actions of ENISA and other EU bodies such as the European Cybersecurity Competence Centre (ECCC), as well as national cybersecurity authorities. Although these roles are often complementary, opportunities exist to further streamline operations and improve organisational efficiency. By formalising cooperation arrangements with other entities, such as EMSA and the JRC, ENISA could better leverage synergies and ensure a unified approach to cybersecurity initiatives. Internal communication and resource management within ENISA should also be refined. ENISA's interaction with private stakeholders and international partners must be more predictable and transparent to maintain confidence and foster collaborative efforts. In this context, private entities, while considering ENISA's contribution beneficial, suggested that ENISA's stakeholder engagement activities could be improved, particularly in relation to collaboration with industry representatives and non-EU countries.

In alignment with the CRA and NIS2 Directive, a clear delineation of ENISA's tasks supporting policy implementation could increase efficiency and ensure consistency across regulatory measures. This clarity would also improve ENISA's ability to respond to sectoral regulatory requirements.

In summary, while ENISA has demonstrated a solid foundation in promoting cybersecurity coherence in the EU, there is potential for it to reprioritise its efforts. This approach will help it to efficiently fulfil its mandate and adapt to the evolving cybersecurity landscape. By addressing current inefficiencies and enhancing inter-agency coordination, ENISA can effectively maintain its crucial role within the EU's cybersecurity framework.

### ECCF

The ECCF's coherence is affected by the lack of clear accountability mechanisms, which has led to difficulties in aligning its objectives with other legislative measures. This

misalignment risks creating overlaps and inefficiencies in the cybersecurity landscape. To ensure a unified approach to cybersecurity, the ECCF needs to be completely coherent with other EU legislative instruments, including the NIS2 Directive and the CRA. In theory, the ECCF is aligned with these legislative measures, designed to address various facets of cybersecurity within the EU landscape, yet real-world integration remains complex and requires diligent oversight. The forthcoming implementation of the EUCC scheme poses a significant test for this coherence: if the scheme is successfully deployed, it will demonstrate the ECCF's ability to harmonise and effectively leverage additional legislative efforts. Stakeholders have emphasised the need for careful coordination between the ECCF and emerging regulatory acts to prevent potential overlaps which could undermine efficiency and dilute intended effects across sectors. Specifically, concerns arise regarding the interface between the ECCF and the CRA, as both initiatives aim to raise cybersecurity standards but risk redundancy if not fully synchronised. On the sectoral side, coherence must extend to accommodate continuing advancements in technologies, ensuring that cybersecurity initiatives are appropriately nuanced to address critical infrastructure needs.

Survey data showed that 83% of stakeholders found the ECCF to be coherent with other EU instruments, with 55% rating it as fairly coherent, 23% as very coherent and 5% as perfectly coherent. However, concerns remain about potential overlaps, particularly with the CRA, which could result in duplication of efforts and inconsistent requirements. More than half of respondents identified overlaps between the ECCF and other EU initiatives. Member States stressed the importance of ensuring coherent implementation of the CSA and CRA and highlighted the need to establish communication channels with international organisations to leverage existing European or international standards and prevent inconsistencies between standards developed at the EU and international levels.

### 4.2. How did the EU intervention make a difference and to whom?

**EU added value**

**ENISA**

ENISA has significantly contributed to enhancing the EU's cybersecurity ecosystem, yet there are opportunities for improvement that could amplify its impact. Serving as a centralised hub, ENISA has facilitated vital cooperation across the EU. It has complemented national efforts, especially in Member States with less developed cybersecurity infrastructures, and aligned cybersecurity practices and policies. Around two thirds of surveyed stakeholders considered that without ENISA, the collection and dissemination of relevant cybersecurity information, the generation of new knowledge, insights and evidence on cybersecurity issues and supporting the implementation of EU cybersecurity policies at the national level would be hard to achieve. Three quarters of respondents believed that without ENISA there would be little effect on improving Member States' cybersecurity capacities, as well as raising awareness of cybersecurity issues. As a decentralised EU Agency, ENISA's specialised mandate has allowed it to consolidate cybersecurity expertise and engage effectively with Member States, playing a pivotal role in shaping Europe's cybersecurity landscape. In this context, ENISA's main focus on Member States is essential, given its role in providing insights into emerging threats and recommending tools and strategies for addressing them.

Moreover, ENISA plays a critical part in promoting cybersecurity certification and supporting standardisation activities, which helps reduce market fragmentation and

fosters robust cybersecurity practices across the EU. Although no other similar bodies with ENISA's expertise and organisational agility exist, its current primary focus on national authorities has attracted criticism from private sector stakeholders. Feedback from large industry players indicates that more could be done to tailor insights to the private sector's specific challenges. Companies reported that they often relied on ISO/IEC standards rather than ENISA schemes. Some organisations valued ENISA's technical guidelines, tools and reports, although they claimed some of them were redundant with existing standards. Though the primary focus on national authorities is crucial, ENISA could address these concerns by strategically improving engagement with stakeholders and collaboration with the industry. Additionally, ENISA's mandate could benefit from strategically reassessing its priorities to adeptly adapt to evolving cybersecurity challenges. This would allow ENISA to maintain its valuable contributions to the EU, while effectively addressing the expanding needs of its varied stakeholders.

**Key achievements and challenges**

ENISA is widely recognised within the EU's cybersecurity community for its robust reputation, quality publications and significant role in fostering cooperation among Member States and other cybersecurity entities. ENISA's work on harmonising cybersecurity requirements is crucial in establishing a consistent level of protection across Member States, contributing directly to capacity building, especially for smaller Member States. This harmonisation not only ensures a secure digital environment across the EU but also elevates cybersecurity preparedness across its stakeholders.

However, the evaluation identified several challenges faced by ENISA. ENISA shows limited agility in responding to evolving cybersecurity threats which may lead to potential delays in its activities. To mitigate the problems of limited resources, the stakeholders[2] emphasised the need for improved recruitment processes and workload management strategies. Expanding ENISA's mandate to extend its operational role could address these concerns, allowing it to leverage technological advancements and improve cybersecurity frameworks. This restructuring would enable ENISA to proactively tackle dynamic threats, increasing its impact through joint training initiatives and making a contribution to policy-making processes.

Finally, ENISA's stakeholder consultation and management systems are deemed effective in facilitating management of stakeholder needs and expectations. However, a stronger, more transparent relationship with Member States is necessary to develop cooperation and information sharing. Future priorities include updating internal frameworks to better manage growing responsibilities and diverse challenges, ensuring that ENISA can fully implement its mandated tasks given its staff size.

**ECCF**

Despite its potential, the ECCF has struggled to deliver added value in fostering a unified and effective cybersecurity environment across the EU. The ECCF sought to significantly enhance the EU's cybersecurity landscape by introducing an unprecedented development procedure and governance structure for certification processes. At its core, the ECCF represented a critical advancement in the EU's ability to create a harmonised approach to the certification of ICT products, services, and processes. The inherent EU added value of this framework lies in its potential to bridge disparate national approaches, fostering an internal market with consistent, reliable, and recognised cybersecurity standards across Member States. However, the protracted timelines and

fragmented implementation have impeded the ECCF's ability to fully capitalise on its envisioned value. Specifically, the delay in actionable schemes, evidenced by the late adoption of initiatives like the EUCC, curtailed immediate impacts, leaving its theoretical potential largely unfulfilled.

The EUCC was adopted in January 2024, 4.5 years after the Commission request was introduced. Based on interviews with Commission, Member States and ENISA, this long timeframe of development and adoption can be attributed to a mix of factors. First, delay was caused by the lack of experience in developing and adopting schemes. Stakeholders confirmed the difficulty of translating the ENISA candidate scheme endorsed by the ECCG into an EU legal text both for the Commission draft implementing act and during the comitology procedure. Stakeholders also confirmed the difficulty of converting an existing intergovernmental certification mechanism (Senior Officials Group Information Systems Security – SOG-IS) into EU law that raised challenges related both to technical complexities and harmonisation with the repeal of national schemes. Moreover, the scheme was impacted by a shift in EU policy priorities due to the concurrent proposal of the CRA in September 2022, as well as by staff turnover and shortage from the Commission side.

The request for EUCS was introduced in November 2019 building on previous stakeholder-driven efforts that started in 2017. According to surveyed stakeholders, the adoption of the EUCS scheme was primarily impeded by issues related to its content and largely due to the politicisation of the debate, which contributed to divide Member States positions within the ECCG. As emerged from the call for evidence and confirmed by interviews with all relevant stakeholder categories (i.e. national authorities, EU institutions and agencies and industry), the discussions surrounding sovereignty concerns resulted in polarized discussion around the draft scheme in the institutional and public spheres. Furthermore, the situation around the EUCS triggered debates related to the scope of the ECCF as well as criticism from stakeholders regarding insufficient involvement in scheme development processes, due to a lack of transparency.

Disparities in systemic implementation, compounded by varying degrees of readiness and resource availability among Member States, further dilute the framework's comprehensive influence. Nevertheless, the ECCF has invigorated cooperative dynamics across the EU. By establishing groups such as the ECCG, it has institutionalised coordination efforts, enabling broader engagement across different governance levels. This collaborative infrastructure encourages information sharing and joint strategies, promoting a unified cybersecurity stance against evolving threats. While the direct influence of the ECCF is limited, stakeholders broadly agreed that the framework brings EU added value compared to what could have been achieved by Member States alone. 92% of stakeholders believed that Member States alone could not have achieved more streamlined and cost-effective certification processes, specifically in terms of uptake of certification, cost-effective processes, cyber-awareness, trust in the EU single market and cybersecurity by default and design. Most stakeholders recognise the added value of the ECCF in achieving a more secure, transparent and cohesive internal market for ICT products, services and processes. According to 88% of stakeholders, Member States alone might not be able (or able only in a limited way) to increase trust and awareness of citizens and businesses regarding the cybersecurity of ICT products, processes and services alone. This suggests the ECCF helps enhance trust.

For the ECCF to unlock its full EU added value, increased and concise stakeholder participation is critical. Fostering an inclusive environment where industry partners, national authorities, and EU bodies actively contribute to and guide the certification process will ensure widespread acceptance and effectiveness of cybersecurity standards.

**Key achievements and challenges**

The ECCF serves as a critical tool for enhancing EU-level collaboration between ENISA, Member States, and industries. Therefore, it has considerable relevance in the dynamic cybersecurity environment. Its adaptability facilitates scheme development through ad hoc working groups and aligns with EU legislative frameworks like NIS2. This potential, while significant, remains largely untapped due to limited implementation of actual schemes.

The ECCF is pivotal in addressing emerging cybersecurity threats and fostering compliance, particularly in leveraging new technologies such as artificial intelligence. Stakeholders acknowledge its role in strengthening cooperation among Member States and improving cybersecurity preparedness. Its value in fostering internal market exchanges, by replacing national certification schemes with EU-wide ones, is also recognised.

However, the ECCF is hampered by significant weaknesses. Lengthy processes for adopting schemes hinder its effectiveness, a challenge exacerbated by technical complexities and political pressures from industry lobbying. These delays undermine trust and prevent the swift adoption of standards. Opportunities exist for the ECCF to enhance EU cybersecurity frameworks, yet threats like resource constraints and geopolitical tensions pose challenges. Shifts in policy priorities and potential legislative overlaps could make the framework less effective, risking market inconsistencies. Addressing these issues is vital for ensuring the ECCF's evolution from a promising concept into a fully operational mechanism, bolstering EU cybersecurity standardisation and certification.

### 4.3. Is the intervention still relevant?

**Relevance**

**ENISA**

ENISA's relevance within the cybersecurity domain is also due to its responsiveness to evolving stakeholder needs and its flexibility to adapt to the changing landscape. ENISA has consistently demonstrated its ability to review and realign its areas of action to address emerging developments, thereby maintaining its position as a vital component in the EU's cybersecurity framework. For example, in 2020, ENISA established the Ad hoc Working Group on Artificial Intelligence Cybersecurity to address the growing need to map the AI threat landscape and develop security measures. In 2021, it set up an interdisciplinary working group on emerging and future cybersecurity challenges, integrating foresight into cybersecurity practices and increasing awareness of future threats.

While stakeholder satisfaction with ENISA's efforts is generally positive, 44% of the surveyed stakeholders and 50% of industry representatives indicated their needs were met only 'somewhat', 'to a small extent', or 'not at all' by ENISA's services and outputs. There are dimensions where its relevance can be further enhanced. Despite its responsive

nature, ENISA could still further improve support and increase visibility among diverse sectors and stakeholders, particularly for SMEs, which often struggle to adhere to cybersecurity requirements. A shift towards providing more direct tools and resources tailored to specific sectors but also providing insights in and tools to address emerging threats can increase ENISA's impact. ENISA's approach to stakeholder engagement was effective, utilising forums, committees and working groups to actively involve national experts in operations and publications. However, the complex decentralised structure within some Member States posed challenges that could be mitigated by better organisation and clearer coordination with national authorities. ENISA's ongoing initiatives, including the development of cybersecurity guidelines and capacity-building programmes, reflect its commitment to fostering cooperation and reinforcing the EU's collective cybersecurity posture. Stronger collaboration across industries and improved information access could address some limitations perceived by the industry sector.

What would really help ENISA to vastly improve would be re-evaluating priorities, streamlining processes, acquiring new appropriate resources and maximising existing resources efficiently, thereby reinforcing its foundational role in Europe's cybersecurity ecosystem. Through strategic alignment with the European cybersecurity strategy, ENISA's new priorities could create pathways towards contributions with greater impact. For ENISA to improve its capacity to provide policy and technical support, it might need to provide more resources, be more selective with its engagements and refine its operational focus areas. In conclusion, while ENISA's relevance is clear, there is still room for improvement.

**ECCF**

The ECCF has emerged as a crucial response to the growing complexity and sophistication of cyber threats across the EU. It aspires to establish harmonised cybersecurity certification schemes that ensure trust and foster a secure digital market. Despite its promising premise, the framework's relevance is still considered more potential than practical, with certification schemes only recently entering the operational phase. The lack of tangible results so far is a sign that implementation is uneven and means the ECCF's current standing in the cybersecurity landscape is uncertain. The significance of the ECCF lies in its strategic role in raising cybersecurity standards and enabling mutual recognition of certifications across Member States, thereby reducing individual enterprise costs and strengthening the internal market. The ECCF seeks robust integration with other EU legal acts, aiming to streamline procedures and facilitate cross-border trade. Yet the protracted timeline for scheme deployment and the discrepancy in expertise and resources among Member States make it much harder for the ECCF to realise its full potential. These challenges hinder collaborative efforts and impede the standardisation process that is central to the ECCF's mission.

Despite these challenges, there are several factors ensuring the ECCF's relevance. One is that the surge in cyber threats intensifies the need for a united cybersecurity strategy that can adapt swiftly to changing scenarios, such as the increased relevance of certification in high-assurance areas like cloud services and 5G infrastructures. Public procurement mandates in these sectors reflect the growing demand for a unified and reliable certification framework that the ECCF can fulfil. Furthermore, the ECCF is linked to emerging legislative acts, notably the CRA and NIS2 Directive, which points to its value in addressing critical infrastructure needs and legal conformity across the EU. ENISA's proactive role and the establishment of NCCAs mark crucial milestones towards strengthening collaborative interactions and promoting certification adoption. However,

there are considerable differences between larger and smaller Member States when it comes to resource allocation and expertise, meaning continued imbalances in participation and effectiveness that impact the development of a collective scheme.

In conclusion, the evaluation finds that EU action has delivered relevant benefits in strengthening the cybersecurity landscape across the EU. ENISA has established itself as a centre of expertise, a facilitator of cooperation and a key contributor to policy development and capacity building, particularly for Member States with less developed cybersecurity capabilities. The ECCF, while still in the early stages of implementation, has laid the groundwork for harmonised certification and increased trust in digital products and services. However, both ENISA and ECCF have faced significant challenges, including resource constraints, delays in scheme adoption and the complexity of aligning with a rapidly evolving legislative and technological environment. Despite these obstacles, they remain highly relevant and continue to provide clear EU added value, especially in fostering cross-border cooperation, supporting SMEs and addressing emerging threats. The findings highlight the need for ongoing adaptation, increased resources and enhanced stakeholder engagement to ensure that the EU's cybersecurity framework remains effective, efficient and fit for future challenges.

## 5. WHAT ARE THE CONCLUSIONS AND LESSONS LEARNED?

This chapter synthesises the main conclusions and lessons learned from the evaluation of EU action on cybersecurity, focusing on ENISA and the ECCF. It provides policy-relevant insights for future development while staying within the limits of a staff working document. The conclusions are based on a systematic screening of evidence from performance data, stakeholder consultations and targeted workshops, highlighting what has worked, what remains uncertain and where challenges persist. Lessons learned are presented as part of the narrative, with attention to regulatory simplification and burden reduction.

### 5.1. Conclusions

The evaluation of ENISA highlights its crucial role in working towards a cohesive cybersecurity landscape across the EU. Although ENISA has shown effectiveness in parts of its mandate and generating valuable outputs, there remains significant room for improvement in handling external disruptions and meeting stakeholder expectations consistently. As demands on ENISA continue to grow, it is important to reassess its mandate and resources to better align it with priorities, with continued emphasis on supporting Member States as they address cybersecurity threats and improve their national cybersecurity infrastructures. Making ENISA more effective would require refinement of its report production process, making reports more tailored to stakeholder needs as well as more user-friendly and accessible through visual aids and concise summaries. Strengthening communication channels is essential to ensure ENISA's activities and services are clearly visible to stakeholders, including industry players. A well-defined communication strategy will aid in fostering stronger connections and cooperation within existing cybersecurity networks such as ISACs.

ENISA can become more efficient through a more strategic focus on task prioritisation, enabling a more streamlined approach to managing workload pressures. To become more relevant to stakeholders, ENISA should continue to expand its central role in supporting Member States by strengthening its capacity to provide timely insights into emerging threats and strategic tools for addressing them. Moreover, as a number of stakeholders noted, ENISA could establish more structured and transparent methods of engaging with private entities, with an emphasis on supporting SMEs. Clarity should be sought regarding ENISA's role in policy implementation with other EU institutions, ensuring that collaboration with Member States is at the forefront of these efforts to reinforce the cohesion of the EU's unified cybersecurity strategy, which would also include strengthening cooperation with other EU agencies and seeking synergies with other cybersecurity bodies for joint actions to improve operational coherence across Europe.

Overall, maintaining ENISA's status as a specialised agency within the EU framework is important, as it ensures continued focus on cybersecurity priorities.

The ECCF has partially achieved its objectives. It has succeeded in improving cooperation and coordination among Member States, EU institutions and the private sector, notably through the creation of forums such as the ECCG and to a lesser extent, the SCCG. These structures have facilitated knowledge sharing and harmonisation, but delays in the adoption of certification schemes, most notably the EUCC, which took nearly five years to implement, have limited ECCF's impact on market fragmentation, trust and transparency. The lack of implemented schemes means that many of ECCF's

strengths remain ‘potential’ rather than realised and the benefits for businesses and citizens are yet to materialise.

The evaluation finds that the EU’s role has been essential in bringing together diverse actors to work on shared solutions that would not have been possible at national level. ENISA’s decentralised structure and the ECCF’s harmonised approach have enabled economies of scale and safeguarded key EU interests in cybersecurity. Stakeholders consistently noted that, without EU involvement, coordination, expertise development and cross-border cooperation would be significantly weaker, leading to fragmented approaches and increased costs.

Unintended effects have also emerged. The politicisation of debates around certification schemes (e.g. cloud sovereignty requirements) has led to delays and decreased trust among stakeholders. Nevertheless, the overall impact of the action remains positive, with stakeholders recognising the need for continued adaptation and coordination.

In terms of regulatory simplification and burden reduction (REFIT), the evaluation highlights the importance of streamlining reporting requirements, improving communication channels and making ENISA’s outputs more accessible and tailored to stakeholder needs. Stakeholders suggested that more concise, practical reports and greater use of visualisations would enhance effectiveness and reduce unnecessary complexity.

### 5.2. Lessons learned

The evaluation yields several lessons that are relevant for future policy development, while acknowledging that some findings remain preliminary and require ongoing monitoring.

First, ENISA’s expanding mandate and the evolving cybersecurity landscape would benefit from a **flexible approach to resource allocation and prioritisation**. ENISA’s effectiveness depends on its ability to match its growing responsibilities with adequate human and financial resources. Lessons from stakeholder consultations indicate that secondment of national officials, partnerships with academic institutions and targeted recruitment programmes could go some way to addressing resource gaps and improving capacity.

Second, the **quality of stakeholder engagement** is a critical determinant of success. ENISA’s effectiveness, efficiency and relevance are closely linked to its relationships with Member States, EU institutions and industry. The evaluation suggests that ENISA could further develop its cooperation strategies, including clearer communication campaigns, more structured engagement with industry (especially SMEs) and improved feedback mechanisms.

Third, the ECCF’s experience highlights the importance of having **clear roles and responsibilities in scheme implementation and maintenance**. Despite ENISA’s pivotal role in fostering cooperation and operational cohesiveness among Member States and other stakeholders, constraints on the efficiency and effectiveness of the ECCF have been evident, mainly due to the complexities of scheme adoption processes. These issues highlight the necessity of a substantial revision in governance structures to improve operational clarity and accountability at all levels. The evaluation also points to the

importance for more granular scheme requests, early preparatory analysis and regular updates to work programmes to align expectations and smoothen adoption processes.

Fourth, developing **streamlined decision-making processes** within the ECCF which clarify roles and responsibilities will promote transparency and efficiency, particularly in collaborative efforts among Member States, the Commission, and ENISA. This will foster accountability and reduce inefficiencies.

Fifth, a commitment to **setting and adhering to realistic timelines** for the development and implementation of certification schemes is essential. This involves supporting detailed technical analysis and bolstering preparatory efforts to effectively anticipate and mitigate political influences.

Sixth, actively investing in the **training and retention of skilled personnel** within ENISA is crucial to ensuring continuity and expertise when navigating complex cybersecurity challenges. Long-term workforce stability will be vital to maintaining the ECCF's operational efficacy.

Seventh, industry and consumer **awareness about the ECCF could be increased** through targeted campaigns and strategic involvement, emphasising the value of certified products and services. A proactive approach to garnering stakeholder support is critical to boosting demand and trust in ECCF initiatives.

Eighth, the relevance and **added value of these efforts remain 'potential'** until schemes are fully implemented and maintained. Promoting uptake among industry, raising awareness among consumers and linking scheme planning to threat monitoring and legislative developments are essential for realising the full benefits of the ECCF.

Finally, the evaluation identifies opportunities for **regulatory simplification and burden reduction**. Streamlining administrative processes, clarifying terminology and harmonising requirements across legislative acts can help reduce unnecessary complexity and improve efficiency. Stakeholders emphasised the value of voluntary approaches, clear guidance documents and coordinated implementation to avoid overlaps and ensure coherence.

Some findings, such as the long-term impact of new certification schemes and the effectiveness of market surveillance, are too preliminary to draw firm conclusions and warrant a 'wait and see' approach. Ongoing monitoring and stakeholder engagement will be necessary to assess whether these issues resolve themselves over time or require further intervention.

## 6. ANNEX I: PROCEDURAL INFORMATION

### 6.1. Lead DG, Decide Planning/CWP references

Lead DG: Directorate-General for Communications Networks Content and Technology (CNECT).

Decide: PLAN/2023/181

Evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework

### 6.2. Organisation and timing

14 July 2023 - 4 December 2024 – The call for evidence was launched on 14 July 2023 (see below) and the final study report was delivered on 4 December 2024 (see below).

### 6.3. Consultation of the RSB

N/A

### 6.4. Evidence, sources and quality

Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework according to Regulation (EU) 2019/881 – STUDY 2023/037, carried out for the European Commission by PwC EU Services EESV, Open Evidence S.L. and PPMI Group, UAB – Final report 4 December 2024

A call for evidence on the impact, effectiveness and efficiency of ENISA's mandate and of the provisions of the European Cybersecurity Certification Framework (ECCF) was conducted from 14 July 2023 to 16 September 2023. The call for evidence was intended to elicit feedback from relevant stakeholders involved in the cybersecurity domain, and, more specifically, from those involved in the EU certification process. Overall, 41 stakeholders contributed to the call for evidence, mostly from the private sector.

## 7. ANNEX II. METHODOLOGY AND ANALYTICAL MODELS USED

*Provide a critical assessment of the work carried out by the external contractor which allows an understanding of why you agreed or disagreed with their conclusions.*

This annex provides a detailed account of the methodology and analytical approaches used in the evaluation of ENISA and the ECCF, as documented in the 2024 ENISA and ECCF Evaluation Report. This annex explains the data collection process, sources and stakeholder consultation activities, as well as the analytical techniques and validation steps applied throughout the evaluation. It also addresses any changes from the original plan, known limitations and the measures taken to ensure the reliability and robustness of the findings. The information presented here is intended to ensure full transparency and to support the credibility of the conclusions of the evaluation.

### 7.1. Overview and process

The evaluation of ENISA and the ECCF was conducted through a comprehensive, multi-method approach designed to ensure transparency, robustness and stakeholder engagement at every stage. The study was carried out by an external contractor, with close involvement and oversight from the European Commission. All planned activities, including surveys, interviews, workshops and desk research, were completed as scheduled, with only minor adaptations to the original plan as set out in the evaluation roadmap. Where challenges arose, such as difficulties in engaging certain stakeholder groups, mitigating measures were implemented to ensure the integrity and completeness of the evidence base.

### 7.2. Data collection and sources

**Desk research and administrative data**

Administrative and monitoring data provided by ENISA and the Commission formed the cornerstone of the evaluation. These data were used to assess the efficiency of ENISA, triangulate stakeholder perspectives and provide a factual basis for answering the evaluation questions. Internal documents, including minutes, reports and audits, were systematically reviewed to complement and validate findings from other sources.

For the ECCF, the evaluation focused on legislative texts, notably the Cybersecurity Act and its amendments, as well as new legislative documents such as the NIS2 Directive, CRA and the Union Rolling Work Programme (URWP). The Commission's call for evidence on the ECCF was also analysed, with particular attention to feedback from SCCG members.

**Document and literature review**

The literature review drew primarily on official documents published by ENISA and the European Commission, including eleven official reports, three studies and relevant website publications. Annual activity reports with annexes were extensively used to assess ENISA's performance. For certification schemes, published draft schemes for the EUCC and EUCS were reviewed to understand the state of play and barriers to adoption.

**Academic literature review**

Academic research was used to situate the evaluation within the broader European cybersecurity debate and to inform the initial focus of data collection. The literature provided critical perspectives on ENISA's epistemic authority, the challenges and vulnerabilities of the European cybersecurity domain and the alignment of the ECCF with international standards and best practices. Comparative studies with other certification schemes were also reviewed to assess the competitiveness and adaptability of the ECCF.

### 7.3. Stakeholder consultation

**Interview programme**

The interview programme was a central pillar of the evaluation, designed to capture a wide range of perspectives from across the EU cybersecurity ecosystem. In total, 182 individuals were contacted (40 for ECCF, 142 for ENISA), resulting in 52 interviews for ENISA and 13 for ECCF. All interviews included questions on both ENISA and ECCF and 19 stakeholders were selected from survey respondents who volunteered for interviews.

**ENISA:** 52 interviews were conducted, involving ENISA staff, representatives from DG CNECT, DIGIT, INTPA, NEAR, other EU entities, industry, academia, international representatives and Member State officials.

**ECCF:** 13 interviews were conducted with 31 interviewees, including EU institutions, ECCG members and SCCG members. Despite challenges in engaging private stakeholders (only three of nine SCCG members responded), the analysis of stakeholder consultation data helped offset this limitation.

**Survey programme**

The survey approach was adapted after the inception report: instead of two separate surveys for internal and external stakeholders, an integrated survey was conducted to address all stakeholder groups. The survey included specific sections on ENISA and the ECCF, with question filtering and branching to ensure relevance.

- **Design:** The survey was developed based on desk research and initial interviews. It included both closed and open questions, with a limited number of mandatory items.
- **Dissemination:** Conducted via EUSurvey, 856 stakeholders received a personal invitation. The Commission and ENISA promoted the survey through various channels and the deadline was extended to maximise responses.
- **Results:** 209 responses were collected, with 70 respondents (33%) involved with the ECCF. The survey results were analysed using data science and analytics software, supplemented by manual analysis.

### 7.4. Workshops and validation activities

**SWOT and recommendations workshops**

SWOT workshop: held online on 21 May 2024 with 32 participants, including experts from academia, ENISA and the Commission. The workshop aimed to develop a SWOT analysis for ENISA and the ECCF, validate preliminary findings and foster technical exchange. Interactive polling and breakout sessions were used to gather and validate stakeholder input.

The results were used to refine the strengths, weaknesses, opportunities and threats identified for both ENISA and the ECCF.

Recommendations workshop: held online on 12 July 2024 with 77 participants. The workshop presented preliminary evaluation results and facilitated collaborative discussions on lessons learned and potential improvements for ENISA and the ECCF. Interactive polls and an anonymous form to be filled by each Member State were used to collect feedback and validate findings.

**Validation and quality assurance**

The evaluation process included multiple validation steps to ensure the reliability and robustness of the findings:

- preliminary findings were presented to stakeholders in workshops, where interactive polling and open discussion allowed for real-time validation and refinement;
- an anonymous asynchronous feedback form was provided to capture additional input from stakeholders unable to participate in real time;
- the iterative process of presenting, discussing and refining findings ensured that the analysis accurately reflected the collective insights and perspectives of all participants.

### 7.5. Analytical approaches and quality assurance

The evaluation combined qualitative and quantitative methods, including desk research, literature review, stakeholder interviews, surveys and workshops. Data analysis was supported by analytics software and manual review. Quality was ensured through:

- iterative validation with stakeholders and expert input during workshops;
- systematic triangulation of data sources to cross-check findings;
- adaptation of tools (e.g. survey design) to maximise relevance and response rates.

### 7.6. Limitations and mitigating measures

- **Data and timing:** the main limitation was the difficulty in securing interviews with private stakeholders, particularly SCCG members. This was mitigated by analysing stakeholders' consultation data and extending the survey deadline.
- **Reliability:** the use of multiple data sources and triangulation of findings enhanced the reliability of the evaluation. Validation through stakeholder workshops and polling further strengthened the robustness of the conclusions.
- **Uncertainty:** some results, especially regarding the ECCF (where only one scheme was adopted by early 2024), are preliminary. The robustness of findings was enhanced by cross-referencing multiple sources and validating with stakeholders, but some uncertainty remains due to the evolving nature of the policy landscape.

### 7.7. Points of comparison

The main point of comparison for the evaluation was the baseline scenario of 2017, reconstructed from the 2017 Impact Assessment for the Cybersecurity Act and supporting studies. This baseline included ENISA's status and resources, the certification landscape,

market and economic data and stakeholder perceptions. All comparisons and assessments were made against this baseline, as set out in the original evaluation roadmap.

### 7.8. Critical assessment of the contractor

The contractor's evaluation of ENISA demonstrated a certain positive bias, largely attributed to interviews with ENISA staff constituting a significant part of the interviews overall. While the report rightly acknowledges ENISA's resource constraints, the analysis could be more balanced regarding other areas for improvement. The study was improved following feedback from DG CONNECT in several instances.

# 8. ANNEX III. EVALUATION MATRIX AND, WHERE RELEVANT, DETAILS ON ANSWERS TO THE EVALUATION QUESTIONS (BY CRITERION)

This annex presents the evaluation matrix that serves as the central organising framework for the assessment of ENISA and the ECCF. It provides detailed, criterion-based responses to the evaluation questions, covering all five evaluation criteria: **effectiveness**, **efficiency**, **coherence, relevance** and **EU added value**.

The evidence and analysis included in this annex substantiate the findings outlined in Section 4 of the main evaluation report. For clarity and transparency, the questions and their corresponding evidence-based answers are presented individually and grouped by evaluation criterion. The depth of coverage for each criterion reflects its relative importance and the extent of supporting evidence available in the main body of the report.

Findings are presented separately for ENISA and the ECCF to reflect their distinct roles and contributions within the broader cybersecurity landscape.



## 8.1. Evaluation matrix:

The following sections present refined and up-to-date evaluation matrices used to assess the effectiveness, impact, efficiency, coherence, relevance and EU added value of both ENISA and the ECCF. These matrices are aligned with the latest edition of the European Commission's Better Regulation Guidelines and outline the evaluation questions (EQs) and operational questions (OQs), along with the corresponding judgement criteria, stakeholder groups and indicators used to evaluate each criterion.

The matrices also specify the data sources required to determine the values of the proposed indicators. Certain EQs and OQs have been specifically designed to address aspects unique to the ECCF.

Functioning as a structured analytical tool, the evaluation matrices demonstrate how evidence collected through various methodologies and data sources contributes to answering the evaluation questions and shaping the overall conclusions.

### 8.1.1. *Effectiveness and impact*

In line with the Better Regulation Toolbox, the effectiveness analysis examined how successfully ENISA and the ECCF have achieved or made progress toward their intended objectives. This involved assessing the actual outputs, results and impacts in relation to the goals of the action.

The effectiveness analysis yielded insights into the progress made so far by ENISA and the ECCF. The evaluation drew heavily on the intervention logic of both entities.

The tables below illustrate the structure of the evaluation matrix. Where appropriate, findings are presented separately for ENISA and the ECCF.

**ENISA**

| | |
|---|---|
| ***Effectiveness***<br><br>**EQ1, ENISA** | **To what extent has ENISA achieved its objectives and implemented the tasks set out in its mandate? What, if anything, could be done to render ENISA more effective in achieving these objectives?** |
| **OPERATIONAL QUESTIONS**<br><br>▪ OQ1: Did the activities of ENISA result in the expected outputs? To what extent were the stakeholders satisfied with their quality?<br>▪ OQ2: To what extent has ENISA become a centre of expertise on cybersecurity? Where relevant, what were the main factors limiting ENISA's contribution to this objective?<br>▪ OQ3: To what extent has ENISA provided guidance, advice and assistance on cybersecurity policy development and implementation for MS and EU institutions? To what extent have ENISA's stakeholders followed the cybersecurity requirements issued by ENISA?<br>▪ OQ4: To what extent has ENISA enhanced MS capabilities in preventing and responding to cyber threats? Where relevant, what were the main factors limiting ENISA's contribution to this objective?<br>▪ OQ5: To what extent has ENISA's reputation in cybersecurity matters remained stable? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: Successful implementation of activities and delivery of outputs as a key precondition for achieving objectives | Number and share of successfully implemented activities and delivered outputs |
| OQ2: Stakeholders identify ENISA as a leading centre of expertise on cybersecurity | Share of stakeholders by group that considers ENISA to be a leading centre of expertise on cybersecurity |

| | |
|---|---|
| OQ3: Stakeholders identify ENISA as a leading partner in cybersecurity policy development and implementation | Share of stakeholders by group that considers ENISA to be a leading partner in cybersecurity policy development and implementation<br><br>Share of stakeholders that adopted regulatory or managerial change as a result of ENISA's support |
| OQ4: MS representatives agree that ENISA provided crucial support in preventing and responding to cyber threats, including via the Cybersecurity Support Action | Share of MS representatives by country that considers ENISA to be a crucial provider of cybersecurity support in preventing and responding to cyber threats<br><br>Share of MS stakeholders that considers the Cybersecurity Support Action effective; number and share of completed *ex ante* and *ex post* activities |
| OQ5: ENISA's reputation remained stable over the evaluation period | Perceptions of stakeholders about ENISA's work (two thirds of stakeholders assess ENISA's reputation in a positive way) |
| **DATA SOURCES**<br><br>▪ Desk research<br>▪ Interviews<br>▪ Survey<br>▪ Case studies<br>▪ Workshop on the intervention logic | |

| | |
|---|---|
| ***Effectiveness***<br><br>**EQ2, ENISA** | **To what extent has the governance framework been effective?** |
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: How effectively have the current governance, internal organisational structure and human resources policies and practices of ENISA contributed to its effectiveness?<br>▪ OQ2: Were the internal mechanisms for programming, monitoring, reporting and evaluating ENISA effective? | |

| JUDGEMENT CRITERIA AND INDICATORS | |
|---|---|
| OQ1: ENISA's governance structure is conducive to the effectiveness of its work | ENISA's stakeholders consider its governance structure effective; ENISA fulfils its annual activities and objectives and complies with the management target scores |
| OQ2: The internal mechanisms for programming, monitoring, reporting and evaluating ENISA were effective | ENISA follows rules and procedures imposed by the Commission; ENISA staff considers the monitoring system effective; EC officials consider ENISA's internal monitoring system effective |
| ▪ **DATA SOURCES**<br>▪ Desk research<br>▪ Interviews<br>▪ Survey | |



| Evaluation results |
|---|
| ENISA successfully fulfilled its mandate by delivering most planned outputs, even during challenging times like the COVID-19 pandemic and Russia's war of aggression against Ukraine. ENISA's effectiveness is largely due to its strong governance and matrix-based organisational model, which aids task delivery and cooperation. However, key areas for improvement have been identified, particularly in strategic prioritisation and resource allocation. Despite a solid governance structure, ENISA experiences delays due to resource constraints and rigid strategic plans, signalling a need for more agile management. Enhancing task prioritisation and aligning operational capacity with strategic objectives could bolster ENISA's efficiency and responsiveness to emergent cybersecurity challenges. The evaluation shows the need for additional resources. Additionally, more streamlined internal governance and dynamic reallocation of tasks and resources could help, to a certain extent, with timely fulfilment of new requests. Lastly, strengthened communication channels and a better-defined communication strategy would support ENISA's outreach to its public and private stakeholders. |

## ECCF

| *Effectiveness* | **To what extent has the ECCF achieved its objectives?** |
|---|---|

| EQ3, ECCF | |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent has the ECCF increased capabilities and preparedness of Member States and businesses, in particular regarding critical infrastructures?<br>▪ OQ2: To what extent has the ECCF improved cooperation and coordination across Member States and EU institutions, agencies and bodies as well as well as with other relevant stakeholders (e.g. industry, standardisation bodies)?<br>▪ OQ3: To what extent has the ECCF improved EU-level capabilities to support and complement the action of Member States?<br>▪ OQ4: To what extent has the ECCF enhanced trust and awareness among the general public and businesses on cybersecurity issues through transparent information?<br>▪ OQ5: To what extent has the ECCF increased the overall transparency of cybersecurity assurance of ICT products and services, ensuring security by default and design as well as mitigation of vulnerabilities?<br>▪ OQ6: To what extent has the ECCF ensured that businesses can sell secure ICT products, services and processes across the internal market at lower administrative and financial costs?<br>▪ OQ7: To what extent has the ECCF reduced fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: All Member States appointed national cybersecurity certification authorities | Number of national cybersecurity certification authorities appointed; resources allocated to national cybersecurity certification authorities |
| OQ1: ICT products, services or processes certified under the EU cybersecurity certification schemes | Number of certification schemes issued and businesses certified |
| OQ2: ECCG set up and taking decisions | Number of ECCG meetings that took place; type of issues discussed; number and type of decisions taken and documents adopted |
| OQ2: Certificates issued under the 'Senior Officials Group Information Systems Security - Mutual Recognition Agreement' (SOG-IS-MRA) extended to the EU27 in view of an equivalent EU scheme | Number of SOGIS-MRA equivalent schemes at EU level, extended to EU27; number and type of decisions taken and documents adopted by the SOG-IS MRA and transferred to EU level |
| OQ3: ENISA has more resources to tackle cybersecurity certification issues | Resources effectively allocated to ENISA (number of staff and financial endowment) to carry out certification-related tasks |

| | |
|---|---|
| OQ4: More people and businesses know about cybersecurity certification | Percentage of the general public and businesses aware of cybersecurity certification; percentage of the general public and businesses aware of the importance of a high level of security of ICT products, services and processes |
| OQ5: Buyers, in particular operators of essential services, are more incentivised to purchase certified ICT products, services and processes compared to before the Cybersecurity Act | Extent to which the ECCF has contributed to the purchase of certified ICT products, services and processes |
| OQ6: Vendors are more incentivised to certify their ICT products, services and processes compared to before the Cybersecurity Act | Extent to which the ECCF has contributed to the certification of ICT products, services and processes |
| OQ7: Less or no cybersecurity certification schemes were developed outside the perimeter of the ECCF compared to before its adoption | Number and type of cybersecurity certification schemes developed outside the ECCF perimeter |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey<br>▪ Workshop on the intervention logic | |



| ***Effectiveness***<br><br>**EQ4, ECCF** | **What are the main gaps and challenges that have hindered the achievement of the objectives of the ECCF? Why?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: Which administrative shortcomings have prevented the ECCF from achieving its objectives? Did these shortcomings appear or increase during the COVID-19 pandemic, following geopolitical tensions or the emergence of other EU policy priorities?<br>▪ OQ2: Which legal shortcomings have prevented the ECCF from achieving its objectives? Did these shortcomings appear or increase during the COVID-19 pandemic, following geopolitical tensions or the emergence of other EU policy priorities?<br>▪ OQ3: Which operational shortcomings have prevented the ECCF from achieving its objectives? Did these shortcomings appear or increase during the COVID-19 pandemic, following geopolitical tensions or the emergence of other EU policy priorities? | |

| JUDGEMENT CRITERIA AND INDICATORS | |
|---|---|
| OQ1: Administrative barriers, such as time-consuming procedures and lack of effective decision-making tools as well as conflicting national certification procedures/requests | Number of administrative procedures initiated and finalised; type of shortcomings in decision-making highlighted by participants in the ECCF (in particular ENISA, Member States and the Commission) |
| OQ2: Legal barriers, such as national legal frameworks and requirements hindering the adoption of EU cybersecurity certification schemes | Number of initiated and finalised legal acts, including implementing law, at both EU and national level; type of shortcomings highlighted by participants in the ECCF (in particular ENISA, Member States and the Commission, SCCG members) |
| OQ3: Operational barriers, such as the lack of online platforms and adequate collaboration tools | Number and type of exchanges allowed by existing collaboration tools; type of shortcomings in operational tools highlighted by participants in the ECCF (in particular ENISA, Member States and the Commission) |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| *Evaluation results* |
|---|
| The ECCF made a modest contribution to enhancing the cybersecurity capabilities of Member States and private companies. National authorities recognised the ECCF's support in developing national cybersecurity certification capabilities but highlighted significant resource disparities between Member States. ENISA reported staffing difficulties, mainly related to turnover and the limited number of personnel available to carry out all activities arising from new schemes, including in Member States. Delays in the adoption of certification schemes caused by disagreements between Member States, legal complications, politicisation and coordination issues, negatively affected the ECCF's effectiveness, thus impacting the achievement of its objectives. Despite these obstacles, the ECCF strengthened cooperation and coordination between Member States and EU institutions in cybersecurity certification. |

### 8.1.2. *Efficiency*

Efficiency-related questions examine the resources invested in relation to the changes generated by the measure. This involves assessing the inputs against the outputs, results and impacts, essentially weighing costs against benefits. The efficiency evaluation explored the costs associated with the EU measure as they affect various stakeholder groups, along with the factors influencing these costs and their connection to ENISA and the ECCF.

This evaluation was conducted based on the outcomes experienced by different stakeholder groups, as identified in the effectiveness analysis. Where feasible, these outputs were quantified. The analysis also acknowledged that while costs may initially outweigh benefits, net benefits could emerge over time, particularly given ENISA's recently extended mandate and the early-stage development of the ECCF.

The overall conclusions drawn from the efficiency questions provided insight into whether the resources allocated to ENISA's activities and the implementation of the ECCF are being used optimally and are necessary to achieve the measure's objectives. Where findings indicated inefficiencies, opportunities for simplification and burden reduction were identified and examined. Where applicable, the evaluation also highlighted areas with the potential for improving efficiency and streamlining the design and implementation of the measure.

The tables below outline the structure of the evaluation matrix. Findings are presented separately for ENISA and the ECCF.

**ENISA**

| ***Efficiency***<br>**EQ1, ENISA** | **To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: Have the resources allocated to ENISA been sufficient for the pursuit of its tasks (input/output analysis)? To what extent has the execution of the tasks been effectively resourced?<br>▪ OQ2: Were the annual budgets of ENISA implemented in an efficient way considering the results achieved? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The extent to which the resources allocated to ENISA have been sufficient for the pursuit of its individual tasks | Title II commitment and paid budget share; opinions of ENISA staff and EC officials on the extent to which individual tasks were effectively resourced |
| OQ2: The annual budget of ENISA has been implemented efficiently | ENISA commitment and paid budget; annual budget implementation targets |
| **DATA SOURCES** | |
| ▪ Desk research | |

| |
|---|
| ▪ Interviews |

| *Efficiency*<br>**EQ2, ENISA** | **To what extent has ENISA adapted to periods of high workload?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: What were the periods of high workload during the evaluation period?<br>▪ OQ2: Did ENISA manage to carry on with all their tasks during these periods? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The high workload periods identified | The periods of high workload are analysed where relevant |
| OQ2: Tasks were implemented during the period of high workload | Findings of other evaluation questions indicate that ENISA kept performing its tasks during the period of high workload |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| *Efficiency*<br>**EQ3, ENISA** | **To what extent have ENISA's internal organisation, governance and procedures been conducive to its efficiency and what administrative costs and burdens do they create and for whom?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent do ENISA's internal organisation, governance and procedures support its ability to perform its tasks, given its mandate and size?<br>▪ OQ2: How does the balance of operational staff and administrative support staff affect the implementation of ENISA's tasks and the achievement of its objectives? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The extent to which ENISA's internal organisation, governance and procedures are fit for purpose without excessive costs and major administrative burdens | Alignment of ENISA's internal organisation, governance and procedures with its mandate and size; the volume of administrative costs and administrative burdens; IAS and ECA opinions on the governance of ENISA |
| OQ2: The balance between operational and administrative support staff is appropriate | Number and share of administrative and operational staff; staff performance management indicators; qualitative opinion of interviewed staff members |
| **DATA SOURCES** | |
| ▪ Desk research | |

| |
|---|
| ▪ Interviews<br>▪ Survey |

| *Efficiency*<br>**EQ4, ENISA** | **What aspects, means, actors or processes render ENISA more or less efficient?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: What are the inefficiencies identified in ENISA's activities?<br>▪ OQ2: Which of ENISA's activities are particularly efficiently or inefficiently implemented? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: ENISA addressed all identified inefficiencies | Findings on the previous efficiency questions and stakeholder perceptions |
| OQ2: Good and bad practices identified in the selected activities | |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Case studies | |

| ***Evaluation results*** |
|---|
| The evaluation highlighted that while ENISA operated efficiently under its governance structure, it struggled with increasing demands and filling specialised positions due to a global IT and cybersecurity specialist shortage and insufficient resources, resulting in task delays and periods of high stress for personnel. Improvements can be made to a certain extent by optimising internal workforce management to handle critical tasks, as demonstrated by reallocating 10.5 FTEs for the Cybersecurity Support Action. Additionally, enhancing budget and procurement management could improve internal efficiency and address the downward trend in balancing appropriations. Although ENISA's budget grew significantly between 2017 and 2023, it continued to face resource constraints that impacted its operational efficiency. |

## ECCF

| *Efficiency*<br>**EQ5, ECCF** | **To what extent has the ECCF been implemented efficiently?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |

- OQ1: What benefits have been experienced by Member States since the establishment of the ECCF?
- OQ2: What costs have been borne at national level since the establishment of the ECCF?
- OQ3: What benefits have been experienced at EU level (i.e. Commission, ENISA) since the establishment of the ECCF?
- OQ3: What costs have been borne at EU level (i.e. Commission, ENISA) since the establishment of the ECCF?
- OQ4: What benefits have been experienced by businesses and the general public since the establishment of the ECCF?

**JUDGEMENT CRITERIA AND INDICATORS**

| | |
|---|---|
| OQ1: Member States confirm they experienced a set of benefits as a result of participating in the ECCF, especially compared to SOG-IS-MRA | Benefits from participating in, and issuing certificates valid under, the SOG-IS-MRA; benefits from participating in the ECCF |
| OQ2: Member States confirm they incurred a set of costs as a result of participating in the ECCF | Costs, including administrative and human resources costs, borne as a result of implementing the ECCF at national level (Member States), including the establishment of national certification authorities |
| OQ3: Commission and ENISA confirm they experienced a set of benefits as a result of participating in the ECCF, especially compared to SOG-IS-MRA | Benefits from participating in, preparing and adopting certification schemes |
| OQ3: Commission and ENISA confirm they incurred a set of costs as a result of participating in the ECCF | Costs, including administrative and human resources costs, borne as a result of implementing the ECCF at EU level (Commission, ENISA) |
| OQ4: Businesses and the general public confirm they experienced a set of benefits deriving from the ECCF | Benefits in terms of competitiveness for businesses; benefits in terms of more awareness for the general public |

**DATA SOURCES**

- Desk research
- Interviews
- Survey

| *Efficiency*<br><br>**EQ6, ECCF** | **What aspects, means, actors or processes render the ECCF more or less efficient?** |
|---|---|

**OPERATIONAL QUESTIONS**

- OQ1: What are the inefficiencies identified in the ECCF's processes or outputs?
- OQ2: What ECCF activities or processes are particularly efficiently implemented? To what extent have the adoption of the Union Rolling Work Programme, the preparation of schemes carried out by ENISA, the opinions provided by the ECCG, advice provided by the SCCG and ad-hoc working groups contributed to the smooth functioning of the ECCF?
- OQ3: What are the factors that could be linked to each of the elements that demonstrate efficiencies and inefficiencies?

**JUDGEMENT CRITERIA AND INDICATORS**

| | |
|---|---|
| OQ1: There are no identified inefficiencies | Findings on the previous efficiency questions and stakeholder perceptions triangulated with additional data sources. |
| OQ2: Identified good practices in the selected activities | |
| OQ3: Causal factors of efficient and inefficient practices are identified | |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| ***Evaluation results*** |
|---|
| The efficiency of the ECCF was shaped primarily by challenges related to both the substance and the procedures involved. Issues concerning content included political factors and the technical complexity of the certification schemes, which varied depending on the stakeholders and the specific products or services subject to certification. Procedural difficulties arose from preparation and adoption processes that had not been previously tested and were potentially cumbersome. On the other hand, the voluntary nature of the schemes did not seem to have a notable influence on the ECCF's efficiency. The formation of dedicated groups and forums facilitated necessary stakeholder involvement even though there remains substantial room for organisational improvement and refinement of internal governance. |



### 8.1.3. *Coherence*

The coherence analysis examined the extent to which the objectives of ENISA and the ECCF align with and complement other initiatives and the work of EU and national bodies in the field of cybersecurity. Specifically, the external coherence analysis assessed how well ENISA and the ECCF support the broader cybersecurity policy goals of the European Commission.

Internal coherence was also evaluated to determine how effectively the various components within ENISA and the ECCF function together to achieve their respective objectives.

The tables below present the structure of the evaluation matrix. Where relevant, findings are presented separately for ENISA and the ECCF.

**ENISA**

| ***Coherence*** | **How well has ENISA supported the overarching policy goals?** |
|---|---|

| EQ1, ENISA | |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent has ENISA contributed to the implementation of the NIS2 Directive? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: ENISA positively contributed to the implementation of the NIS2. | Quality of implementation of NIS2 provisions. |
| | |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| *Coherence*<br>**EQ2, ENISA** | **To what extent has ENISA fostered cooperation at EU and national level?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent has ENISA exploited synergies in expertise and knowledge sharing with other stakeholders and EU/MS bodies and private and public stakeholders?<br>▪ OQ2: To what extent has ENISA coordinated its work with other EU/national bodies and private and public stakeholders in preventing and responding to cyber threats? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: ENISA sufficiently exploited synergies in expertise and knowledge sharing with other stakeholders and EU/MS bodies | Opinions of stakeholders (with two thirds of all stakeholders having a positive opinion); share of synergies exploited and their contribution to the quality of achieved outputs |
| OQ2: ENISA made the best use of existing resources while working with other EU/national bodies and private and public stakeholders in preventing and responding to cyber threats (while avoiding overlaps) | Share of complementarities and overlaps in the work of ENISA with other EU/national bodies[284]; opinions of stakeholders on this issue (with two thirds of all stakeholders having a positive opinion) |

[284] Other EU and national bodies working on cybersecurity and digital privacy include various Commission directorates, the European External Action Service and other EU bodies and agencies such as BEREC, EUROPOL and CERT-EU, national cybersecurity competent authorities or regulators, national CSIRTs/Computer Emergency Response Teams and more recently the European Cybersecurity Competence Centre (ECCC) and its network of national coordination centres (NCCs).

| | |
|---|---|
| OQ3: Stakeholders confirm ENISA's leading role in the cooperation between MS, EU institutions, companies and other groups in the cyber domain | Share of stakeholders by group and country that considers ENISA's role in maintaining cooperation among them as crucial |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| **Evaluation results** |
|---|
| The findings reveal that ENISA played a proactive role in encouraging collaboration and the exchange of knowledge among stakeholders. While ENISA effectively promotes cybersecurity cooperation across the EU, there is room for improvement in streamlining operations and enhancing synergies with EU bodies like the ECCC and national authorities. Formalising cooperation with agencies such as EMSA and the JRC could make for a more unified approach to cybersecurity initiatives. Furthermore, refining internal communication and clarifying ENISA's role in policy implementation could improve efficiency and regulatory consistency. |



## ECCF

| ***Coherence***<br>**EQ3, ECCF** | **To what extent is the ECCF coherent or overlapping with other relevant initiatives in the area of cybersecurity market?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent is the ECCF coherent and complementary with other policy, legal and funding instruments adopted at EU and national level?<br>▪ OQ2: To what extent does the ECCF overlap or create gaps with other policy, legal and funding instruments adopted at EU and national level? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The ECCF's scope complements that of other EU and national instruments | Extent to which the ECCF complements EU measures that have already been adopted (i.e. NIS2 Directive, European Cybersecurity Competence Centre and Network, Digital Europe programme) or that have been proposed (i.e. Cyber Resilience Act, Cyber Solidarity Act); extent to which the ECCF complements national cybersecurity certification measures adopted since the entry into force of the Cybersecurity Act; share of Member States detecting complementarity |
| OQ2: Other EU and national instruments tackle different aspects of securing the cybersecurity of ICT products, services and processes | Extent to which the ECCF scope overlaps with EU measures adopted (i.e. NIS2 Directive, European Cybersecurity Competence Centre and Network, Digital Europe programme) or proposed (i.e. Cyber Resilience Act, Cyber Solidarity Act); extent to which the ECCF scope overlaps with national cybersecurity certification measures adopted since the |

| | |
|---|---|
| | entry into force of the Cybersecurity Act; share of Member States detecting complementarity |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| ***Coherence***<br>**EQ4, ECCF** | **To what extent is the ECCF coherent internally?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent are the various elements of the ECCF coherent among themselves? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The ECCF procedures, governance mechanisms and working arrangements are coherent among themselves | Number and type (e.g. legal, administrative, operational) of issues identified by ENISA, the Commission and relevant forums (i.e. ECCG, SCCG, ad hoc working group members) |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| ***Coherence***<br>**EQ5, ECCF** | **To what extent is the ECCF coherent with other EU-level actions, particularly sectoral ones, in the area of certification?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent does the ECCF complement or overlap with EU policies in the area of certification?<br>▪ OQ2: To what extent is the ECCF coherent with the EU digital strategy and other relevant sectoral strategies? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| Other EU initiatives (e.g. delegated act under Radio Equipment Directive, etc.) to secure/certify ICT products, services and processes do not overlap with the ECCF | Number and type of sectoral EU policies implemented; extent to which the sectoral policies overlap with the ECCF |
| The ECCF ensures trust in ICT products, services and processes that otherwise would not be covered by other cybersecurity requirements | Number and type of digital strategy actions and sectoral strategies implemented; extent to which digital strategy actions and sectoral strategies overlap with the ECCF |
| **DATA SOURCES** | |
| ▪ Desk research | |

| |
|---|
| ▪ Survey<br>▪ Interviews |

| *Evaluation results* |
|---|
| While theoretically consistent with EU legal measures on cybersecurity, in particular the CRA (proposal at the time of the evaluation) and the NIS2 Directive, the ECCF has been found to lack clear accountability mechanisms ensuring consistency with the existing EU legal framework and requiring diligent oversight. The CRA (under development) is expected to considerably impact the legal framework related to the security evaluation and certification of ICT products. In this regard, the forthcoming implementation of the EUCC scheme will significantly test its coherence with the existing EU legal framework. |



#### 8.1.4. *EU added value*

In accordance with the Better Regulation Toolbox, the assessment of EU added value focused on identifying changes resulting from the activities of ENISA and the ECCF that would not likely have occurred through actions taken solely by Member States. The evaluation considered the factors contributing to EU added value, such as enhanced coordination, improved effectiveness or efficiency and reduced administrative burden, among others.

The tables below outline the structure of the evaluation matrix. Findings are presented separately for ENISA and the ECCF.

**ENISA**

| ***EU added value***<br>**EQ1, ENISA** | **Could the identified outputs, results and impacts have been achieved without EU intervention?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: What other possible options are there for achieving the outputs and results?<br>▪ OQ2: Is it still valid to assume that the objectives of the action can best be met by action at EU level? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |

| | |
|---|---|
| OQ1: Feasibility of alternative options for achieving the outputs and results of ENISA | List of alternative options and their description |
| OQ2. EU-level action is considered the most optimal | Stakeholders' opinions on the added value of ENISA |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews | |

| ***EU added value***<br>**EQ2, ENISA** | **What would be the most likely consequences of stopping or withdrawing EU involvement?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: How would the EU cybersecurity landscape change if EU involvement were to be withdrawn or stopped?<br>▪ OQ2: What would stakeholders see as a suitable alternative to the current EU action? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: Anticipated quality of feasible alternative options | Stakeholders' opinions on the added value of ENISA |
| OQ2: Stakeholders see ENISA as the most optimal option | |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews | |

| ***Evaluation results*** |
|---|
| The achievements in terms of outputs, results and impacts would have been difficult to attain without ENISA's involvement. ENISA's dedicated focus on the implementation of cybersecurity policy, combined with its ability to coordinate and align efforts across Member States, represents a unique contribution that other EU bodies may not be able to provide due to their broader mandates or more narrowly defined roles. ENISA brought added value to EU cybersecurity through its independent and decentralised structure, which enhanced cooperation with Member States and supported responses to cybersecurity threats. Without ENISA, the EU would likely encounter greater difficulties in coordinating efforts across borders and would face a more fragmented cybersecurity landscape, particularly affecting those Member States with less advanced capabilities in this field. Strategically increasing stakeholder engagement and reassessing resources could help ENISA better adapt to evolving cybersecurity threats and expand its operational role. Future priorities include improving recruitment processes, managing workload and strengthening transparent relationships with Member States to enhance cooperation and information sharing. Addressing criticism from private-sector stakeholders by tailoring insights to their specific challenges should also be considered. |

## ECCF

| *EU added value*<br>**EQ3, ECCF** | **To what extent has the ECCF brought EU added value compared to what could have been achieved by Member States alone?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: Could the same outcomes of the ECCF be achieved by participating countries adopting cybersecurity certification schemes outside the European framework?<br>▪ OQ2: To what extent could Member States have achieved the same outcomes without the ECCF?<br>▪ OQ3: To what extent has the ECCF increased the likelihood of achieving a more secure, transparent and cohesive internal market for ICT products, services and processes? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: Member States state that they prefer to use the ECCF to achieve a harmonised, streamlined and coherent cybersecurity certification mechanism | Number of Member States preferring to use the ECCF; number and type of parallel certification procedures carried out by Member States |
| OQ2: Member States' unilateral and uncoordinated measures were ineffective in securing ICT products, services and processes placed on the internal market | Number of national certification measures successfully certifying ICT products, services and processes; number of certification procedures carried out under the SOG-IS-MRA |
| OQ3: ECCF increases the security of ICT products, services and processes sold in the internal market | Extent to which the certification of ICT products, services and processes through the ECCF has guaranteed more security |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Survey<br>▪ Interviews | |

| ***Evaluation results*** |
|---|
| Stakeholders generally agreed that the ECCF delivers added value at EU level beyond what individual Member States could achieve on their own, even though its direct impact remains limited. This added value was particularly noticeable in areas such as the adoption of certification, the use of cost-efficient procedures, the promotion of cyber-awareness, the strengthening of trust within the EU single market and the encouragement of cybersecurity principles by default and by design. Most stakeholders also acknowledged the ECCF's role in contributing to a more secure, transparent and unified internal market for ICT products, services and processes. However, the added value of the ECCF has been somewhat limited due to its shortcomings in reaching its objectives (see effectiveness criteria) and its lack of efficiency (see efficiency criteria). |

### 8.1.5. *Relevance*

According to the Better Regulation Toolbox, the relevance evaluation compared the needs and challenges present at the time of the adoption of Regulation (EU) 2019/881, which established ENISA's current mandate and the European cybersecurity certification scheme, with those encountered during its implementation. The evaluation also examined how the current and anticipated future needs and problems within the EU align with the objectives of ENISA and the ECCF.

The relevance evaluation identified potential mismatches between the objectives of ENISA and the ECCF and the evolving cybersecurity landscape. For instance, some of the 'problem drivers' outlined in the original impact assessment may no longer be applicable, while emerging technological developments could introduce new challenges related to cybersecurity innovation.

The tables below outline the structure of the evaluation matrix. Findings are presented separately for ENISA and the ECCF.



**ENISA**

| ***Relevance***<br>**EQ1, ENISA** | **Are objectives and tasks revisited periodically to identify upcoming and urgent needs?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: How flexible has ENISA been in adapting to the evolving landscape of threats, regulatory changes and policy responses? Where relevant, what were the main factors limiting ENISA's contribution to this objective? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| ENISA quickly adapted to the evolving landscape of threats, regulatory changes and policy responses | Speed of organisational responses to the changing regulatory environment and policy responses; speed and quality of responses to emerging cyber threats |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| *Relevance*<br>**EQ2, ENISA** | **Did ENISA's objectives and tasks respond successfully to the overall EU policy objectives and the needs of stakeholders?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: Has ENISA correctly identified the needs of its stakeholders and the EU policy objectives?<br>▪ OQ2: Has ENISA successfully responded to the needs of its stakeholders and the EU policy objectives? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The needs of ENISA's stakeholders and the EU policy objectives (including priorities) were duly identified. | Needs of stakeholders were acknowledged in ENISA's organisational decision-making; practices of stakeholder consultation have been duly established and implemented; positive perceptions of ENISA's stakeholders on those issues |
| OQ2: ENISA responded well to the needs of stakeholders and the EU policy objectives. | EU policy objectives (including priorities) in the field of cybersecurity were acknowledged and referred to in ENISA's documents |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Interviews<br>▪ Survey | |

| *RELEVANCE*<br>**EQ3, ENISA** | **To what extent has ENISA supported the Commission and Member States in their policy-related tasks?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent do ENISA's stakeholders indicate that the role and purpose of ENISA in policy-related tasks are clear and properly defined?<br>▪ OQ2: To what extent have ENISA's operations enabled Commission staff to better focus on the institutional tasks? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| EC officials consider ENISA's operation optimal for its institutional tasks. | Opinion of EC officials on the operation of ENISA; IAS, ECA evaluations<br>Perception of ENISA's stakeholders (two thirds of surveyed/interviewed stakeholders have a positive opinion on the specific aspects of ENISA's performance) |
| ENISA's stakeholders view its policy development support positively. | |
| ENISA's stakeholders view its policy implementation support positively. | |
| ENISA's stakeholders view ENISA's advice and opinion positively. | |
| **DATA SOURCES** | |
| ▪ Desk research | |

| |
|---|
| ▪ Interviews<br>▪ Survey |

| ***Evaluation results*** |
|---|
| ENISA's significance in the cybersecurity domain is highlighted by its adaptability to evolving stakeholder needs and its ability to realign its focus to meet emerging developments. ENISA reacted successfully to changes in the cybersecurity environment, resulting in high levels of satisfaction among stakeholders. However, some expressed concerns about ENISA's ability to fully address the rising cyber threats across Europe. National cybersecurity bodies and smaller Member States benefited from ENISA's initiatives in building capacity and providing regulatory guidance. Nonetheless, there remain opportunities to strengthen ENISA's relevance, particularly by taking a more proactive role in offering tools and support tailored to specific sectors. This is especially important for small and medium-sized enterprises (SMEs), which face distinct needs and challenges. By revisiting priorities, improving its communication, streamlining processes, ensuring adequate resources and, to a certain extent, efficiently utilising existing resources, ENISA can strengthen its foundational role within Europe's cybersecurity framework and better align with the dynamic demands of the European cybersecurity landscape. |



## ECCF

| ***Relevance***<br>**EQ4, ECCF** | **To what extent are the scope and objectives of the ECCF still relevant?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: To what extent are the objectives of the ECCF still relevant for addressing the cybersecurity threat landscape?<br>▪ OQ2: To what extent are the objectives of the ECCF still relevant considering how the EU policy context has changed since its adoption? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The ECCF is still needed to tackle cybersecurity threats to the EU. | Number of ECCF objectives which are still relevant in the current threat landscape. |
| OQ2: The ECCF is still needed despite the EU policy and programmes implemented since its introduction. | Number of objectives which are still relevant after the introduction of the NIS2 Directive, the European Cybersecurity Competence Centre and Network, the EU cybersecurity strategy and the Digital Europe programme as well as the proposals for a CRA and a Cyber Solidarity Act. |
| **DATA SOURCES** | |
| ▪ Desk research | |

| |
|---|
| ▪ Interviews |

| ***Relevance***<br>**EQ5, ECCF** | **To what extent is the ECCF still relevant in terms of achieving its objectives?** |
|---|---|
| **OPERATIONAL QUESTIONS** | |
| ▪ OQ1: Are the features of the ECCF (schemes and procedures) envisaged in the Cybersecurity Act still relevant in terms of fulfilling its objectives in the current threat landscape?<br>▪ OQ2: To what extent is the ECCF relevant in terms of securing ICT products, services and processes? To what extent has it increased or decreased in relevance in view of increasing geopolitical tensions in digital policy? | |
| **JUDGEMENT CRITERIA AND INDICATORS** | |
| OQ1: The Commission and Member States do not highlight the need for adjustments to fulfil its objectives in the current threat landscape. | Extent of possible adjustments needed to tackle current cybersecurity threats. |
| OQ2: The relevance of the ECCF increased for Member States. | Number and type of cybersecurity certification initiatives launched, both in the EU and internationally since the adoption of the Cybersecurity Act; extent to which Member States state that cybersecurity certification is needed. |
| **DATA SOURCES** | |
| ▪ Desk research<br>▪ Survey<br>▪ Interviews | |

| ***Evaluation results*** |
|---|
| The ECCF remains relevant in supporting the objectives of the internal market. Given the rising frequency and seriousness of cybersecurity threats, stakeholders considered EU cybersecurity certification to be a useful and important tool to enhance Europe's cyber resilience and preparedness. Several elements contributed to the ECCF's perceived relevance, including enhanced cooperation at EU level, assistance in the development of standards and the possibility of requiring certification for critical infrastructure (e.g. under NIS2) and recipients of public procurement. In addition, stakeholders pointed to the ECCF's ability to strengthen collaboration among EU Member States and promote trade by offering a harmonised certification platform. |

## 9. ANNEX IV. OVERVIEW OF BENEFITS AND COSTS [AND WHERE RELEVANT, TABLE ON SIMPLIFICATION AND BURDEN REDUCTION]

Annex IV provides an overview of the costs and benefits projected in the preferred options of the 2017 CSA IA. It also shows the potential simplification and burden reduction savings identified in the current 2025 IA for the updated CSA preferred options. This annex presents a comparison, highlighting both the initial expectations and the most recent projections for the main policy options considered for ENISA and the ECCF. It is important to note that, at the time of this evaluation, there is no quantitative data available on the simplification or burden reduction already achieved for ENISA. For certification, no realised savings can be reported yet, as the first EU-wide certification scheme was only adopted in May 2025 and the evaluation was conducted between 2023 and 2024. As a result, the annex focuses on projected and potential impacts, rather than on realised monetary benefits or cost reductions for either ENISA or the ECCF.

***Table 1. Overview of the costs and benefits identified in the evaluation***

| | **Citizens/Consumers** | | **Businesses** | | **Administrations** | |
|---|---|---|---|---|---|---|
| | **Quantitative data** | **Comment** | **Quantitative data** | **Comment** | **Quantitative data** | **Comment** |
| **Costs** | | | | | | |
| **Direct compliance costs** (adjustment costs, administrative costs, regulatory charges) | No monetary costs were projected. | No direct compliance costs for citizens/consumers identified. | No monetary costs were projected. | No direct compliance costs for businesses in the short term, as certification remains | **ENISA:** +EUR 9-12 million/year (to reach EUR 20-23 million/year); 50 additional staff (36 permanent, 14 external) | ENISA costs mostly borne by EU budget; ECCF costs for Member States relate to setting up and running |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | voluntary. | (recurrent).<br><br>**ECCF:** Member States: ~EUR 1.6 million/year per authority for personnel, equipment and operations (recurrent).<br><br>**EU Commission:** 3 FTEs for scheme adoption (recurrent).<br><br>**Expert group:** EUR 16 000-17 000/year (recurrent). | certification authorities. |
| **Enforcement costs:** (costs associated with activities linked to implementing an initiative, such as monitoring, inspections and adjudication/litigation) | No monetary costs were projected. | Not specified. | No monetary costs were projected. | Not specified for businesses. | **Member States:** ~EUR 290 000-300 000/year per authority for enforcement and supervision (recurrent). | Applies to operational management of certification authorities. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Indirect costs** (indirect compliance costs or other indirect costs such as transaction costs) | No monetary costs were projected. | Not specified. | No monetary costs were projected. | Not specified for businesses | No monetary costs were projected. | Not specified. |
| **Benefits** | | | | | | |
| **Direct benefits** (such as improved wellbeing, changes in pollution levels, safety, health, employment, market efficiency) | No monetary costs were projected. | Not directly quantified. Expected reduction in cyber incidents and improved trust and security (recurrent). | No monetary costs were projected. | Direct benefits from reduced investment in commercial analyses/reports; free access to ENISA outputs; improved competitiveness; reduced market-entry barriers for SMEs; and access to wider cybersecurity market (recurrent). | No monetary costs were projected. | Efficiency gains for EU budget; economies of scale in information collection and operational cooperation; reduced need for new EU body (saves EUR 21.9 million in set-up costs) (one-off). |
| **Indirect benefits** (such as wider economic benefits, macroeconomic benefits, social impacts, environmental impacts) | No monetary costs were projected. | Not specified. | Expected reduction in costs of cybercrime | Indirect benefits from harmonised policy; reduced administrative | No monetary costs were projected. | Member States benefit from economies of scale, reduced duplication |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | incidents (currently ~0.41% of EU GDP, ~EUR 55 billion/year) (recurrent). | burden; mutual recognition of certificates; increased trust in digital solutions; and improved access to public procurement (recurrent). | | and more harmonised approaches. |

| ***PART II: II <u>Potential</u> simplification and burden reduction (savings)*** | | | | | | |
|---|---|---|---|---|---|---|
| | **Citizens/Consumers/Workers** | | **Businesses** | | **Administrations** | |
| | **Quantitative data** | **Comment** | **Quantitative data** | **Comment** | **Quantitative data** | **Comment** |
| **Description:** | | | | | | |
| **Option A.2: Reform of ENISA's mandate** | Attestation cost per attestation: ~EUR 300-350 (public) vs ~EUR 677 (private). | Better visibility on the labour market for cybersecurity professionals; better career progression; better wages; increased portability of skills. | EUR 3.7 to 4.4 billion over five years (broad estimate) for faster incident detection and response. | Reputation of skills attestation providers; access to the cybersecurity skills market (especially SMEs); improved incident response | Fees offset ENISA operational costs. | Cost avoidance for public authorities that are developing or plan to develop attestation schemes (reduced compliance and supervisory burden for |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | reduces breach costs; streamlined certification processes. | | authorities); use of national liaison officers for some tasks. |
| **Option B.2: Reform the ECCF by revising procedures and extending scope to simplify regulatory compliance** | No monetary savings were projected. | Faster access to certified services; indirect benefit from improved security and reduced incident costs. | N/A | Single certification instead of multiple national ones; reduced compliance costs; lower cyber insurance premiums; increased mutual recognition. | Reduced time to develop schemes. | Reduced supervisory burden; streamlined scheme adoption and monitoring. |
| **Option C.2: Targeted action – further simplification of compliance with relevant EU cybersecurity legislative framework** | No monetary savings were projected. | Reduced compliance costs for individuals in reclassified entities; indirect benefit from improved security and fewer incidents. | Annual savings in compliance costs of EUR 14.6 billi on over five years. | Reduced administrative burden due to fewer entities in scope; streamlined demonstration of compliance via certification. | Annual savings in enforcement costs of EUR 7.5 million over five years. | Reduced supervisory burden for authorities; simplified compliance monitoring; 28 700 fewer NIS2 entities to be supervised. |

# 10. ANNEX V. STAKEHOLDER CONSULTATION - SYNOPSIS REPORT

This annex summarises all the consultation activities carried out as part of the evaluation of ENISA and the ECCF. The consultation strategy was designed to collect input from all relevant stakeholder groups, including public authorities, EU institutions, industry, academia, civil society and individual citizens. It covers the full range of activities undertaken, such as the call for evidence, the targeted survey, targeted interviews and dedicated workshops. It provides a consolidated overview of stakeholder feedback on the performance, strengths, weaknesses and areas for improvement of ENISA and the ECCF. The evidence collected through these activities forms a key part of the analytical framework supporting the evaluation and informs the recommendations for future policy development.

## 10.1. Consultation scope and objectives

### Scope

The stakeholder consultation activities were undertaken as part of the evaluation of ENISA and the ECCF, in accordance with Article 67 of Regulation (EU) 2019/881, known as the Cybersecurity Act. The evaluation covered the period from 2017 to 2023 and sought to assess the performance of ENISA and the ECCF against the criteria of effectiveness, efficiency, relevance, coherence and EU added value. The consultation activities were designed to gather evidence from a wide range of stakeholders in order to inform the evaluation and support evidence-based policy-making.

The consultation addressed both ENISA and the ECCF, focusing on ENISA's mandate, objectives, governance, working practices and the implementation of the ECCF. The scope included assessing ENISA's support for policy development and implementation, capacity building, stakeholder engagement, and the development and adoption of cybersecurity certification schemes under the ECCF.

### Objectives

The objectives of the stakeholder consultation were as follows:

- to collect comprehensive and representative feedback from all relevant stakeholder groups regarding the performance, strengths, weaknesses and areas for improvement of ENISA and the ECCF;
- to assess the effectiveness, efficiency, relevance, coherence and EU added value of ENISA's activities and the ECCF, as perceived by stakeholders;
- to identify lessons learned and recommendations for potential changes to the existing Regulation and for improving the performance of ENISA and the ECCF;
- to ensure that the evaluation is informed by the experiences, needs and expectations of Member States, EU institutions, industry, standardisation bodies, academia, non-governmental organisations and other relevant actors;

- to gather input on the implementation and impact of the ECCF, including the development and adoption of certification schemes, stakeholder involvement, transparency and alignment with EU and international standards.

The consultation was structured in such a way as to provide evidence for the evaluation's analytical framework, which included a mixed-methods approach comprising desk research, surveys, interviews and workshops. The consultation aimed at systematically collecting and analysing the perspectives of all key stakeholders, including public authorities, the private sector, civil society, members of academia, experts and individual citizens, to inform the evaluation conclusions and the policy-making process.

### 10.2. Mapping of stakeholders

The consultation activities to evaluate ENISA and the ECCF were designed to ensure broad and balanced representation of all relevant stakeholders in the European cybersecurity landscape. Stakeholders were identified and mapped according to their institutional role, their involvement in cybersecurity policy and practice, and their relationship to ENISA and the ECCF. This mapping informed the design and targeting of surveys, interviews and workshops.

The main stakeholder categories included:

- **EU institutions and bodies:** this group comprised the European Commission, the European Parliament and decentralised agencies with responsibilities in cybersecurity policy, oversight and implementation. Their input focused on policy development, regulatory coherence and cross-border coordination.
- **National public authorities:** national cybersecurity agencies, competent ministries, regulators and other authorities responsible for implementing and enforcing cybersecurity policy were included. These stakeholders provided perspectives on national approaches, regulatory challenges and the practicalities of executing policy.
- **Industry and private sector organisations:** this category included companies involved in developing, providing or operating digital products and services, such as hardware manufacturers, software developers, cloud service providers and cybersecurity solution vendors. Their input was essential for understanding the impact of certification schemes and regulatory requirements on market stakeholders.
- **Industry associations and representative bodies:** associations representing the collective interests of businesses and industry sectors were engaged to reflect the perspectives of both large enterprises and SMEs. These organisations often acted as intermediaries, helping their members participate in the consultation process.
- **SMEs:** these were consulted both directly and through representative associations. Their feedback was important for assessing the proportionality and accessibility of the regulatory framework, given their specific resource constraints and operational realities.
- **Academic and research institutions:** universities, research centres and think tanks with expertise in cybersecurity, standardisation and policy evaluation contributed analytical and technical perspectives. Their involvement ensured a robust assessment of the strengths and limitations of the current framework.

- **Consumer and civil society organisations:** organisations advocating for consumer rights, privacy, digital security and broader societal interests were included to ensure that the public interest was reflected in the evaluation. Their contributions addressed issues such as transparency, user protection and the societal impact of cybersecurity measures.
- **International organisations and standardisation bodies:** relevant international entities and standardisation organisations were engaged to provide input on how well European initiatives were aligned with global standards and practices.
- **Individual citizens:** members of the public were invited to participate, particularly through the targeted survey, to capture user experiences, perceptions of cybersecurity risks and expectations regarding digital security and trust.

This mapping ensured that the consultation strategy was inclusive and balanced, avoiding overreliance on any single group. It also guided the development of survey instruments and interview protocols, ensuring that questions were tailored to the specific roles and expertise of each stakeholder category.

### 10.3. Consultation activities

Consultation activities were conducted to support the evaluation of ENISA and the ECCF. The objective was to collect robust and representative evidence from all relevant stakeholder groups, ensuring that the evaluation was informed by a wide range of perspectives and experiences.

The main consultation activities included:

- **Call for evidence:** a call for evidence was organised to collect feedback from a wider audience, including stakeholders not directly targeted by the survey or interviews. The call for evidence was open from 14 July to 16 September 2023 and received 41 contributions from a diverse range of stakeholders, including business associations, companies, public authorities, consumer organisations, NGOs and individual citizens. The targeted survey provided additional perspectives on the effectiveness, efficiency and impact of ENISA and the ECCF.
- **Survey:** a targeted survey was conducted using the EUSurvey platform. The survey was designed to involve all stakeholder groups, including those involved with ENISA and the ECCF. It included both closed and open questions, with filtering to ensure that it was relevant to different respondents. The survey was sent to 856 stakeholders and was also promoted by the European Commission, ENISA and relevant associations. The survey was open from 13 February to 5 March 2024, with extensions to maximise participation. In total, 209 responses were collected, covering a broad spectrum of stakeholder categories, such as national authorities, industry stakeholders, academic institutions, consumer organisations and EU institutions.
- **Interviews:** a structured interview programme was carried out to gather in-depth qualitative insights. The study team contacted 182 individuals and conducted 49 interviews for ENISA and 13 for the ECCF. Interviewees included ENISA staff and representatives of the European Commission, national authorities, industry, academia and international organisations. The interviews were designed to explore key evaluation questions in greater detail and to validate findings from other consultation activities.

- **Workshops:** two main workshops were held for collective discussion and validation of findings. The first was a SWOT and recommendations workshop, which brought together stakeholders from academia, ENISA, the European Commission and industry to discuss strengths, weaknesses, opportunities and threats related to ENISA and the ECCF. This workshop included interactive polling and breakout sessions to gather detailed feedback and suggestions for improvement. The second workshop focused on validating preliminary evaluation results and collecting recommendations for future improvements. Participants included representatives from the European Commission, Member States and other key stakeholder groups.

The overarching objective of these consultation activities was to ensure that the evaluation of ENISA and the ECCF was informed by stakeholder input. Each activity was designed to capture a specific type of evidence: desk research provided context and baseline data; the survey programme enabled quantitative analysis of stakeholder views; interviews offered qualitative depth and validation; and workshops allowed collective reflection and consensus-building. Together, these activities ensured that the evaluation reflected the experiences, needs and expectations of all relevant stakeholders in the European cybersecurity ecosystem.

### 10.4. Call for evidence

The call for evidence was conducted from 14 July to 16 September 2023 to collect stakeholder feedback on the impact, effectiveness and efficiency of ENISA's mandate and the ECCF. The consultation aimed to gather views from a broad range of stakeholders, particularly those involved in the EU cybersecurity certification process. In total, 41 responses were received from 13 EU Member States and two non-EU countries, with the majority of contributions coming from the private sector. Nearly half of the respondents were business associations (20), followed by companies and businesses (9), public authorities (4), consumer organisations (1), NGOs (1), research centres and standards associations (4), and individual citizens (2). Most respondents (85%) were based in the EU, with the remainder from the USA and the UK. Sectoral representation was also diverse, with significant input from digital service providers, digital infrastructure providers, manufacturing trade associations and generalist organisations.

The call for evidence sought to assess three main areas: the overall organisation and performance of ENISA, the functioning of the ECCF and feedback on specific certification schemes, particularly the Cloud Services Scheme (EUCS). Stakeholder feedback on ENISA was generally positive, with around 30% of respondents recognising ENISA as a leading centre of cybersecurity expertise in the EU. Particularly appreciated were its contributions to cyber resilience, incident response and the promotion of cooperation and best practice exchange. However, almost 22% of respondents said that ENISA's resources and capabilities needed to be distributed adequately and consistently, citing also challenges in recruiting qualified staff. Stakeholders recommended increasing cooperation with academic and research institutions to maintain specialised expertise.

A recurring theme in the feedback was the need for greater transparency and stakeholder involvement in ENISA's processes. Over 40% of respondents expressed concerns about insufficient engagement, particularly for smaller organisations and civil society representatives. Stakeholders called for more meaningful participation and improved communication, and for

‘update only’ meetings to be avoided. While it was highlighted that ENISA engaged with Member States through the national liaison officers network, some respondents noted limited benefits from existing working groups due to organisational challenges.

Regarding the ECCF, stakeholders generally viewed EU cybersecurity certification as a useful and promising tool, but highlighted several areas for improvement. Delays in adopting certification schemes and the Union rolling work programme (URWP) were frequently mentioned as limiting the impact of the framework. Approximately 34% of respondents reported that they were insufficiently involved in developing certification schemes). A similar proportion (32%) highlighted a lack of transparency in ECCF procedures, including opaque decision-making, insufficient information sharing and changes to draft schemes without prior consultation. Stakeholders emphasised the importance of increasing transparency regarding the composition and functioning of ad hoc working groups, and of ensuring that members have access to draft schemes and are promptly informed of significant changes.

The mandatory nature of certification schemes was another area of debate. Of the 34% of respondents who raised this issue, the majority were opposed to mandatory requirements, citing concerns about increased costs and barriers to the internal market, particularly for SMEs. Those in favour of mandatory certification stressed the need for sectoral approaches, alignment with international standards and the use of impact assessments to evaluate the potential effects on economic operators and the internal market.

The Cloud Services Scheme attracted particular attention, with 9 out of 10 stakeholders concerned about the certification process being politicised, especially regarding data localisation requirements. Respondents warned that such requirements could disrupt business relationships and hinder market competition, particularly for providers headquartered outside the EU.

Stakeholders also stressed the importance of aligning EU certification schemes with international standards (21% of respondents) and ensuring coherence with the broader EU legislative framework (20%). Recommendations included streamlining compliance, allowing audit reports to be reused for multiple legal acts and ensuring mutual recognition of cybersecurity certificates across EU countries.

In summary, the call for evidence highlighted both strengths and areas for improvement in ENISA’s mandate and in the ECCF. Stakeholders recognised ENISA’s expertise and positive impact, but called for adequate resources that are distributed appropriately, for greater transparency and for more inclusive stakeholder engagement. As regards the ECCF, the feedback underscored the need for schemes to be adopted in a timely manner and for greater transparency, stronger stakeholder involvement and alignment with international standards and EU law. The consultation also revealed concerns about certification processes being politicised by considerations related to non-technical risk factors. Overall, the feedback emphasised the importance of collaborative and inclusive approaches to developing effective European cybersecurity policies and certification frameworks.

## 10.5. Targeted survey

The targeted survey formed a central part of the evaluation of ENISA and the ECCF. It aimed to collect evidence and perspectives from a broad pool of stakeholders across the European cybersecurity ecosystem. The consultation was designed to assess the effectiveness, efficiency, relevance, coherence and added value of ENISA and the ECCF, and to ensure that the evaluation was informed by the experiences and expectations of all relevant stakeholders. This included stakeholders directly involved with ENISA and the ECCF, as well as those who benefit from their outputs and activities.

The survey programme was conducted via the EUSurvey platform, with the questionnaire developed on the basis of desk research, initial interviews and feedback. The survey included both closed and open questions, with filtering and branching logic to ensure that respondents were asked questions relevant to their background and involvement with ENISA and/or the ECCF. The survey was launched on 13 February and closed on 5 March 2024, with extensions and follow-up reminders to maximise participation.

### 10.5.1. *Stakeholder participation*

A total of 856 stakeholders received a personal invitation to complete the survey. The survey link was also promoted via the Commission's news page, in ENISA's internal communications and by the relevant associations. Up to three follow-up emails were sent to non-respondents and the deadline was extended by one week to accommodate additional responses. In total, 209 responses were received, representing a broad cross-section of stakeholder groups and ensuring a robust and representative evidence base for the evaluation.

**Table 1. Number of survey responses per stakeholder group (overall)**

| | ENISA Ad hoc Working Groups | ENISA Advisory Group | ENISA Executive Board | ENISA Management Board | ENISA National Liaison Officer | ENISA Staff | External to ENISA | Total |
|---|---|---|---|---|---|---|---|---|
| **Academia / research** | 2 | 2 | | | | | 3 | 7 |
| **Consumer organisation** | | 1 | | | | | 4 | 5 |
| **EU institution/ body** | 2 | 3 | | 1 | | | 7 | 13 |
| **Individuals** | 1 | 4 | | | | | | 5 |
| **Industry organisation** | 23 | 21 | | | | | 18 | 62 |
| **International body or** | | 1 | | | | | 5 | 6 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **network** | | | | | | | | |
| **National cybersecurity authority/ agency** | 22 | | 2 | 7 | 10 | | 37 | 78 |
| **Other competent authority** | 5 | | | 1 | | | 13 | 19 |
| **Other** | | 1 | | | | | | 1 |
| **Total** | **55** | **33** | **2** | **9** | **10** | **13** | **87** | **209** |

### ECCF-specific stakeholder participation

Of all the respondents, 70 (33%) indicated that they were involved with the ECCF and received a specific set of questions about its implementation. The breakdown for ECCF stakeholder groups is as follows:

**Table 2. Number of survey responses per stakeholder group (ECCF)**

| Stakeholder group | Number of responses |
|---|---|
| **ENISA ad hoc working group(s) related to cybersecurity certification** | 37 |
| **Stakeholder Cybersecurity Certification Group (SCCG)** | 24 |
| **European Cybersecurity Certification Group (ECCG)** | 21 |
| **National Cybersecurity Certification Authorities** | 19 |

Note: Respondents could select more than one option.

#### 10.5.2. *Summary of results*

### ENISA survey results

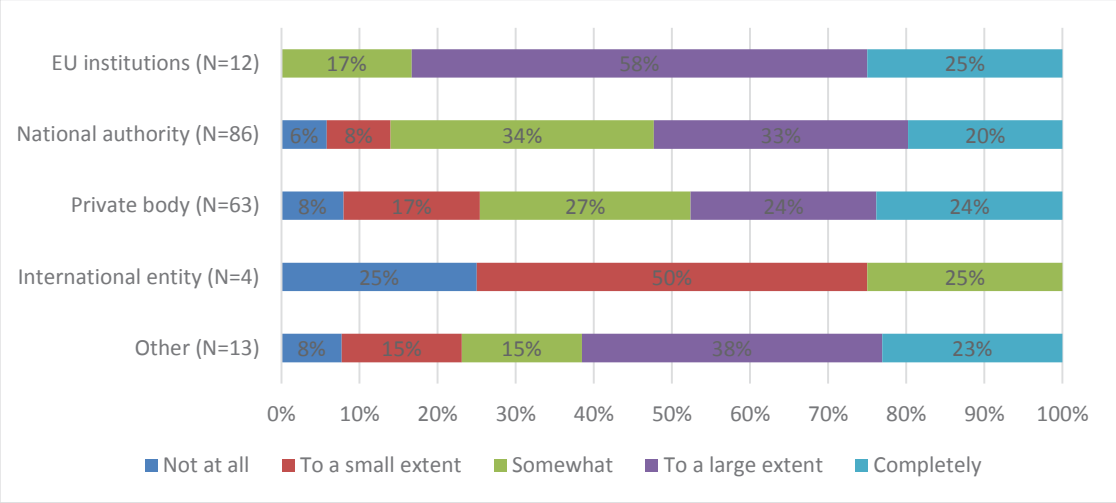
### Effectiveness

ENISA is generally acknowledged by stakeholders as effective in fulfilling most of its mandate. According to the survey, 71% of stakeholders considered ENISA a leading centre of expertise on cybersecurity, able to deliver valuable outputs, including for policy-making and decision-making processes. ENISA's support was particularly appreciated during critical periods, such as the COVID-19 pandemic, and for its operational cooperation with Ukraine.

ENISA's publications were cited most frequently by stakeholders in the cybersecurity field, confirming ENISA's status as a centre of expertise in this area. Between 2017 and 2023, ENISA produced and issued a total of 286 publications. These covered a wide range of topics, with the most frequent being cybersecurity policy (72 publications), cyber threats (48), critical infrastructure (38), incident reporting (24) and emerging technologies (21). Stakeholders were involved in the preparation of these publications through workshops and studies. While these publications were highly cited and appreciated for their independence and clarity, many respondents noted in the open-ended follow-up questions that these could be made more concise and practical. There was a clear call for using summaries and visualisations more widely to make key information easier to identify.

Supporting policy implementation is one of ENISA's key tasks, as reinforced by the Cybersecurity Act. ENISA's support has contributed to its stakeholders adopting regulatory or policy changes and innovations. Respondents provided concrete examples, such as adopting structured threat communication protocols and using ENISA's guidance on implementing the NIS Directive to improve cybersecurity resilience. Respondents also underlined the influence of ENISA's frameworks on national cybersecurity certification schemes and the fact that ENISA's foresight activities helped anticipate future regulatory needs. Over 80% of ENISA's contribution was related to organising workshops and conferences. However, according to survey results, only about half of national authorities and companies consistently used ENISA's outputs for policy- or decision-making processes.

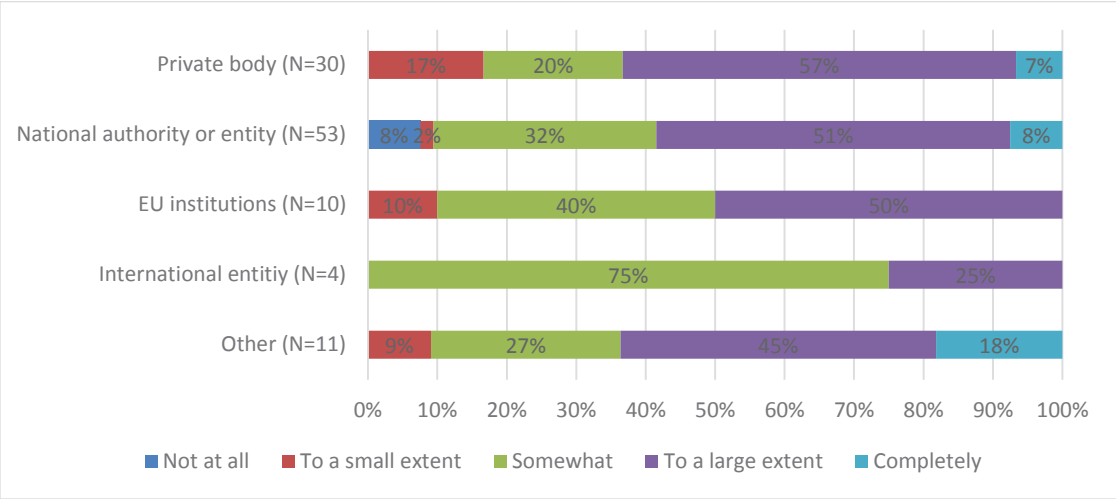
*Figure 13 2 ENISA's outputs in policy tasks*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 21 'Please indicate to which extent ENISA's activities and outputs contributed to the following aspects? My organisation uses ENISA's outputs in its policy and or decision-making processes'.

The consultation results also show ENISA's effectiveness in supporting Member States through the Cybersecurity Support Action. 58 % of all stakeholders agreed that ENISA effectively supported Member States in preventing and responding to cyberattacks through that Action, with no notable differences between various stakeholder groups. However, the consultation also revealed that 44% of survey respondents were unable to assess the usefulness of the Action, indicating that the visibility of the Action needed to be improved.

*Figure 143 The Cybersecurity Support Action's support to Member States in preventing and responding to cyber attacks*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 25 'In your opinion, to which extent has the ENISA Cybersecurity Support Action been effective in supporting EU member states in preventing and responding to cyberattacks?'

In summary, while stakeholder satisfaction with ENISA's approach and activities is generally positive, given its valuable outputs and role as a centre of expertise in cybersecurity, there are areas where its relevance can be significantly improved. ENISA's contributions to policy implementation and capacity building are appreciated by stakeholders, although there are clear opportunities for improvement in communication, stakeholder engagement and resource allocation.

**Efficiency**

During the 2017-2023 evaluation period, stakeholders were enthusiastic about ENISA's performance, praising it for successfully delivering its outputs even during periods of high workload, and recognising its operations as mostly efficient under its existing governance structure. Despite this, the evaluation and survey highlighted several key areas where stakeholders found that ENISA still had room to become more efficient.

Responses to open-ended questions showed that some stakeholders were confused about ENISA's role within the EU's cybersecurity framework. Notably, 28% of the respondents surveyed were more restrained with regard to seeing ENISA as the centre of expertise on cybersecurity. They noted that the lack of a more effective communication system jeopardises ENISA's standing as the centre of expertise and that the complicated structure of ENISA's website prevented them from interacting properly with its outputs.

Interviews with ENISA's staff, stakeholder surveys and internal documentation indicated that ENISA struggled to keep pace with increasing demands and struggled to fill specialised positions, exacerbated by a global shortage of IT and cybersecurity specialists. This led to delays, reprioritisation of tasks and periods of high stress and workload. Periods of high workload for ENISA were often associated with adopting and implementing new policies or legal acts, with developing cybersecurity certification and with operational activities related to geopolitical developments. However, 63% of stakeholders gave a positive assessment of

ENISA's performance ('successful' or 'very successful') during such periods. The survey results indicate that ENISA's organisational arrangements were relatively well adapted to managing periods of high workload. A total of 84% of stakeholders 'completely', to a 'large extent' or 'somewhat' agreed with this statement.

However, resources and resource allocation, operational inefficiencies and challenges stemming from the political and regulatory environment were identified as the main obstacles to ENISA's performance during periods of high workload. The 2022 Staff Satisfaction Survey shows that 64% of respondents experienced stress due to high workload.

In 2023, an average of 76% of staff reported working more than 40 hours per week monthly and in 2022, 4 FTEs resigned due to overwork and work over weekend. Some stakeholders noted that more resources and, to some extent, a more agile approach to deploying resources could be a way for ENISA to better adapt to evolving cybersecurity demands and to minimise delays. Other stakeholders thought that ENISA could increase its capacity to provide policy and technical support by being more selective with its engagements and refining its operational focus areas.

Stakeholders also noted that budget management presents opportunities for improvement. Despite significant budget growth from 2017 to 2023, resource constraints persisted. ENISA's budget grew unevenly, with notable increases in 2019 (over 46%), 2020 (30.5%) and 2022 (72.4% compared to 2021, due to the Cybersecurity Support Action). ENISA encountered a downward trend in balancing approved and committed appropriations between 2019 and 2022 due to delays in actions like the Cybersecurity Support Action. Reversing this trend and dedicating efforts towards managing administrative expenditure, including addressing procurement delays, could further improve internal efficiency.

In summary, ENISA demonstrated efficiency in implementing its tasks, supported by a revised governance structure. However, stakeholders underlined opportunities for ENISA to become more efficient by improving its communications and by making more resources available or allocating resources in a more strategic manner.

**Relevance**

ENISA's relevance within the cybersecurity domain is shown by its responsiveness to evolving stakeholder needs and its flexibility to adapt to the changing landscape. According to stakeholders, it has consistently demonstrated its ability to review and realign its areas of action in response to emerging developments. Thus, it continues to be a vital part of the EU's cybersecurity framework.

The results of the survey confirmed that ENISA's work was mostly relevant to stakeholders' needs. It regularly reviewed its areas of activity to respond to emerging needs and remained agile by setting up ad hoc working groups. Stakeholders expressed a high level of satisfaction with how ENISA responded to changes in the cybersecurity landscape, although some felt that it needed more tools to effectively address the growing cyber threats in Europe. National cybersecurity authorities and smaller Member States benefited from ENISA's capacity building initiatives and regulatory insights. However, stakeholders noted that ENISA could further increase its relevance in some areas. To do this, they suggested that it improve its support and increase its visibility among various sectors and stakeholders, especially SMEs, which often find

it hard to meet cybersecurity requirements. Stakeholders also called for more sector-specific tools and resources, as well as insights and tools to tackle emerging threats.

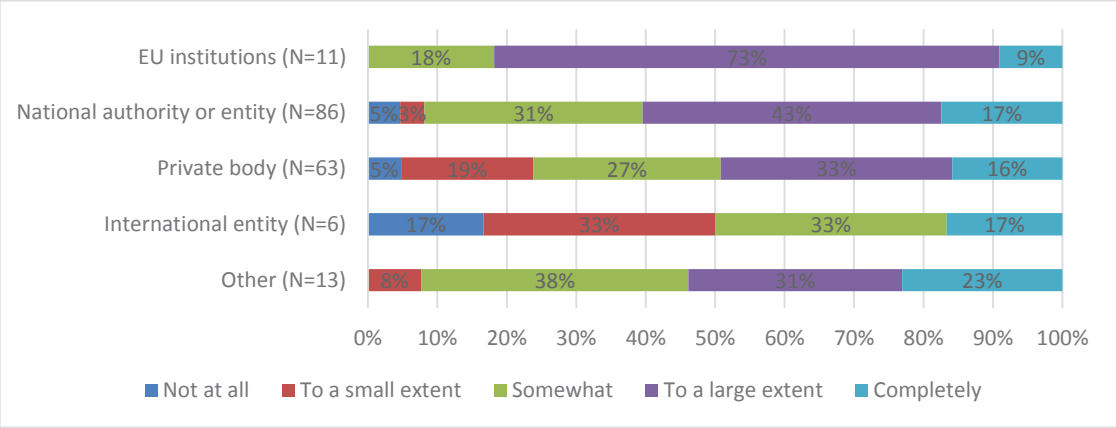
The stakeholders surveyed reported being satisfied with ENISA's ability to adapt to the changing cybersecurity landscape. Specifically, 74% of respondents mostly or strongly agreed that ENISA quickly adapted to changes in the cybersecurity landscape in 2019-2023, and 70% mostly or strongly agreed that ENISA sufficiently addressed all major unforeseen cybersecurity incidents during that period. There were no notable differences between the responses of different stakeholder groups.

While stakeholders acknowledged ENISA's efforts, some respondents felt that it needed greater capabilities to effectively address all cyber threats in Europe. Respondents argued that ENISA lacked an effective incident response unit and operational capabilities to act quickly in the face of cybersecurity incidents. They felt that these were not sufficiently supported by ENISA's mandate and governance structure. Some respondents stressed that directly managing cybersecurity incidents was not the purpose of ENISA and that it had no capabilities in this area. Instead, ENISA supports Member States in dealing with incidents, and those respondents pointed to successes in this context with the CSIRTs network. ENISA contributed to the EU's preparedness to face cyber threats by supporting and organising cyber exercises and by improving operational cooperation between Member States, including through its support to the CSIRTs network.

ENISA set up appropriate practices for stakeholder consultation and management, however industry stakeholders expressed dissatisfaction with the consultation and collaboration processes that involved them, as well as with the difficulty in accessing information.

While ENISA's outputs and services generally align with stakeholder needs, notable discrepancies exist in how different groups of stakeholders perceive ENISA's responsiveness to their needs. ENISA's support is perceived as most relevant by EU institutions, and relevant to a lesser extent by national authorities or entities and private bodies. The difference in the relevance of ENISA's work to its stakeholders was underlined by the varying level of satisfaction with its services and outputs. 44% of all respondents indicated that their needs were met only 'somewhat', 'to a small extent' or 'not at all'. This figure rises to 50% for respondents representing industry organisations, with a comparatively higher proportion of respondents selecting 'to a lesser extent'. This data suggests that there is still room for ENISA to tailor its efforts to better meet the needs of national organisations and private bodies.

*Figure 15 4 Relevance of ENISA's support to different groups of stakeholders*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 21 'Please indicate to which extent ENISA's activities and outputs contributed to the following aspects: ENISA's outputs and services correspond to my organisation's needs'.

National cybersecurity authorities and agencies valued ENISA's role as a key facilitator of cooperation and information exchange between Member States, as well as in promoting technical cooperation and a common standard of cybersecurity. They also valued the insights provided by ENISA on new regulations, guidelines, best practices and national requirements. Capacity-building initiatives were particularly appreciated by smaller Member States with more limited internal capabilities, while support for common standards proved particularly beneficial for EU candidate countries.

Representatives of international organisations, industry and vendors highlighted the importance of ENISA in representing the EU's position in the increasingly complex regulatory landscape of cybersecurity compliance and technical policy. ENISA's role in facilitating cooperation between different types of national and international stakeholders was described as crucial for ensuring a common understanding among different stakeholders. However, respondents called for ENISA to play a more direct role in providing tools and support to different sectors in order to increase its visibility and impact. ENISA could improve support for SMEs across the Digital Single Market to help such companies better integrate and comply with cybersecurity standards.

ENISA's support to EU institutions was well received, including its support in promoting situational awareness and crisis management. Its role in collecting information and liaising with Member States on cybersecurity was also valued. Respondents from the Commission expressed confidence in ENISA as a reliable implementing partner and a source of technical and operational expertise. ENISA has made contributions to national and EU policies and legislative initiatives, which have been generally well received by stakeholders. According to ENISA, its ability to provide policy support to the Commission is mainly hindered by a lack of qualified policy experts.

The role and purpose of ENISA in policy-related tasks were found to be clear and properly defined, as confirmed by 72% of the stakeholders surveyed. However, some stakeholders had expected ENISA's role in policy-related tasks to go beyond its current mandate.

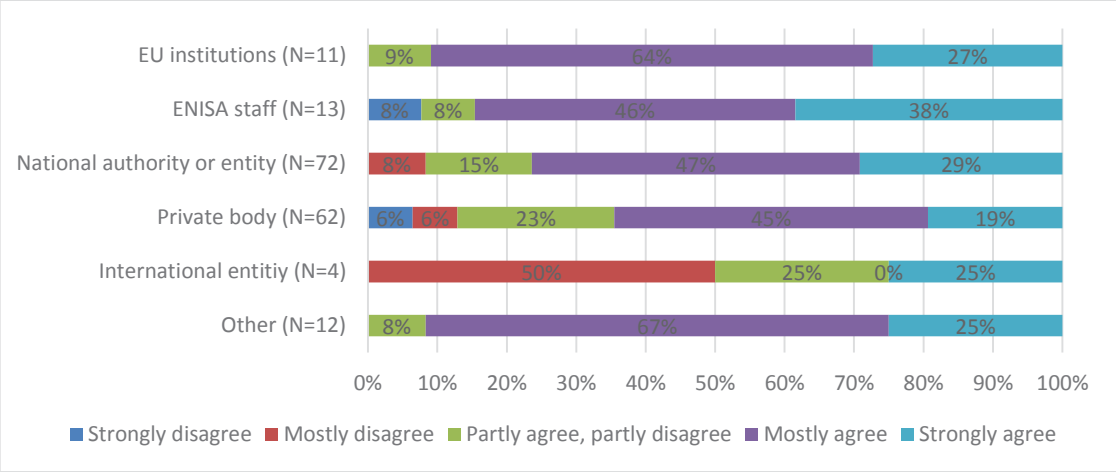
In summary, ENISA's relevance is well established, and its flexibility, strategic alignment and stakeholder engagement are valued. Nevertheless, stakeholders stressed that there is still significant room for ENISA to better meet their needs.

**Coherence**

ENISA played an active role in fostering cooperation and knowledge sharing among stakeholders, as confirmed by the results of the survey. Its efforts were thought to complement those of national cybersecurity authorities and CERT-EU, although some interviewees noted that there were areas of overlap. ENISA supported key EU networks such as CSIRTs and EU-CyCLONe, organised exercises such as CyberEurope, and facilitated the exchange of best practices through the NIS Cooperation Group.

Survey respondents provided a positive assessment of ENISA's efforts to exploit synergies in expertise and knowledge sharing with other stakeholders. Representatives of private bodies were somewhat less satisfied (65%) compared to other stakeholder groups (74% overall).

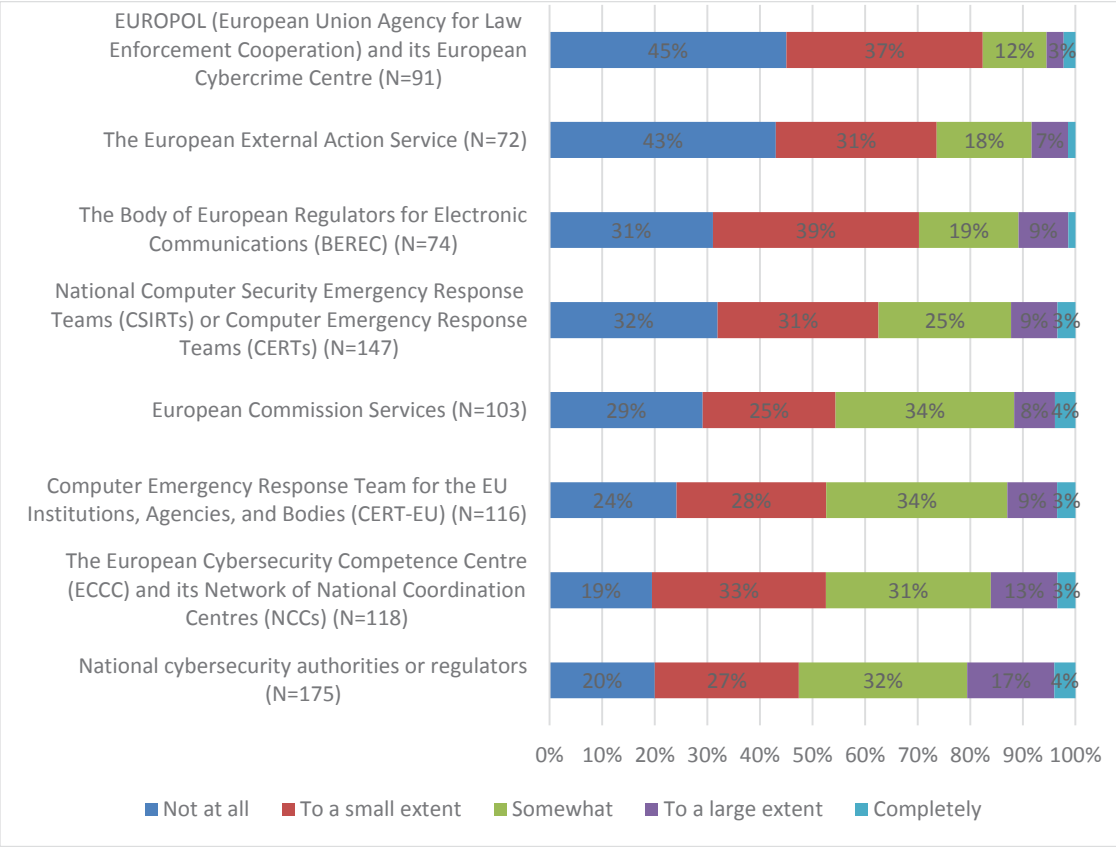
*Figure 16 5 ENISA sufficiently exploited synergies with other stakeholders*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, questions 15 and 23: 'Please indicate to what extent you agree or disagree with the following statements about ENISA: ENISA sufficiently exploited synergies with other stakeholders'

There were a few overlaps between the formal responsibilities of ENISA and those of other relevant stakeholders, but these activities were mostly carried out in a complementary way. Stakeholders saw the greatest overlap between ENISA and the national cybersecurity authorities, the ECCC, CERT-EU and Commission services. They identified a need to improve synergies between the responsibilities and actions of ENISA and those of other EU bodies. Responses to open-ended follow-up questions indicated that there were already complementarities with national authorities in policy-related tasks, risk management, capacity building and incident response, which were mutually beneficial. Some survey respondents underlined that, by formalising cooperation arrangements with other entities, such as EMSA and the JRC, ENISA could better leverage synergies and ensure a unified approach to cybersecurity initiatives.

*Figure 176 Overlaps between ENISA and other stakeholders in the field of cybersecurity*

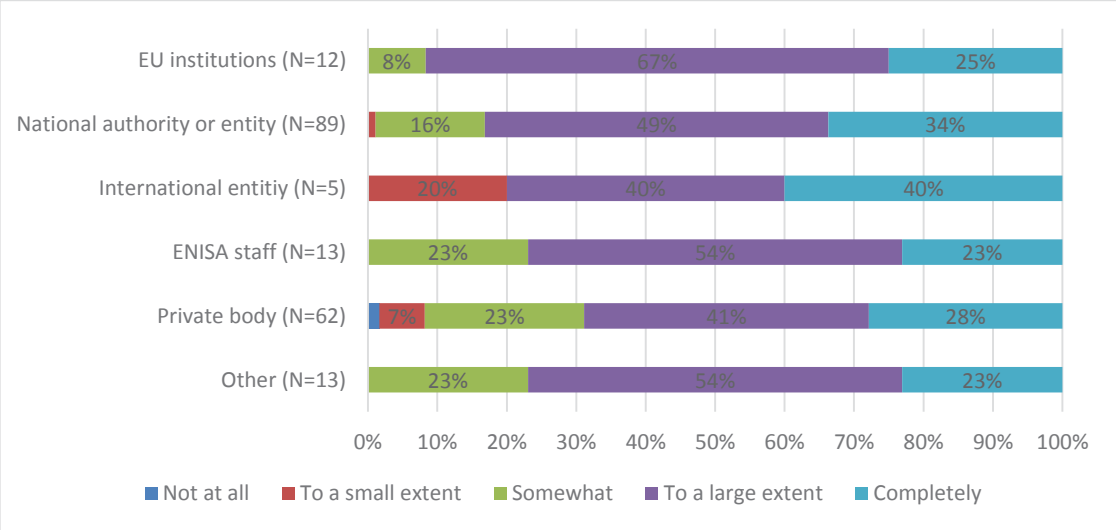



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 26 'In your view, to what extent, if at all, do ENISA's outputs and services overlap with those of the following institutions active in the area of cybersecurity?'

ENISA strengthened its cooperation with EU, regional and international stakeholders during the evaluation period. This was demonstrated by the increasing number of structured cooperation frameworks set up. Several MoUs were signed with other EU bodies to improve working arrangements and facilitate the sharing of knowledge, information and expertise. ENISA also signed a service level agreement with the ECCC in the fields of research, innovation and administration in 2022. This was followed by an MoU in 2023 to coordinate the implementation of operational tasks and research initiatives. Despite this, some survey respondents still see a need to further calibrate activities and increase coordination between both organisations.

ENISA facilitated cybersecurity cooperation at EU and national levels. Stakeholders had positive opinions of ENISA's promotion of cybersecurity cooperation, including information sharing and coordination, during the evaluation period. National authorities assessed ENISA's contribution to cybersecurity promotion especially positively, with 83% of survey respondents indicating that it had achieved this objective to a large extent or completely.

*Figure 18 7ENISA's contribution to promoting cybersecurity cooperation*

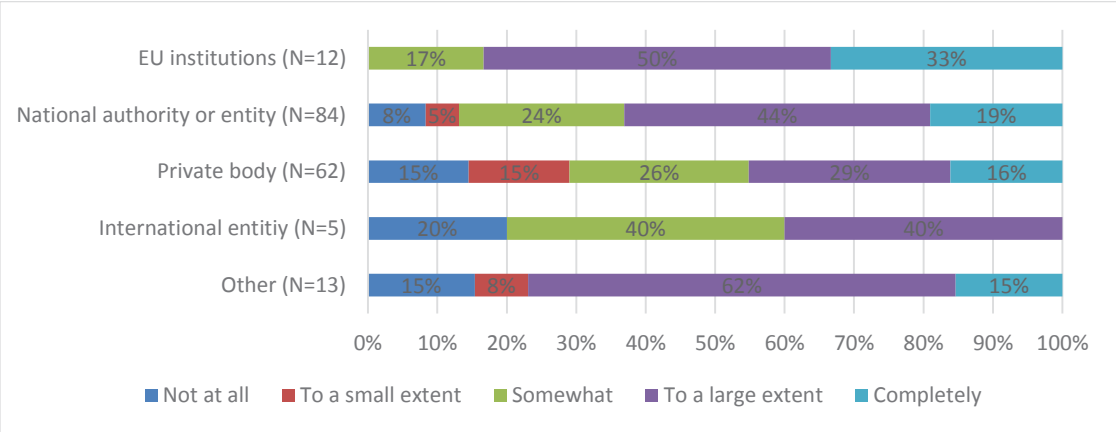



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 16: 'In your opinion, to what extent has ENISA achieved the following objectives during the period of 2019-2023? Promoting cybersecurity cooperation, including information exchange and coordination, at EU level between MS, EU institutions, bodies, offices and agencies and relevant private and public stakeholders'

ENISA also strengthened its regional cooperation with non-EU countries, particularly with the Western Balkans and Ukraine. ENISA set up working arrangements with the US Cybersecurity and Infrastructure Security Agency (CISA) in the areas of capacity building, exchange of best practices and increasing situational awareness.

Survey respondents and interviewees expressed that ENISA's interactions with private stakeholders and international partners must be more predictable and transparent to maintain confidence and foster collaboration. Around half the representatives of private bodies found ENISA's role in contributing to cooperation and coordination between stakeholders to be limited. In this context, private bodies suggested that ENISA could improve its outreach and stakeholder engagement activities and could expand its partnerships with global cybersecurity stakeholders, particularly as regards collaborating with industry representatives and non-EU countries.

*Figure 19 8ENISA's contribution to cooperation and coordination between stakeholders*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 21 'Please indicate to which extent ENISA's activities and outputs contributed to the following aspects: The activities of ENISA have improved the cooperation and coordination between my organisation and other stakeholders'

In summary, stakeholders found that ENISA demonstrated a solid foundation in promoting cybersecurity coherence in the EU. They thought that its structured cooperation frameworks, support for key EU networks and facilitation of best practice exchanges contributed to a coordinated and coherent approach to cybersecurity across the EU. Some recommendations included addressing current inefficiencies and improving inter-Agency coordination.

**EU Added Value**

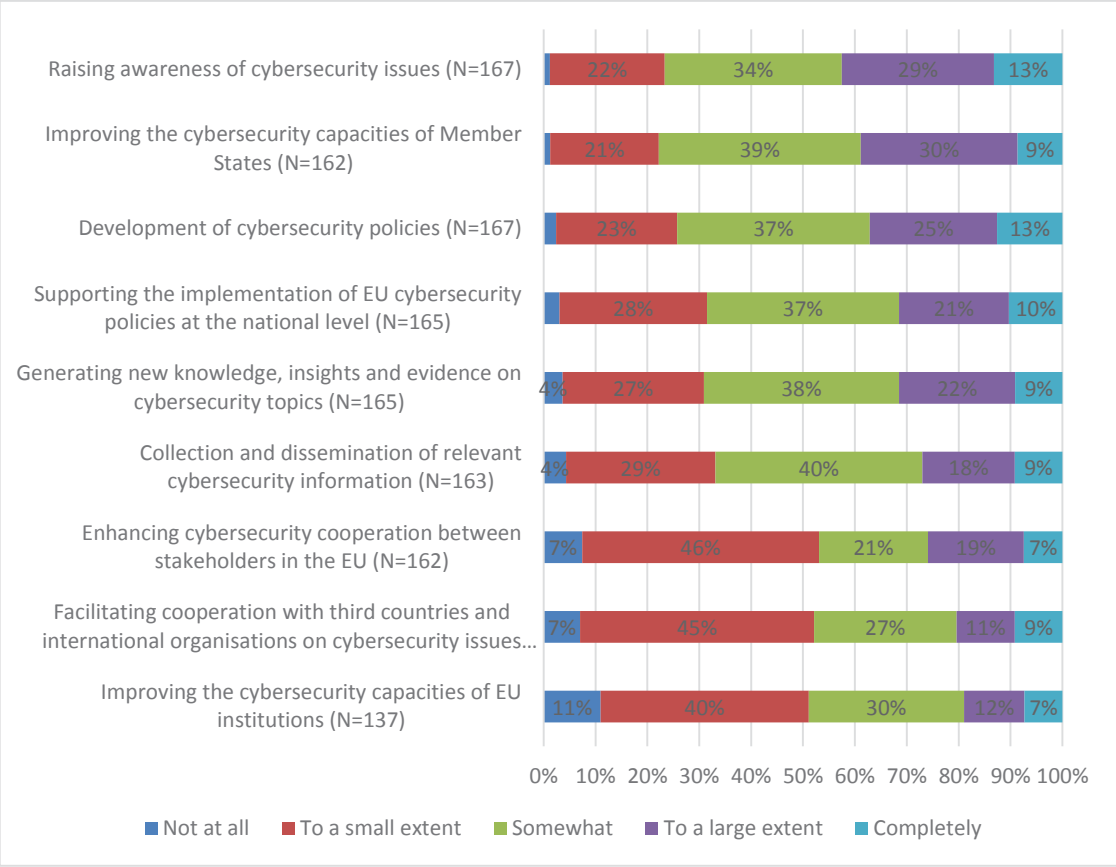
According to stakeholders and survey respondents, ENISA has made a significant contribution to the strengthening of the EU's cybersecurity ecosystem. It is seen as a central hub that has encouraged vital cooperation across the EU, supported national efforts, particularly in Member States with less mature cybersecurity frameworks, and helped align cybersecurity practices and policies. At the same time, stakeholders have identified areas where ENISA's impact could be reinforced.

ENISA's current configuration was considered optimal for maintaining independence and facilitating close cooperation with Member States. Stakeholders emphasised that ENISA's independence from political influence added great value.

ENISA's role in promoting convergence and harmonisation across the European cybersecurity landscape was achieved through active engagement with Member States, including the involvement of national experts in strategic and day-to-day discussions. ENISA coordinated with bodies such as CERT-EU, Europol and EC3 to produce joint reports, avoiding duplication and improving shared situational awareness. Agreements with other EU bodies, such as the ECCC and the European Union Agency for Railways (ERA), facilitated cooperation and avoided overlapping mandates. ENISA's secretariat roles in the CSIRTs network and EU-CyCLONe ensured continued coordination between and the effectiveness of these groups.

According to the survey, around two thirds of stakeholders considered that the collection and dissemination of relevant cybersecurity information, the generation of new knowledge, insights and evidence on cybersecurity issues and support for the implementation of EU cybersecurity policies at the national level would be hard to achieve without ENISA. Three quarters of respondents believed that improving Member States' cybersecurity capacities, and raising awareness of cybersecurity issues, would have little effect in the absence of ENISA. Around half of respondents believed that improving the cybersecurity capacities of EU institutions would be possible only to a small extent or would not be possible at all without ENISA. As for facilitating cooperation with third countries and international organisations, 45% of respondents said this would be possible only to a small extent without ENISA and 7% said it would not be possible at all. For enhancing cybersecurity cooperation between stakeholders in the EU, 46% said this would be possible only to a small extent and 7% said not at all.

*Figure 209 Achieving ENISA's objectives without ENISA itself*



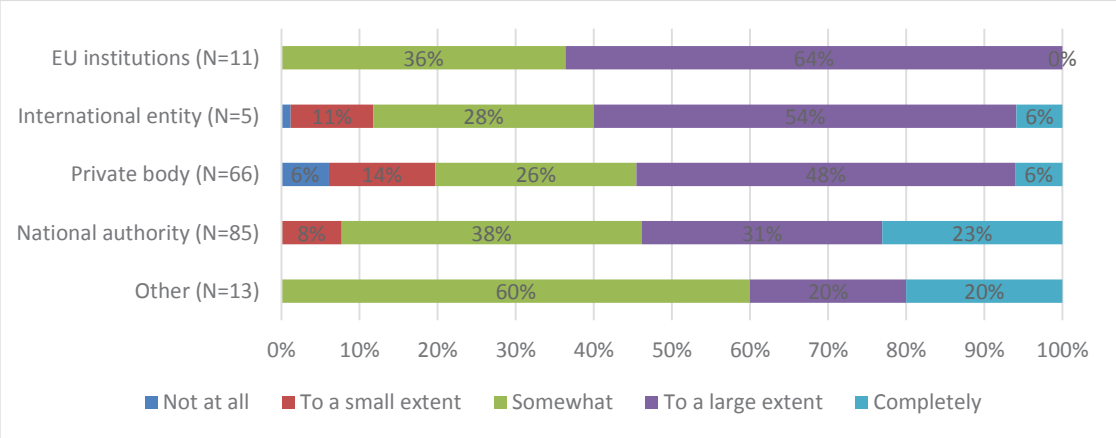

Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 34 'In your view, to what extent would the following results have been possible to achieve by Member States alone, without ENISA's involvement?'

Most respondents said ENISA provided clear EU-level added value to the cybersecurity of the EU. ENISA's specialised mandate, allowing it to act as a separate EU decentralised body, allowed for a dedicated and independent approach to cybersecurity. As an EU agency, ENISA's structure and governance allows for better and easier cooperation with Member States. Its

expertise continues to be important in addressing the complex and evolving threats facing the EU.

However, private entities were more critical of the idea that ENISA provided added value. For example, 6% of private bodies responded 'not at all' and 14% 'to a small extent' when asked about ENISA's added value to their activities, compared to 0% and 8% respectively among national authorities. ENISA's primary focus was on national authorities, making sector-specific outputs less visible and impactful. The overall impact of guidelines and events depended on the level of maturity and specific needs of the organisation ENISA dealt with. Major industry players with a longstanding commitment to cybersecurity found ENISA's activities aligned with their routine operations but lacked new insights, indicating that more could be done to tailor insights to the private sector's specific challenges. Companies reported that they often relied on International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standards rather than ENISA initiatives. Some organisations valued ENISA's technical guidelines, tools and reports but claimed several of them were redundant in the context of existing standards. Private stakeholders monitored ENISA's work in areas such as IoT security and cybersecurity certification to ensure consistency with international standards.

*Figure 21 10 Added value of ENISA's activities*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 35: 'Overall, to what extent has ENISA provided added value to the activities of your organisation during the period of 2019-2023?'

In the event of the withdrawal of EU action, the most likely consequences were expected to be increased difficulties in achieving trans-national coordination and the development of expertise in the field of cybersecurity. Overall, according to stakeholders, abolishing ENISA would lead to coordination challenges, less effective cybersecurity measures and potentially disjointed national approaches to cybersecurity issues.

ENISA is recognised for its specific focus on cybersecurity policy implementation, stakeholder engagement and comprehensive support to Member States, which positions it uniquely within the EU's cybersecurity landscape. While focusing on national authorities is essential, respondents said that ENISA could improve by increasing engagement with stakeholders and

collaboration with industry. They also suggested that increased resources and better prioritisation could help ENISA adapt to evolving cybersecurity challenges.

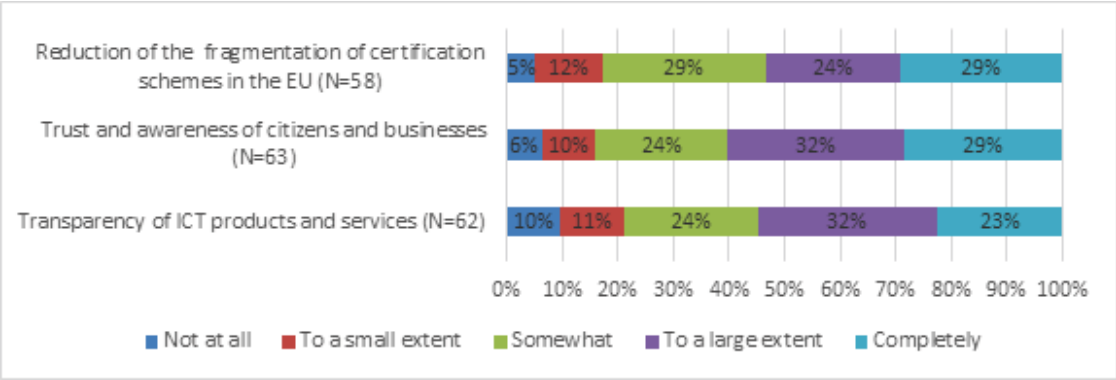
### ECCF survey results

### Effectiveness

The ECCF contributed only somewhat to improving the cybersecurity capabilities of Member States and private companies, according to the survey. 53% of stakeholders believed that the ECCF contributed only to a small extent to enhancing the capabilities and preparedness of private companies to face cybersecurity threats, while 19% did not consider the ECCF to have made any contribution to private companies at all. For Member States, 50% of survey respondents believed that the ECCF improved their capabilities only slightly, despite the establishment of national certification authorities across all Member States. The framework was considered to fall short in its ability to support national authorities in their efforts to increase national cybersecurity certification capabilities.

The survey results also indicated that delays in the adoption of certification schemes deeply affected the ECCF's ability to attain its objectives. Specifically, 55% of stakeholders believed that certification scheme delays negatively affected the ECCF's ability to improve the transparency of ICT products and services. Moreover, 61% said these delays negatively impacted the public's and businesses' trust in and awareness of cybersecurity, and 53% believed that delays hindered efforts to reduce the fragmentation of certification schemes within the EU.

*Figure 22 11 Objectives that were not reached according to stakeholders*



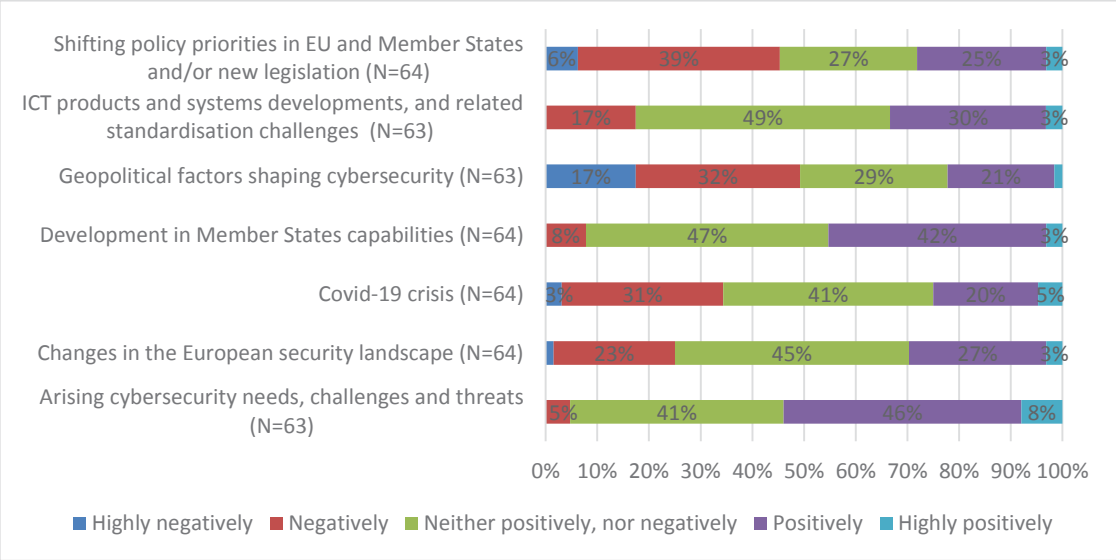

Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 48: 'Do you agree with the following statements'

Despite these challenges, according to the survey, 52% of respondents reported that the ECCF improved cooperation and coordination across Member States and EU institutions, bodies and agencies.

External factors also influenced the effectiveness of the ECCF. According to the survey, 46% of stakeholders said emerging cybersecurity needs, challenges and threats had positively influenced the ECCF's effectiveness; 42% of respondents indicated that the increase in Member States' capabilities in cybersecurity had had a positive impact on the ECCF. However, 45% of stakeholders considered that changes in policy priorities at the EU and Member State levels had

had a negative impact on the ECCF. Geopolitical factors were also significant, with 49% of stakeholders saying that they had impacted the ECCF negatively or highly negatively. The COVID-19 pandemic had had a slightly negative impact, according to 31% of survey respondents.

*Figure 23 12External factors influencing the ECCF's objective*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 49: 'In your opinion, to what extent have the following external factors positively or negatively influenced the ECCF in achieving its objectives?'

In summary, the ECCF's effectiveness in fulfilling its objectives was limited by resource imbalances, delays in adopting schemes and external factors such as changing policy priorities and geopolitical influences. While the ECCF improved cooperation and harmonisation among Member States and EU institutions, significant challenges remained in the drive to improve certification capabilities and reduce fragmentation across the EU.

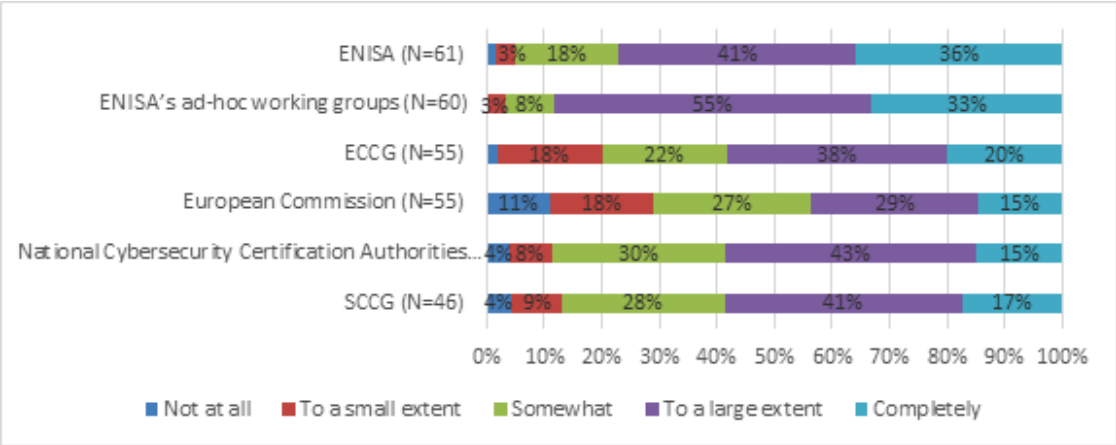
**Efficiency**

The efficiency of the ECCF was mostly impacted by content- and process-related issues. According to the survey, 77% of respondents reported that content issues, such as technical complexity or political impact, were the factor that most hindered the operation of the ECCF. 70% of respondents identified process-related issues, including the functioning of the preparation and adoption process, as significant obstacles to efficiency. Legal concerns, such as shortcomings in the legal framework at EU or national level, had less impact (identified by 43% of respondents).

As regards the EUCS scheme, 46% of survey respondents indicated that content issues, resulting largely from the politicisation of the debate, were the primary impediment to adoption. In the case of EU5G, 38% of stakeholders raised content-related issues and 32% attributed delays to process-related issues. The EUCC scheme was adopted in January 2024 after about 55 months of discussion, with delays attributed to technical complexity, lack of experience in developing schemes and changing policy priorities.

Survey respondents identified ENISA and its ad hoc working groups as the stakeholders that contributed most to the smooth functioning of the framework, with 77% and 88% of respondents respectively agreeing completely or to a large extent that these bodies had made a contribution. The ECCG, SCCG and NCCAs also garnered rather positive opinions, with 58% of respondents expressing a positive view for each of these stakeholder categories.

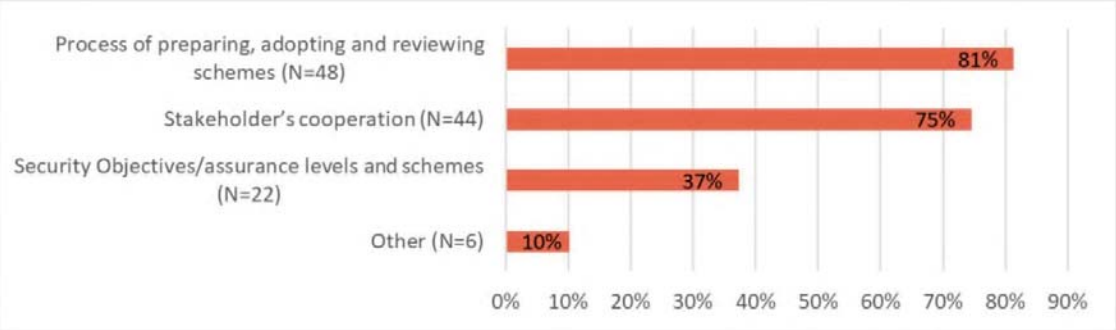
*Figure 24 13 Stakeholders' contribution to ensuring smooth functioning of the ECCF*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 51: 'In your opinion, to what extent have the following stakeholders and processes contributed to ensuring a smooth functioning of the ECCF?'

According to the survey, areas of the ECCF that could be improved include the process of preparing, adopting and reviewing schemes (suggested by 81%), stakeholder's cooperation (75%) and security objectives/assurance levels and schemes (37%).

*Figure 2514 ECCF improvements*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 64: 'Which of the following areas of the ECCF, if any, could be improved?'

Given the EUCC scheme was adopted only recently, it is too early to identify the costs borne or the benefits experienced by stakeholders in terms of compliance with ECCF requirements. However, survey respondents indicated some costs and benefits related to preparatory activities, such as the development of standards, capacity building, and awareness-raising.

In summary, while ENISA and ad hoc working groups were seen as positive contributors, improvements are needed in the area of stakeholder cooperation and decision-making transparency, as well as in process management.

**Relevance**

The ECCF is seen as highly relevant to the achievement of internal market objectives in the current cybersecurity landscape. Stakeholders said that, given the increase in the number and intensity of cybersecurity threats, EU cybersecurity certification is a valuable asset. Key aspects that make ECCF relevant include the closer level of EU cooperation, its contribution to the development of standards and the ability to require critical infrastructures and public procurement beneficiaries to become certified. Stakeholders emphasised ECCF's capacity to effectively improve cooperation between EU Member States and to streamline trade by providing a unified certification platform.

The ECCF's relevance is further underscored by references to it in other EU legislation, including the Cyber Resilience Act (CRA), the NIS2 Directive and the European Digital Identity Regulation, which were all pending adoption by the co-legislators or proposed at the time of the evaluation. The CRA is expected to be crucial in promoting the certification of software and products with digital elements. The ECCF has provided input to the development of new standards and to addressing gaps in existing ones, such as for the cloud and 5G.

The mutual recognition of certified products, services and processes across the EU is still considered an effective tool to reduce individual costs for enterprises, thereby strengthening the single market and facilitating trade within the EU. The ECCF was also identified as a platform for cooperation among Member States at the EU level, aimed at fostering comprehensive evaluation and coordination.

Survey respondents confirmed the relevance of the ECCF's scope. Specifically, 86% agreed that the scope of the ECCF is sufficient in terms of the elements within each scheme (security objectives, assurance levels and types of requirement) and 88% agreed that it is adequate to cover ICT products, processes and services.

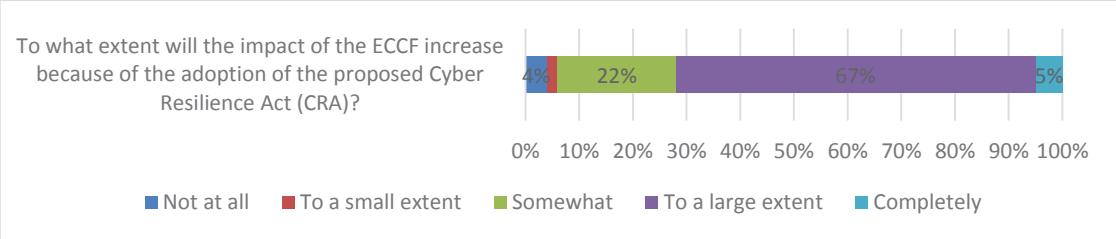
**Coherence**

The ECCF has demonstrated coherence with existing cybersecurity legislation and its operations are expected to be influenced significantly by the implementation of legislative measures such as the CRA, the European Digital Identity Regulation and the NIS2 Directive, according to the survey. Some stakeholders expressed concern about the risk of potential overlaps between the CSA and the CRA; this shows that real-world integration will be a challenge and will require oversight.

Ensuring the CSA's consistency with other EU policy and legislative measures, both cybersecurity-related (e.g. the NIS2 Directive and the CRA) and sectoral (e.g. the European Digital Identity Regulation), is essential for facilitating compliance and ensuring successful implementation of the ECCF. According to the survey, 83% of stakeholders found the framework to be coherent with existing instruments in the EU regulatory framework, with 55% answering 'fairly coherent,' 23% 'very coherent,' and 5% 'perfectly coherent.'

A broad majority – 72% of survey respondents – agreed that the then-planned adoption of the CRA would have a significant effect on the ECCF. The CRA is expected to introduce mandatory conformity assessment of cybersecurity requirements; existing certificates under an EU scheme may offer a presumption of conformity. While the CSA and CRA legal texts seemed fairly coherent, Member States stressed that it will be important to ensure a consistent implementation of the two acts.

*Figure 26 15 Impact of the CRA proposal on the ECCF*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 63: 'In your view, to what extent will the impact of the ECCF increase because of the adoption of the proposed Cyber Resilience Act (CRA)?'

Despite recognising the overall coherence, more than half of respondents (54%) identified overlaps between the ECCF and other EU initiatives. Stakeholder contributions indicated that this concern stemmed from a potential overlap with the CRA, which could result in a duplication of efforts and inconsistent requirements. Member States also reported a risk of overlaps and noted the challenges involved in aligning the ECCF with international and European standardisation processes. They emphasised the need to establish a communication channel with international standardisation organisations to leverage existing European or international standards and prevent inconsistencies between standards developed at the EU and international levels.

In summary, stakeholders found the ECCF to be largely consistent with the existing EU regulatory framework, but also highlighted the importance of ensuring consistent alignment with forthcoming legislation and avoiding overlaps with other initiatives. Continued attention to terminology and standardisation processes will be necessary to maintain coherence as the framework evolves.

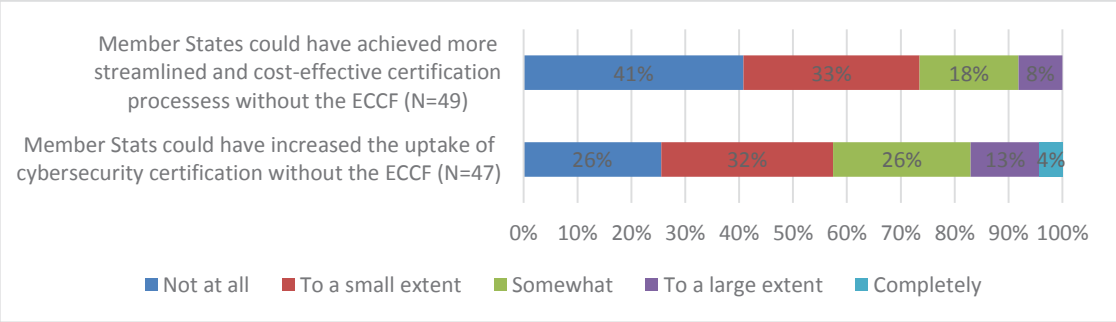
**EU Added Value**

Stakeholders broadly agreed that the ECCF brings clear EU added value compared to what could have been achieved by Member States alone. The framework's harmonised approach to cybersecurity certification across all Member States provides a common EU baseline of security requirements for digital products, processes and services within the EU single market. This builds trust among consumers and businesses and promotes cross-border cooperation. Most stakeholders recognised the added value of the ECCF in achieving a more secure, transparent and cohesive internal market for ICT products, services and processes.

According to the survey, 84% of stakeholders believed that Member States alone could increase the uptake of certification only to some extent or to a limited extent. Furthermore, 92% of stakeholders believed that Member States alone could not have achieved more streamlined and

cost-effective certification processes. For example, 41% of respondents said Member States could not have achieved more streamlined and cost-effective certification processes at all and 33% said they could have done so only to a small extent.

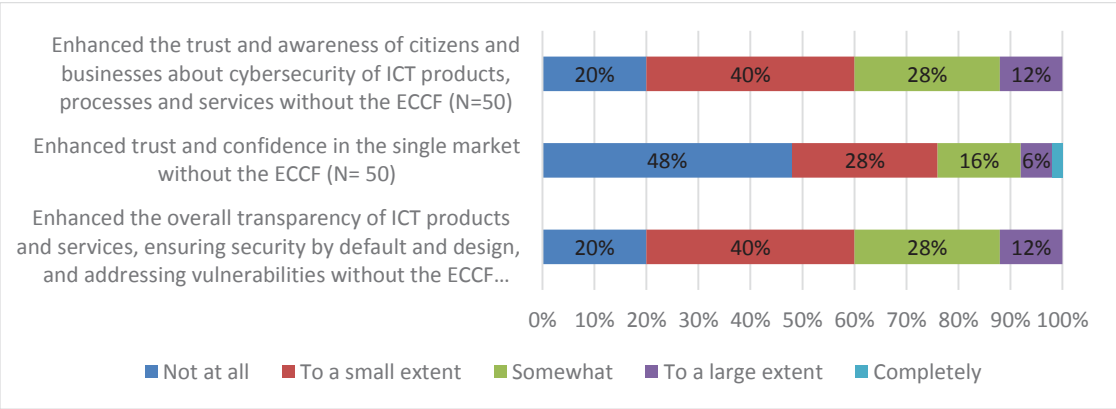
*Figure 2716 ECCF added value*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 60: 'Do you agree with the following statements?': 'Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have increased the uptake of cybersecurity certification more than what the ECCF has done' and 'Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have achieved more streamlined and cost-effective certification processes than what the ECCF has done.'

When considering the benefit of the ECCF on increasing levels of trust, 88% of stakeholders agreed that Member States alone might not be able, or able only in a limited way, to increase trust and awareness among the public and businesses about the cybersecurity of ICT products, processes and services. Additionally, 92% of stakeholders agreed that Member States alone could not have increased trust and confidence in the single market more than the ECCF had done. Regarding transparency challenges, 88% of stakeholders agreed that Member States alone could have increased the transparency of ICT products and services, ensuring security by default and design, only to a limited extent. For example, 48% of respondents said Member States could not have enhanced trust and confidence in the single market at all and 28% said they could have done so only to a small extent.

*Figure 2817 ECCF trust and transparency added value*




Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 60: 'Do you agree with the following statements':' Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have enhanced the trust and awareness of citizens and businesses about cybersecurity of ICT products, processes and services more than what the ECCF has done', 'Due to the delay in the adoption of European cybersecurity

certification schemes, Member States alone could have enhanced trust and confidence in the single market more than what the ECCF has done' and 'Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have enhanced the overall transparency of ICT products and services, ensuring security by default and design and addressing vulnerabilities more than what the ECCF has done.'

In summary, the ECCF's EU added value is widely recognised by stakeholders. The framework enables harmonised certification, increases trust and transparency and streamlines processes across the EU, achieving outcomes that would be difficult for Member States to accomplish on their own.

### 10.6. Targeted consultation (interviews)

As part of the evaluation of ENISA and the ECCF, a structured interview programme was implemented to collect qualitative insights from key stakeholders. In total, 49 interviews were conducted for ENISA and 13 interviews for the ECCF, involving a diverse range of participants including ENISA staff and representatives of the Commission, national cybersecurity authorities, industry associations and international organisations. The interviews were designed to complement the survey and the call for evidence by providing detailed perspectives on the implementation of ENISA's mandate, the functioning of the ECCF and the practical challenges and opportunities encountered by those directly involved in the European cybersecurity ecosystem.

**ENISA**

Interviewees consistently recognised ENISA's changing and increasingly central role in the EU cybersecurity landscape. ENISA was widely regarded as a trusted coordinator and facilitator, particularly valued for its support to Member States, its expertise in policy implementation and its contribution to operational cooperation. However, resource constraints were frequently mentioned as a limiting factor, with stakeholders noting that ENISA's expanding mandate and growing responsibilities were not always matched by adequate allocation or reallocation of financial and human resources. The agency's matrix-based organisational model and its governance structure were viewed positively, but interviewees called for further strengthening of internal coordination and prioritisation mechanisms to manage periods of high workload and to ensure the efficient delivery of outputs. Stakeholders from national authorities and EU institutions emphasised ENISA's valuable support in the implementation of cybersecurity policies, including the NIS Directive, the NIS2 Directive and sector-specific regulations. ENISA's technical guidance, best practice-sharing and capacity-building initiatives were cited as particularly beneficial for smaller Member States and as being effective in harmonising approaches across the EU. However, some stakeholders expressed a need for more tailored, sector-specific guidance and for better dissemination of ENISA's outputs to ensure they are taken up in practice by a wider range of stakeholders.

The interviews highlighted ENISA's added value in fostering cooperation and knowledge-sharing among Member States, EU institutions and other stakeholders. The agency's role as a facilitator of networks such as the CSIRTs network and EU-CyCLONe was also appreciated. Nonetheless, several interviewees identified areas for improvement, including the need for more structured and regular engagement with industry, SMEs and civil society, as well as greater transparency and inclusiveness in stakeholder consultations. Some stakeholders suggested that

ENISA could further strengthen its engagement with international partners and standardisation bodies to augment the global relevance of EU cybersecurity policies and certification schemes.

Across all interviews, there was a clear call for greater clarity, flexibility and resourcing at both the EU and national levels. Stakeholders recommended beefing up ENISA's mandate and resources to enable the agency to fulfil its expanding responsibilities, particularly in the areas of operational cooperation, policy support and certification scheme development. Suggestions included formalising ENISA's leadership in key networks, improving internal coordination and increasing the frequency and depth of stakeholder engagement. Interviewees also emphasised the need for ongoing investment in capacity building, knowledge-sharing and the development of sector-specific guidance.

**ECCF**

Interviewees provided detailed feedback on the implementation and governance of the ECCF. While the framework was recognised as a valuable tool for harmonising cybersecurity certification across the EU, stakeholders identified several challenges. Delays in the adoption of certification schemes, particularly the EUCC and EUCS, were attributed to complex technical requirements, political sensitivities and coordination difficulties among Member States and EU institutions. Industry representatives and national authorities expressed concerns about insufficient involvement in scheme development, limited transparency in decision-making processes and the need for clearer roles and responsibilities among key actors, including ENISA, the Commission and the ECCG and SCCG groups.

Interviewees also highlighted the importance of aligning certification schemes with international standards and ensuring consistency with other EU legislative instruments, such as the NIS2 Directive and the proposed CRA. The voluntary nature of schemes was not seen as a major problem, but the lack of experience in developing certification schemes contributed to delays and uncertainty. Stakeholders called for more structured engagement in the framework through clear processes and realistic timelines, as well as for regular meetings with clear objectives and sufficient time to prepare.

There was a strong emphasis on the need for more effective mechanisms to resolve political and technical deadlocks during scheme development, as well as for greater transparency and information-sharing throughout the process. Interviewees stressed that the ECCF's added value would only be fully realised if these governance and operational challenges were addressed, enabling the framework to deliver on its promise of a harmonised and effective European cybersecurity certification landscape.

### 10.7. SWOT and recommendations workshops

As part of the evaluation process for ENISA and the ECCF, two dedicated workshops were organised to facilitate collaborative analysis and gather targeted recommendations. These workshops brought together a wide range of stakeholders, including experts from academia and representatives from ENISA, DG CNECT, Member States and the study team. The workshops were conducted online and structured to maximise technical exchange, validation of findings and the formulation of actionable suggestions for future improvements.

#### 10.7.1. *SWOT Workshop*

The SWOT workshop was held on 21 May 2024 via MS Teams, with 32 participants, including six study team members. The objective was to conduct an analysis of ENISA and the ECCF, using data collated by the study team and direct input from stakeholders. The workshop aimed to improve understanding of the strengths, weaknesses, opportunities and threats facing both ENISA and the ECCF and to foster dialogue on potential improvements to the Cybersecurity Act.

**ENISA SWOT Results**

Stakeholders confirmed the strengths identified by the study team, including ENISA's positive reputation within the EU cybersecurity community, the quality of its publications, effective collaboration among Member States, harmonisation efforts and capacity building. Its weaknesses were also attested, including resource shortages, strategic rigidity, potential delays, lack of clarity of ENISA's policy role and limited operational support. Opportunities identified included increased impact and services, collaborative training initiatives, the harmonisation of standards, policy engagement and an expanded mandate for more direct operational roles. Threats discussed included rapid technological advancement, the proliferation of funding initiatives, unexpected resource constraints, complacency and geopolitical instability.

**ECCF SWOT Results**

The ECCF SWOT analysis was similarly confirmed by participants. Strengths included boosting cooperation at EU level, adaptability to evolving technologies and legislative frameworks, the ability to mobilise experts and contribute to the development of standards, ENISA's capacity to ensure smooth scheme adoption, its relevance for internal market objectives and the added value of EU action. Weaknesses raised were the time-consuming scheme adoption processes, complexity in scheme development, susceptibility to geopolitical pressure and policy priority changes, a perceived lack of involvement of industry and external stakeholders and an unproven capacity to support cybersecurity preparedness and transparency.

Opportunities identified included greater flexibility and usefulness in tackling emerging threats such as artificial intelligence, strengthening Member State capabilities, the possibility of using certification as a presumption of conformity, potential mandatory requirements from upcoming legislation, the extension of its scope to managed security services, and providing impetus to standardisation processes. Threats included a lack of resources, potential shifts in policy priorities, increasing geopolitical instability, the risk of overlaps with other EU legislation and a risk of internal market distortions due to national cybersecurity requirements.

#### 10.7.2. *Recommendations Workshop*

The recommendations workshop took place on 12 July 2024, also via MS Teams, with 77 participants, including seven study team members. The aim was to gather ideas for improving the performance of ENISA and the ECCF, drawing on the evaluation results and stakeholder input.

**ENISA Recommendations**

Polling results showed an average score of 3.9 (on a scale from 1 (not at all) to 5 (completely/fully agree)), indicating general agreement with the evaluation findings but with some reservations, particularly regarding efficiency and internal governance. Stakeholders emphasised the need for adequate financial resources and stressed the importance of maintaining a clear focus within the mandate to avoid resource dilution. Coordination with other bodies such as ECCC, EU-CyCLONe and CSIRT was highlighted as a way of avoiding duplication and improving efficiency.

Suggestions for governance included creating platforms for Member States to share information, streamlining the production of reports and balancing ENISA's advisory and executive roles. The importance of seconded members from Member States for increasing alignment with national priorities was noted, though retaining qualified staff remains a challenge. Stakeholder engagement should be efficient and tailored to different audiences, with feedback systematically incorporated into future planning.

ENISA's position in the EU cybersecurity landscape could be strengthened by it prioritising services and support to Member States, acting as an impartial facilitator and fostering robust cooperation with bodies such as the ECCC. Suggestions were also made for ENISA to establish cooperation with US entities such as MITRE[285] and NIST (regarding the NVD)[286] to improve threat intelligence and vulnerability management.

**ECCF Recommendations**

Polling results for the ECCF averaged 3.8 (on a scale from 1 to 5), indicating general agreement with the evaluation findings, but revealed more disparate views on coherence and added value. Discussions focused on the future purpose and scope of EU certification, with participants divided on whether the ECCF should address non-technical threats. Some argued for keeping the framework technical while others saw value in using certification to address strategic issues.

Process improvements were suggested across all stages of scheme development, including early preliminary assessments, realistic timeframes, increased involvement of the ECCG and early legal advice from the Commission. Greater independence for ENISA in scheme development and limiting political elements were also recommended. Simplifying administrative processes and considering the elimination of implementing acts for voluntary schemes were proposed to streamline adoption. Participants discussed the future roles of stakeholders, including the role of the ECCG in the maintenance of the schemes. Alignment with existing standardisation efforts was emphasised, as was the need for more industry involvement and input from independent experts.

[285] https://www.mitre.org/
[286] https://nvd.nist.gov/

# ANNEX 9: REGULATORY GAPS

Since the adoption of the CSA in 2019, the cybersecurity threat landscape has changed significantly with the increasing sophistication and speed of cyber-attacks, impact of emerging and advanced technologies. The EU cybersecurity regulatory landscape evolved considerably since 2019 (and the adoption of the CSA), with of key legislative acts, recommendations and policies like the NIS2 Directive, Cyber Resilience Act (CRA) and Cyber Solidarity Act (CSoA), the EU Cyber Blueprint, the 5G Cybersecurity Toolbox and the Cybersecurity Skills Academy. There are also other sectoral legislations that include elements relevant to support cybersecurity objectives. Each of the instruments is filling regulatory gaps or setting new policy objectives. The interplay between those new instruments and the CSA is presented in the picture below.

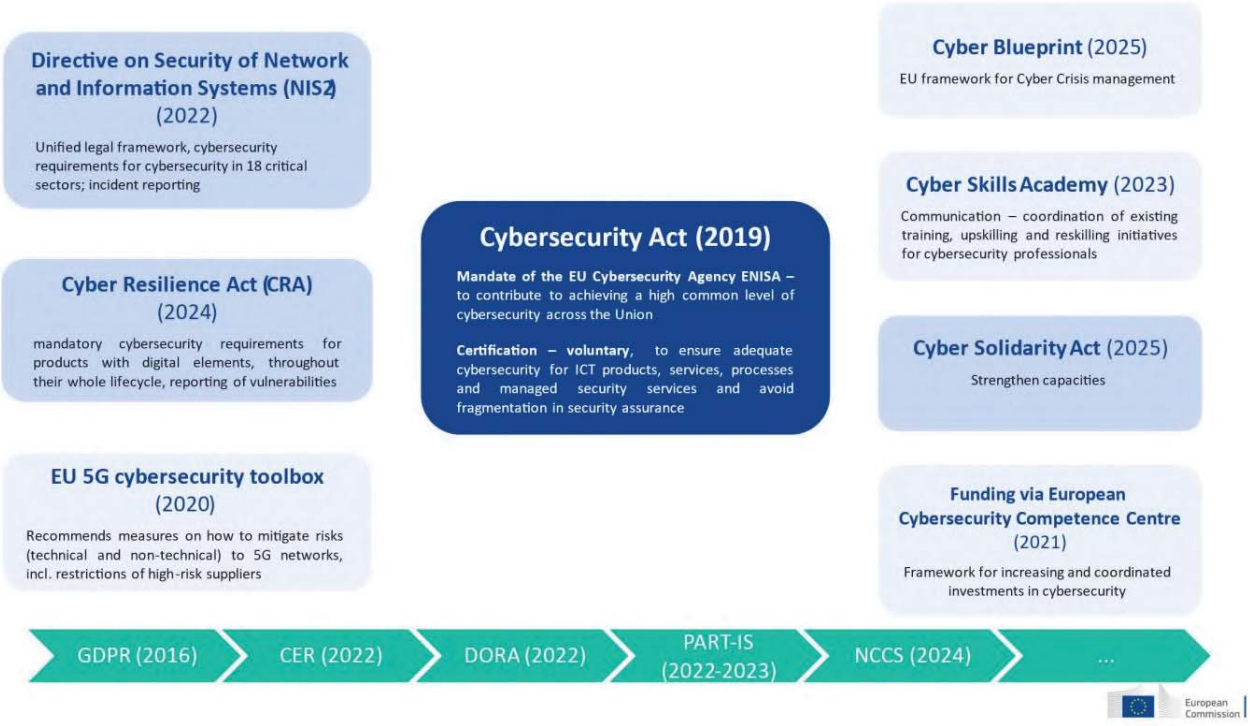



*Figure 29 Cybersecurity regulatory landscape and the place of CSA (2025 before CSA revision)*

(1) More specifically, the following main regulatory gaps were identified:

- **The Cybersecurity Act (2019)** provides for an ***ENISA mandate*** and sets a framework (***ECCF)*** for the development, at EU level, of voluntary European cybersecurity certification schemes for specific ICT products, services, processes, and, through a later amendment, for managed security services, to ensure an adequate level of cybersecurity and avoid fragmentation and for which ENISA plays a key role.

  *Limitations of the mandate of ENISA:*

  - **ENISA's mandate does not provide for the possibility to effectively support Member States in mutual assistance and information exchange at EU level for**

**potential cross border incidents**. Meanwhile, capabilities are uneven in Member States: a number of Member States already have large cyber agencies, less mature Member States lack the capacity. With an average 179% percent increase in supply chain attacks[287] (which by nature are cross border) and where the time to exploit due to Artificial Intelligence is significantly shorter, Member States cybersecurity agencies and CSIRTs need to share even faster information about incidents (e.g. indicators of compromise) as well as mitigation measures with critical entities. Discussions in the NIS Cooperation Group on the implementation of supervision and mutual assistance revealed that "*Member States face difficulties in applying this provision in the absence of standardised procedures and coordination efforts"* at Union level.

- **Lack of efficient tools and mandate of ENISA for EU wide situational awareness on cybersecurity:** Today, the cyber situational awareness is fragmented along national lines. Additionally, after Brexit, the EU is not part of the main intelligence network (the 5 eyes agreement between the US, CAN, UK, NZ and AU). There is therefore an urgent need to build up a European capacity for a shared and agreed EU cyber situational awareness. Given the sensitivities of Member States on information exchange, it is considered that – ENISA operating within a hybrid governance with Member States – is more acceptable for Member States than any other more structural change that would be granted to the Commission. Empowering ENISA with such a competence appears therefore to be the least resistance path to increase cyber posture. However, the current mandate of ENISA does not provide for a clear task, adequate tools or a stable resourcing to effectively support and bring significant added value to the **operational cooperation** among Member States such as the shared Union situational awareness of the cybersecurity threat landscape.
- **Dependency on a single third country's vulnerability management system:** The publicly available catalogue Common Vulnerabilities and Exposure (CVE) is a key element of vulnerability management and essential for cybersecurity risk management worldwide as it keeps an updated repository of known vulnerabilities, including a unique identifier and patches (where they exist). Today, CVE is the global reference standard and depends on a repository run by a US association – MITRE – which is dependent on the US government funding. This creates a strong dependency of and single point of failure for the EU cybersecurity ecosystem. The recent threats to the funding of MITRE have highlighted the urgency and importance of ensuring a European equivalent system and reducing this strategic dependency. Today, the current mandate of ENISA does not allow for ENISA to play a more prominent role in the vulnerability management at Union level and the CVE process on international level.

[287] CheckPoint, *What is a supply chain attack?*, https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-a-supply-chain-attack/#:~:text=Supply%20Chain%20Attacks%20Are%20Surging,semiconductor%20companies%20increased%20by%20179%25.

- **Lack of effective framework to support closing the cybersecurity talent and associated skills gap:** the gap in the cybersecurity workforce grew from an estimated 274,000 in 2023 to 299,000 in 2024[288]. What is more, the companies, and especially SMEs encounter difficulties to hire people with adequate competences in cybersecurity[289]. ENISA's current mandate on skills is limited to capacity-building activities and lacks appropriate tools and resources to effectively promote the European Cybersecurity Skills Framework among stakeholders (Member States, industry, academia), nor to ensure that the ECSF is the reference framework to the skills and competencies recognition associated to cybersecurity role profiles. Currently, individual certifications recognised on the market are rather coming from a handful of non-European private players and prove expensive for individuals to obtain. A mandate for ENISA does not allow to run an EU attestation mechanism that could be used by individuals to demonstrate having cybersecurity competences and skills and for Member States and industry to have a clear reference framework.
- **Lack of tasks to support European and international standardisation work related to the CRA, the ECCF as well as to the efforts to EU-US work on ensuring mutual recognition of cybersecurity standards.** Standards play an essential role in facilitating compliance and supporting industry in the implementation of cybersecurity policy at European level. It is also a cornerstone to promote technical alignment and mutual recognition with important international partners, such as the United States, as outlined in the 2025 EU US Joint Statement on transatlantic trade and investment[290]. ENISA's mandate does not provide for the clear tasks and resources to reflect such needs. In particular, the mandate does not explicitly entitle ENISA to engage and contribute to standards development activities at European and international level and does not envisage a role for ENISA in drafting and maintaining technical specifications to support Union legislation, and in particular the CRA and ECCF. In particular, because of the nature and the broad scope of the CRA (covering all hardware and software products), its implementation will involve considerable technical work on standards and technical guidance over time, that cannot be achieved without extensive support from ENISA.
- **Insufficient and unsustainable resourcing model:** ENISA is small in size compared to other Union security agencies. Since 2019, the Commission has added tasks and resources to ENISA through contribution agreements, effectively increasing staff count from 130 [291] in the establishment plan to 148. It should also be mentioned that the transfer of additional resources to ENISA via contribution agreements generates additional overhead costs of their conclusions and management for ENISA and the Commission. Different legislative acts, adopted post CSA, provide for specific tasks for ENISA, such as the administration and organisation of the EU Cybersecurity

[288] ISC2, *First Look at the 2024 Cybersecurity Workforce Survey*, https://digital-skills-jobs.europa.eu/system/files/2024-12/ISC2_Workfoce-Study-Findings-EU.pdf.
[289] Eurobarometer (2024) on Cyberskills, https://europa.eu/eurobarometer/surveys/detail/3176.
[290] Examples include the EU-US Action Plan for Cybersafe products signed in January 2024 and the recent announcement of a mutual recognition agreement on cybersecurity between the EU and US.
[291] 82 FTE from establishment plan for 2025 + 32 contract agents and 15 seconded national experts = 130.

Reserve or reviewing incidents within the European Cybersecurity Incident Review Mechanism by the CSoA, setting up and managing the vulnerabilities platform, establishing a single reporting platform or supporting Member States' market surveillance activities under the CRA. Without a clear overreaching take of how such tasks fit together, **ENISA's ability to prioritize resources effectively is impacted, leading to operational inefficiencies**. Furthermore, ENISA currently does not have the capacity to generate own resources. The current mandate lacks a legal basis for ENISA to request *fees* to sustain activities that serve enhancing the cybersecurity of the Union, reflecting also the conclusions of 2023 report from the Court of Auditors.

*Limitations of the ECCF:*

- **Legal shortcomings** in the Cybersecurity Act relating to the scope and risks covered, as well as procedural aspects. This has led to delays and blockage in schemes development on key technologies (cloud and 5G) and a lack of agility to rapidly respond to technological advances and market needs. In this context, Member States are proceeding with the adoption of national schemes leading to increased market fragmentation and undermining Europe's technological leadership.
- The ECCF was designed to provide a harmonised level of cybersecurity for ICT solutions **but does not allow for a mechanism to address non-technical risks**[292]. There is in general a lack of clarity as to what type of risk are in the scope of the framework. Regarding the development of European cybersecurity schemes, currently the technical preparation of the two schemes related to cloud services (EUCS) and related to 5G (EU5G) are fully on hold due to concerns and uncertainty related to how non-technical risks, would be addressed.
- The **scope of the ECCF** has not been future proof to meet the legislative and market demand in terms of security assurance. The limited scope (covering ICT products, services and processes) already required an amendment to the CSA to include the possibility to certify managed security services. Furthermore, the framework **does not allow to certify cyber posture of entities**, allowing to demonstrate compliance with the organisation cybersecurity measures, i.e. set out by the NIS2 Directive *(see below)* and other relevant Union legal acts in the future, such as GDPR.
- The framework lacks attributing clear **ownership to the actors involved in the strategic planning,** development **procedure** and does not specify a **maintenance framework** for adopted scheme. This results in **strategic planning** (i.e. *'Union Rolling Work Programme'*) and development procedure being vulnerable to delays. In

[292] Such non-technical risks may be linked, but not limited, to the jurisdiction to which the supplier is subject, the characteristics of its corporate ownership and the links of control by a third-country government where it is established, in particular where a third country engages in economic espionage, carries out malicious cyber activities or campaigns against the Union and its Member States, or engages in irresponsible state behaviour in cyberspace, and its legislation allows arbitrary and possibly extraterritorial governmental access to any kind of company operations or data, including commercially sensitive data. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency.

addition, there is a risk of adopted schemes quickly becoming outdated, and the credibility of European scheme being undermined.

- The EUCC has evidenced the need to entrust ENISA with the **maintenance** of the scheme that involves mostly technical work. In practice, the maintenance of the EUCC, includes the drafting and maintenance of more than 50 **technical specifications** (so-called state-of-the-art documents that interpret the Common Criteria evaluation standards for specific use cases) supporting and referenced in the scheme[293]. Furthermore, there is currently no legal basis in the ECCF that technical specifications drafted by ENISA can be directly referenced for European cybersecurity certification schemes. This leads to burdensome legislative procedures of amending schemes (since its adoption in 2024, the EUCC is now undergoing its second amendment). In the absence of clear role for ENISA and legal basis in this area it is unclear how the maintenance both of the EUCC and of future schemes would be sustained and financed.
- Furthermore, the **global impact** of the European cybersecurity certification framework requires to explore technical alignment where possible with other international frameworks and to engage and contribute to international standardisation activities. Engaging meaningfully in the contribution of international standards both for the EUCC and other schemes in the future requires a clear tasks and appropriate resources for ENISA. This is ever the more needed to deliver on the commitment to mutual recognition of cybersecurity standards in the context of the EU US joint statement on an agreement on reciprocal and fair and balanced trade,

- **Simplification:** The revision of the CSA also represents an opportunity to contribute to the Commission's simplification and burden reduction agenda. **The Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive)** – *in force since January 2023, with the transposition deadline due on 17 October 2024* – mandates Member States to ensure that entities operating in highly critical and other critical sectors implement cybersecurity risk management requirements, including supply chain security measures, and report significant incidents.

  *Limitations:*

  - With the NIS2 being a Directive, there are diverging national transposition frameworks for cybersecurity risk management, which poses an issue for companies operating in and having to **demonstrate compliance in several Member States leading to important administrative burden**. Member States impose different levels of compliance proof requirements *(e.g. audits, testing)* which poses challenges notably to entities operating in multiple Member States. Currently there is no tool in NIS2 or ECCF to allow a levelling of the playing field for demonstrating compliance with NIS2 when it comes to supervision requirements across Member States.

[293] See ENISA website, https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en#state-of-the-art-documents-for-eucc.

- The NIS2 Directive provides for **minimum harmonisation.** Even when the EU adopts an implementing regulation to harmonise these cybersecurity risk management measures, Member States can still gold plate. This is a constant concern flagged by the industry, which may need to comply with 27 different implementation models, standards and requirements. In line with the **recommendations of the Draghi report,** the CSA will amend the NIS2 directive, ensuring maximum harmonisation when an implementing regulation is adopted.
- There are also certain **unclarities surrounding the scope and definitions** in NIS2. One example is the reference to the definition of electricity producers without any further specification, which leads to the interpretation that any medium-sized entity owning solar panels should be treated as producer of electricity and thus subject to NIS2 Directive. The use of guidelines to clarify the issue will not provide for sufficient **legal certainty**. What is more, smaller and medium companies in certain sectors are currently treated as essential entities under the NIS2 Directive leading to quite significant documentation requirements in comparison to the impact of the entity on the market and overall cybersecurity. This may concern documentation requirements for around 20.000 companies. Introducing clarification on definitions and the types of entities provides legal certainty and ensures a contained scope of application reduced with an estimated number of 24.500 entities, a large proportion of which would be medium-sized entities. Furthermore, reducing the scope by removing the approximately 6.200 [294] micro and small DNS service providers would address the concerns of both Member States authorities that would have been required to supervise an important number of small market players for which complying with the requirements of the NIS 2 Directive would have constituted an important financial and organisational burden. This would support the Commission's goal to cut administrative costs by 25% overall and by 35% for SMEs.
- When it comes to **ransomware reporting**, divergent requirements cause authorities to have a disjointed overview of the landscape of such incidents, whereas entities face diverging requirements between Member States. NIS2 currently does not require or empower to specify further notification of the information necessary to effectively combat the prime threat of ransomware, such as ransom payments. Such information, paired with other relevant information, could significantly contribute to effective incident response and investigation of ransomware incidents, including the tracing of payments on cryptocurrency exchange platforms in order to identify the recipients. This would also enable the Union to gain an overview of the damages caused by ransomware attacks.

As a matter of clarification, as regards the interplay with the **CER Directive**, mention should be made that the latter requires from Member States to identify the critical entities from the list of sectors, while NIS2 Directive applies to all entities from the list of sectors where these meet a certain threshold. Also, while any entity identified as critical in accordance with the CER

[294] The estimation of the number of affected DNS service providers and number of entities affected by clarifying and the definitions and types of entities is based on an extrapolation of the number of essential and important entities that five Member States notified the Commission of pursuant to Article 3(5) of the NIS 2 Directive.

Directive becomes a NIS2 entity, NIS2 entities are not automatically critical entities under CER. Therefore, while enhancing the legal clarity by way of fine-tuning and adjustments to the scope of the NIS2 Directive is necessary due to the size-cap approach enshrined in NIS2, it does not directly affect the CER Directive.

- **ICT Supply Chain Security:** The growing presence of digital technologies in supply chain has increased the attack surface, given especially the fast penetration of Chinese technologies as well as dependencies on non-EU technologies in general. The current cybersecurity framework does not reflect sufficiently non-technical risks and where reflected; those measures are of a non-binding nature. As evidenced by the 5G toolbox, attempt to address such risks through non- binding instrument has led to fragmentation.

  *Limitations:*

  - **The current EU regulatory framework addresses only technical risks.**
  - The NIS2 Directive imposes on entities operating in key sectors obligations to apply **appropriate** organisational risk management measures in relation to the supply chain security. When applying these measures, the entity should take into account the results of Union level coordinated security risk assessments where non-technical risk factors can also be addressed. However, there is no legal obligation for entities to comply with the identified mitigating measures.
  - **In the field of the electronic communications sector, the 5G cybersecurity Toolbox** recommends measures on how to mitigate risks (technical and non-technical) to 5G networks including recommending restrictions or exclusions of high-risk suppliers.
    - While the 5G cybersecurity Toolbox is a robust, risk-based approach to the 5G networks security, it remains a policy and a non-binding document developed and agreed with Member States. According to the Second Progress Report implementing the EU Toolbox on 5G Cybersecurity[295], only thirteen Member States have implemented restrictions on high-risk suppliers. In addition, the scope of potential restrictions on high-risk suppliers is fragmented across Member States[296] which opens the door to vulnerabilities that could affect the entire network. Only ten Member States require information for 5G equipment sourcing. This means that very likely a majority of Member States' authorities have no clear picture of which suppliers are present in the deployed networks. These divergences create fragmentations in the Single Market and weaken the security of networks as a whole.
    - The 5G cybersecurity Toolbox does not cover other ICT supply chains. While there is a possibility to develop similar recommended measures under the

[295] NIS Cooperation Group, *Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023,* https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.
[296] Ibid.

mechanism laid down in Article 22 of the NIS 2 Directive, they would have the same drawbacks as the current 5G cybersecurity toolbox (voluntary non harmonised approach).

While there is no existing framework, NIS2 Directive has established in fact the first step of the necessary procedure with the Union level coordinated security risk assessment, which could include recommended mitigation measures. The CSA revision will build therefore on this.

# ANNEX 10: OVERVIEW OF ENISA'S KEY STAKEHOLDERS' NEEDS

This Annex provides a general overview of **ENISA's key stakeholders, their expectations and unmet needs** based on the objectives of ENISA in the current CSA, the main ENISA-related tasks stemming from the NIS2 Directive and Cyber Solidarity Act, as well as other available information deriving from evidence such as Council conclusions, public consultation on the CSA review[297], ENISA's Single Programming Document[298], ENISA's 2024 Consolidated Annual Activity Report[299] and 2024 Evaluation report[300] (Annex 8). Due to the recent adoption of the CRA (2024), needs of stakeholders have not been evaluated yet. CRA-related expectations have therefore not been integrated in the table. Unmet needs can only be backed by evidence where stakeholders have clearly expressed fulfilment of their needs or where some concrete actions from ENISA's current mandate have not, in part or in full, been implemented.

This Annex distinguishes between the scope of the tasks of ENISA and the scope of the ECCF in the current mandate.

*Table 30: General overview of ENISA's key stakeholders, their expectations and unmet needs in relation to ENISA's current tasks*

| Key stakeholders | Expectations from stakeholders | Are the needs met? | Evidence of needs met/not met |
|---|---|---|---|
| **All** | Be a **centre of expertise on cybersecurity** | Partially | According to ENISA[301], 389 reports and studies were produced in 2023, they were mentioned 102 times in media and downloaded 74,761 times.<br><br>Despite ENISA's annual activity report which reads that 88% of stakeholders find significant added value in the results of ENISA's work and 82% of stakeholders rating the likelihood of taking up the |

[297] See Annex 2 to this Impact Assessment.

[298] ENISA, *ENISA Single Programming Document 2025-2027*, https://enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA%20Single%20Programming%20Document%202025-2027.pdf.

[299] ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf, presents the results of the Second Stakeholders Satisfaction Survey.

[300] The 2024 Evaluation report.

[301] ENISA, *ENISA 2023 Consolidated Annual Activity Report*, https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2023.

| | | | |
|---|---|---|---|
| | | | results of ENISA work in support of their tasks in the immediate to medium term, the study on the evaluation of ENISA[302] states that **Agency's reports could be better tailored to the stakeholders' needs** (p. 10). Some stakeholders interviewed in the context of the evaluation perceived **ENISA's publications and guidelines as overly detailed,** highlighting the need for more practical, hands-on guidance (p. 44).<br><br>ENISA stakeholders believe that better promotion and awareness of ENISA's materials is needed to ensure that they reach a wider audience[303]<br><br>Open-ended contributions to the Public Consultation stated that **ENISA should be a more proactive and technically authoritative** Agency that drives innovation, coherence, and resilience across the European cybersecurity landscape.<br><br>For example, ENISA should play a more prominent role in the development of open standards, the coordination of cybersecurity exercises, and the creation of a European cybersecurity laboratory infrastructure.<br><br>When asked whether ENISA is performing its technical tasks effectively, overall, 25.39 % of respondents to the Public Consultation answered yes, 27.98 % said no, and 46.63 % had no opinion.<br><br>ENISA is not able to provide policy support in a satisfying way to its stakeholders[304]. |
| **National authorities** | Assist Member States in **developing and implementing Union policies** related to cybersecurity, including | Partially | Overall satisfaction of Member States is emphasized in the Council conclusions on ENISA[305]: "RECOGNISES that over the past two decades ENISA has proven to be an invaluable entity in the |

[302] The 2024 Evaluation report, p. 10.
[303] The 2024 Evaluation report, p. 65.
[304] The 2024 Evaluation report, p. 43.
[305] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.

**sectoral** policies on cybersecurity

Support **capacity-building and preparedness** across the Union by assisting Member States to increase the protection of their network and information systems, to develop and improve cyber **resilience** and **response** capacities, and to develop **skills** and competencies in the field of cybersecurity.

The CRA single reporting platform is being established by ENISA, due to be finalized by mid-2026.

European cybersecurity ecosystem, playing a crucial role in actively supporting Member States and EU institutions, bodies, offices and agencies (EUIBAs) in their implementation and development of cybersecurity policies, in their capacity-building and preparedness, in their cooperation and in their promotion of cybersecurity awareness and certification. At the same time, the conclusions stress the need to enhance ENISA's role in a number of areas.

ENISA published sectoral reports as well as NIS360 Report and NIS Investment report and conducts a mapping of National Strategies[306]

ENISA contributed to major deliverables of the NIS Cooperation Gorup since the adoption of the NIS2 Directive, such as the Recommendations for the implementation of NIS2 Directive Article 28 (Database of domain name registration data), the Compendium on Elections Cybersecurity and Resilience (2024 Updated Version) and the Guidelines on implementing national Coordinated Vulnerability Disclosure (CVD) policies.[307]

In 2023, ENISA developed and implemented the **Cybersecurity Support Action** to assist Member States in their efforts to improve their capability to respond to cyber threats and incidents. The Council Conclusions on ENISA[308] recognise the benefits of the Cybersecurity Support Actions and highlights that ENISA should have a central role in the administration and operation of the EU Cybersecurity Reserve, taking its experience in the Support Action.

In 2024, ENISA has organized online **training** sessions for 3,800 public authorities participants from the cybersecurity community (impact not evaluated) and 220 individuals form the cyber

[306] ENISA, *National Cyber Security Strategies*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.
[307] Documents available at: NIS Cooperation Group | Shaping Europe's digital future
[308] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.

| | | | |
|---|---|---|---|
| | | | communities benefitted from train-the-trainer and train-the-planner events[309].<br><br>ENISA has conducted **cybersecurity exercises on a biennial basis,** with lessons learned drawn and policy recommendations systematically made post exercise |
| | **Effectiveness and efficient use of resources** | No | The 2024 Evaluation report highlights that ENISA is not able to implement its mandate efficiently and effectively due to a lack of resources [310]<br><br>The Council invites the Commission to enhance "the effectiveness and efficient use of resources", calling on the Commission to ensure that "ENISA's mandate to support Member States and EU institutions, bodies, offices and agencies (EUIBAs) is focused and clearly-defined, with concrete strategic objectives and prioritised tasks, in addition to a more precise division of tasks and competences with respect to other actors"[311] |
| | Promote **cooperation**, including **information sharing and coordination** at Union level<br><br>Contribute to increasing **cybersecurity capabilities** at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents. | Mostly not | ENISA provided support to set up or enhance capabilities of CSIRTs through exercises and supporting information sharing as secretariat to the group.<br><br>However, Member States expressed clearly in the Council conclusions on ENISA that their **cooperation expectations were not met,** with the Council calling in particular for enhancing common situational awareness and to further build trust with Member States on information sharing. [312]<br><br>In addition, **ENISA did not meet the target for 2024** for the tasks |

[309] ENISA, *ENISA Single Programming Document 2025-2027*, https://enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA%20Single%20Programming%20Document%202025-2027.pdf.
[310] The 2024 Evaluation report, p. 43.
[311] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.
[312] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.

| | | | |
|---|---|---|---|
| | | | "ENISA is able to provide regular risk monitoring towards specific targets or at the national level, including by leveraging commercial off-the-shelf platforms, and provide specific risk assessments and threat landscapes as requested by MS" (target set on 50%, result for 2024 was 30%)[313]. |
| **Companies** | Support **capacity-building and preparedness** across the Union by assisting private stakeholders | Partially | ENISA has developed cooperation with the private sector in recent years. However, the Council encourages ENISA to work in close cooperation with the Member States and across EU entities to bolster cooperation with the private sector because of its continuous monitoring of the cyber threat landscape which could help to improve **common situational awareness**[314].<br><br>Stakeholders perceive ENISA's operational activities, in particular through the National CSIRTs, as "closed", which requires them to directly engage with the Member States to improve their access to the ENISA's activities[315]<br><br>ENISA did not perform skill-related activity targeting the cybersecurity workforce in support of industry, with the exception of the development of the **European Cybersecurity Skills Framework** (2022) and the organisation of the annual **European Cybersecurity Skills Conferences** (since 2022)[316].<br><br>Publication of technical guidelines, notably the Technical Implementation Guidance and Mapping for companies subject to Commission Implementing Regulation (EU) 2024/2690, where individuals, private organisations, associations and members of the open source software community that contributed to an open |

[313] ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf, presents the results of the Second Stakeholders Satisfaction Survey.
[314] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24, point 25.
[315] The 2024 Evaluation report, p. 65.
[316] ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf, presents the results of the Second Stakeholders Satisfaction Survey.

| | | | |
|---|---|---|---|
| | | | consultation. |
| **European Union institutions, bodies, offices and agencies (EUIBAs)** | **Assist EUIBAs** in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity<br><br>Support **capacity-building and preparedness** across the Union by assisting the Union institutions, bodies, offices and agencies to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity. | Mostly met | ENISA has concluded:<br><br>- a service level agreement with EU-LISA which covers support services on the planning, execution and evaluation of exercises<br><br>- a MoU with the European Cybersecurity Competence Centre (ECCC) to help to tackle the skills gap in cybersecurity under the European Cybersecurity Skills Framework, to set up a joint cybersecurity market observatory to help ENISA fulfil its new market related tasks under the CRA<br><br>- MoUs with the European Railway Agency (ERA), the European Banking Authority (EBA), ESMA and EIOPA (concerning the implementation of incident reporting under DORA and its alignment with other corresponding NIS2 requirements) on incident reporting<br><br>ENISA also established structured cooperation with CERT-EU in 2020, supporting joint situational awareness reports. ENISA and CERT-EU cooperation has been strengthened by joint work on the EUIBA Standard Operating Procedures, which serve as a foundation for coordinated responses to incidents and intelligence sharing with other EU agencies.<br><br>The agency executed its biennial Cyber Europe flagship exercise in 2024, helping to improve and develop the capabilities of MS and EUIBAs, as well as various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the EU.<br><br>The agency made positive strides to meet the obligations of Regulation (EU, Euratom) 2023/2841 on a high common level of cybersecurity at EUIBAs, including by conducting risk assessments |

| | | | |
|---|---|---|---|
| | | | and a horizontal cybersecurity audit that will form the basis for the agency's long-term cybersecurity strategy and planning.[317]<br><br>The ECA report highlighted that ENISA dropped a planned assessment of EUIBAs' cybersecurity maturity due to lack of resources. Training efforts have primarily targeted Member States, with limited focus on EUIBAs, and minor support was provided to CERT-EU.[318] Interviewed ENISA staff mentioned that ENISA shifted to a "train the trainers" model, helping communities reach a maturity level where they can organise their own exercises, to save costs and increase ENISA's effectiveness. |
| **Citizens** | - On awareness: promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses<br><br>- On skills for professionals: to develop skills and competencies in the field of cybersecurity | Partially awareness<br><br>No for skills for professionals | Yearly cybersecurity **awareness campaign widely supported by 78.75 % of respondents to the public consultation** agreeing or strongly agreeing.<br><br>Publication of toolkits and course "**Awareness raising in-a-box**": 2 725 visitors, 68 694 pageviews, 4 352 downloads[319]<br><br>Development of **Cybersecurity Higher Education Database (CyberHEAD)**[320] which enables perspective students to make well-informed decisions about the diverse academic paths available in cybersecurity. However, the database future is uncertain due to funding.<br><br>**Cybersecurity skills and workforce development activities have been deprioritized**, notably training activities and Capture The Flag competitions: "the plan is to gradually transfer knowledge and |

[317] ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf, presents the results of the Second Stakeholders Satisfaction Survey.
[318] The European Court of Auditors (2022), *Cybersecurity of EU institutions, bodies and agencies. Special report*, *https://www.eca.europa.eu/en/publications/SR22_05*.
[319] ENISA, *2024 Consolidated Annual Activity Report*, https://enisa.europa.eu/sites/default/files/2025-07/Consolidated%20Annual%20Activity%20Report%202024.pdf, presents the results of the Second Stakeholders Satisfaction Survey.
[320] ENISA, CYBERHEAD - Cybersecurity Higher Education Database, https://www.enisa.europa.eu/tools/cyberhead-cybersecurity-higher-education-database.

| | | | |
|---|---|---|---|
| | | | empower MSs, in particular NCCs, national operational communities and the ECCC, and to organise and financially support CTF training sessions at national and EU level with ENISA maintaining a facilitating role". ENISA will further "limit the number of targeted exercises and training sessions focusing on empowering the trainers with the intention to enhance the resilience, maturity and preparedness of NIS sectors"[321]<br><br>The disengagement of the agency towards cybersecurity professionals marks a **discrepancy with 69.43% of respondents to the public consultation who indicated that ENISA should lead the development of an attestation scheme for cybersecurity skills[322],** indicating overall support for professional skills development framework.<br><br>ENISA does not offer trainings to citizens[323] |

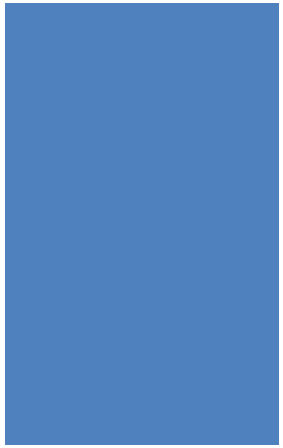
*Table 31: ENISA's key stakeholders, their expectations and unmet needs in relation to the ECCF*

| Key stakeholders | Expectations from stakeholders | Are the needs met? | Evidence of needs met/not met |
|---|---|---|---|
| **National authorities** | Implement the European **cybersecurity certification framework** and contribute to the establishment and maintenance of a European cybersecurity | Mostly not | **Member States** are concerned by the lengthy process of selection, elaboration and adoption of cybersecurity certification schemes [324]<br><br>Meanwhile Member States recognise the importance of the ECCF and have urged the Commission to introduce a leaner, |

[321] ENISA, *ENISA Single Programming Document 2025-2027*, https://enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA%20Single%20Programming%20Document%202025-2027.pdf.
[322] Annex 2 to this Impact Assessment.
[323] ENISA, *ENISA Single Programming Document 2025-2027*, https://enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA%20Single%20Programming%20Document%202025-2027.pdf.
[324] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.

| | | | |
|---|---|---|---|
| | certification framework | | risk-based as well as more transparent and faster approach to the development of EU cybersecurity certification schemes.[325]<br><br>The replies to public consultation show **dissatisfaction of over 70% of the respondents** with the time required to develop and adopt European cybersecurity certification schemes. Most prominently, it was the public authorities which expressed, 25.0 % dissatisfaction, and 62.5 % strong dissatisfaction.<br><br>The 2024 Evaluation Report stresses that Member States see the **need to increase ENISA's independence** in delivering on schemes, and express **concerns** related to political interferences in the process. The Study also stresses that the **added value** of the certification framework has fallen short in its ability to support them in increasing national cybersecurity certification capabilities. |
| **Companies** | Implement the European **cybersecurity certification framework** in a predictable manner | No | Member States and industry are concerned by the lengthy process of selection, elaboration and adoption of cybersecurity certification schemes[326]<br><br>The replies to public consultation show dissatisfaction of over 70% of the respondents with the time required to develop and adopt European cybersecurity certification schemes. **Companies were particularly critical in this regard, showing alignment between large companies (80%), small companies (78%).** Without a clear timeline and predictability of the framework the business cannot consider certification a viable business opportunity.<br><br>However, the replies to public consultation also reveal a broad and well-substantiated interest in advancing the implementation of the ECCF. Certification is widely perceived as a tool to enhance product and service security, with 41.45 % |

[325] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24, point 7.
[326] Council of the European Union, Council conclusions on ENISA, 6 December 2024, no. 16527/24.



of respondents strongly agreeing with this view and the vast majority of the rest of the respondents agreeing. Similarly, 47.67 % strongly support its role in ensuring regulatory compliance, and 41.45 % emphasize its importance in facilitating market access through mutual recognition. Among business associations, 33.33 % strongly agree on the security benefits and 40.74 % on compliance vast majority of the rest of the respondents agreeing. Large companies show a notably high agreement of 62.0% on compliance. Medium and small enterprises demonstrate strong support, with 50.0 % to 55.56 % strongly agreeing on the security dimension, while micro businesses are the most supportive, with 66.67 % strongly agreeing that certification improves security.

# ANNEX 11: EVOLUTION OF ENISA'S ACTIVITIES FROM 2017 UNTIL 2024, INCLUDING RESOURCE ALLOCATION (BUDGET AND FTES)

The table below sets out the evolution of ENISA's activities from 2017 (before the CSA 2019) until 2024, including the resource allocation in terms of actual budget (from 2021) and actual FTEs (from 2017) by activity. The number of FTEs increased from 83.25 in 2017 to 121.04 in 2020. It decreased in the next two years, reaching 97.54 FTEs is 2022. Then it increased again to 110.74 in 2024. The number of main activities carried out by ENISA grew from 5 Activities in 2017 to 13 in 2024.

*Table 32: Evolution of ENISA's activities from 2017 until 2024, including resource allocation (budget and FTEs)*[327]

| Year | Activity | Actual Budget | Actual FTEs |
|---|---|---|---|
| 2017 | Activity 1 - Expertise. | n/a | 12.55 |
| | Activity 2 - Policy. | n/a | 23.83 |
| | Activity 3 - Capacity. | n/a | 9.97 |
| | Activity 4 - Community. | n/a | 10.60 |
| | Activity 5 - Enabling. | n/a | 26.30 |
| | TOTAL | 10,608,963.75 | 83.25 |
| 2018 | Activity 1 — Expertise. | n/a | 12.55 |
| | Activity 2 — Policy. | n/a | 23.83 |
| | Activity 3 — Capacity. | n/a | 9.97 |
| | Activity 4 — Community. | n/a | 10.60 |
| | Activity 5 — Enabling. | n/a | 26.30 |
| | TOTAL | 10,785,705.70 | 83.25 |
| **2019** | Activity 1 — Expertise. | n/a | 9.00 |
| | Activity 2 — policy. | n/a | 16.90 |
| | Activity 3 — Capacity. | n/a | 7.50 |

[327] ENISA's Annual Activity Reports from 2017 until 2024.

| | | | |
|---|---|---|---|
| | Activity 4 — Community. | n/a | 10.60 |
| | Activity 5 — Enabling. | n/a | 43.57 |
| | TOTAL | 16,292,952.05 | 87.57 |
| 2020 | Activity 1 – Expertise. | n/a | 13.62 |
| | Activity 2 – Policy. | n/a | 13.45 |
| | Activity 3 – Capacity. | n/a | 12.19 |
| | Activity 4 – Cooperation. | n/a | 12.22 |
| | Activity 5 – Develop Cybersecurity Certification schemes for digital products, services and processes | n/a | 7.33 |
| | Activity 6 - Enabling. Reinforce ENISA's impact | n/a | 62.23 |
| | TOTAL | 21,149,119 | 121.04 |
| 2021 | Activity 1: Providing assistance in policy development | 1,393,794.52 | 7.25 |
| | Activity 2: Supporting implementation of Union policy and law | 3,395,688.26 | 16.62 |
| | Activity 3: Building capacity | 3,907,076.25 | 16.93 |
| | Activity 4: Enabling operational cooperation | 2,753,446.25 | 10.97 |
| | Activity 5: Contribute to cooperative response at Union and Member States level | 2,044,536.29 | 6.40 |
| | Activity 6: Development and maintenance of EU cybersecurity certification framework | 2,147,521.14 | 11.00 |
| | Activity 7: Supporting the European cybersecurity market and industry | 2,027,048.34 | 10.64 |
| | Activity 8: Knowledge on emerging cybersecurity challenges and opportunities | 2,881,670.90 | 12.05 |
| | Activity 9: Outreach and education | 2,170,368.01 | 8.35 |
| | TOTAL | 22,721,149.95 | 100.20 |

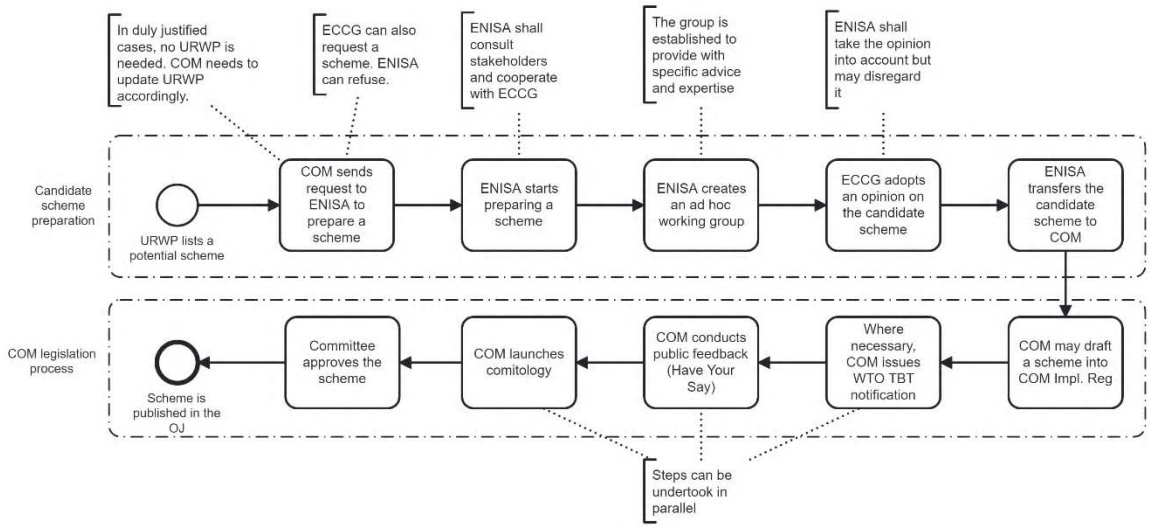
| | | | |
|---|---|---|---|
| 2022 | Activity 1: Providing assistance in policy development | 1,504,130.01 | 7.09 |
| | Activity 2: Supporting implementation of Union policy and law | 2,996,538.66 | 13.66 |
| | Activity 3: Building capacity | 4,273,363.95 | 14.50 |
| | Activity 4: Enabling operational cooperation | 1,922,081.06 | 1.48 |
| | Activity 5: Contribute to cooperative response at Union and Member States level | 19,130,992.46 | 20.31 |
| | Activity 6: Development and maintenance of EU cybersecurity certification framework | 2,911,478.39 | 12.04 |
| | Activity 7: Supporting the European cybersecurity market and industry | 1,336,552.76 | 5.98 |
| | Activity 8: Knowledge on emerging cybersecurity challenges and opportunities | 3,486,726.99 | 15.07 |
| | Activity 9: Outreach and education | 1,617,541.66 | 7.41 |
| | TOTAL | 39,179,405.95 | 97.54 |
| 2023 | Activity 1: Providing assistance in policy development | 685,149.03 | 2.49 |
| | Activity 2: Supporting implementation of Union policy and law | 2,184,963.86 | 9.90 |
| | Activity 3: Building capacity | 3,431,079.23 | 12.03 |
| | Activity 4: Enabling operational cooperation | 3,148,642.37 | 7.73 |
| | Activity 5: Contribute to cooperative response at Union and Member States level | 2,265,238.41 | 9.55 |
| | Activity 6: Development and maintenance of EU cybersecurity certification framework | 1,897,832.93 | 7.71 |
| | Activity 7: Supporting the European cybersecurity market and industry | 1,159,070.48 | 6.08 |
| | Activity 8: Knowledge on emerging cybersecurity challenges and opportunities | 1,757,071.27 | 6.84 |

| | | | |
|---|---|---|---|
| | Activity 9: Outreach and education | 1,610,449.89 | 7.93 |
| | Activity 10: Advise on research and innovation needs and priorities | 657,331.70 | 3.34 |
| | Activity 11. Performance and risk management | 2,758,381.07 | 16.74 |
| | Activity 12. Staff development and working environment | 3,627,725.20 | 14.31 |
| | TOTAL | 25,182,935.43 | 104.64 |
| 2024 | Activity 1: Providing assistance in policy development | 840,266.83 | 3.29 |
| | Activity 2: Supporting implementation of Union policy and law | 2,293,362.76 | 9.90 |
| | Activity 3: Building capacity | 2,944,951.11 | 10.83 |
| | Activity 4: Enabling operational cooperation | 3,103,844.35 | 8.81 |
| | Activity 5: Contribute to cooperative response at Union and Member States level | 2,854,659.00 | 13.22 |
| | Activity 6: Development and maintenance of EU cybersecurity certification framework | 1,763,664.55 | 8.13 |
| | Activity 7: Supporting the European cybersecurity market and industry | 998,729.06 | 5.08 |
| | Activity 8: Knowledge on emerging cybersecurity challenges and opportunities | 1,879,102.03 | 7.62 |
| | Activity 9: Outreach and education | 1,633,620.09 | 8.34 |
| | Activity 10: Research and innovation | 455,501.81 | 2.29 |
| | Activity 11. Performance and sustainability | 2,360,523.21 | 11.48 |
| | Activity 12. Reputation and trust | 795,811.95 | 4.47 |
| | Activity 13. Effective and efficient corporate services | 4,294,684.64 | 17.28 |
| | TOTAL | 26,218,721.39 | 110.74 |

# ANNEX 12: EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK (ECCF)

The CSA established the ECCF to increase the level of cybersecurity within the Union by enabling the development of Union wide cybersecurity certification schemes. These schemes are intended to ensure a consistent level of cybersecurity assurance for information and communication technology (ICT) products, services, processes and managed security services (entities not covered) across the European Union (EU). The procedure for developing such schemes consists of three main phases: the planning, led by the European Commission (EC), the technical preparation of a candidate scheme, coordinated by ENISA, and the adoption of the final scheme through a legislative procedure led by the EC. A visual summary of the full EU cybersecurity certification scheme development process is provided in the figure below and explained in detail thereafter.

*Figure 3018 EU Cybersecurity Certification Scheme Development Process*




The process begins with the identification of a new certification need, usually reflected in the Union Rolling Work Programme (URWP). This programme outlines strategic priorities and reflects a shared vision between the EC and ENISA on emerging certification requirements (CSA, Article 47). In exceptional and duly justified cases, a scheme may be launched even if it was not initially included in the URWP. In such situations, the EC must formally update the URWP to reflect the decision (CSA, Article 48 (2)).

The EC initiates the development process by formally requesting ENISA to prepare a candidate scheme (CSA, Article 48(1)). The ECCG, composed of representatives from national cybersecurity certification authorities, may also suggest new schemes to ENISA. However, unlike for EC requests, ENISA is not obliged to act upon scheme requests from the ECCG (CSA, Article 48(2)). The requests provide only a high-level description of the objective that the schemes should be conform with and does not provide any development planning[328]. Once ENISA accepts a request, it becomes responsible for

[328] The request for a candidate EUCS scheme included the following: *"In accordance with Article 48(2) of the Cybersecurity Act, we would like to request ENISA to prepare a candidate European cybersecurity*

coordinating the technical drafting process in cooperation with relevant stakeholders and national authorities (CSA, Article 49 (1)).

Throughout this process, ENISA must carry out targeted consultations. It works in close collaboration with the ECCG to ensure that the draft scheme reflects the needs and expectations of Member States (CSA, Article 49 (5)). ENISA may also engage with the Stakeholder Cybersecurity Certification Group (SCCG), a group representing industry and other non-governmental actors (CSA, Article 22 (3)).

A key component of the technical drafting process is the creation of an Ad Hoc Working Group (AHWG). This group is composed of external experts selected by ENISA on the basis of professional competence and geographical balance. The AHWG supports the technical preparation of the scheme. The involvement of an AHWG is required under Article 48(4) of the CSA and is a central element of the framework. This requirement is further specified in Recital (59) of the CSA, which states that the Executive Director should ensure that the members of ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure gender balance and an appropriate balance, according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies and the private sector, including industry, users, and academic experts in network and information security.

ENISA drafts the candidate scheme based on inputs from the AHWG, results of stakeholder consultations, and ongoing collaboration with the ECCG (CSA, Article 49 (3)-(6)), and also based on the EC's request. The draft must include all mandatory components as laid out in Article 54 of the CSA, such as the scope and purpose of the scheme, assurance levels, conformity assessment processes (CSA, Article 56), and references to applicable standards. Additional technical elements may be included to address specific risks or sectoral needs, as appropriate.

Once the draft is ready (timeline not specified), ENISA submits it to the ECCG for an opinion (CSA, Article 49 (5)). The ECCG may provide comments, raise concerns, or make suggestions for improvement. ENISA is required to take this opinion into account but retains the discretion to deviate from it if duly justified (CSA, Article 49 (6)). In practice, the opinion is drafted by the Commission based on the comments and put forward to the group for further comments. After this review, ENISA may transmit the final draft to the EC or seek to improve the text and repeat the procedure.

The EC is responsible for transforming the draft candidate scheme developed by ENISA into a legally binding instrument at its discretion. The legal drafting on the basis of technical document and adoption process may (or often does) lead to amendments in the draft text. Once finalised, the draft implementing act is published on the EC's Have Your Say portal for public consultation. This allows stakeholders, including industry, public authorities, and citizens, to comment on the proposed scheme. The feedback received is reviewed and may lead to further revisions. Furthermore, under the TBT Agreement, WTO Members have the obligation to notify, through the WTO Secretariat, draft measures that may have a significant effect on trade of other Members and are not based

---

*certification scheme for cloud services. The candidate scheme should provide for cybersecurity certification of cloud services and should take into account existing and relevant schemes and standards. The candidate scheme should conform to the requirements of Articles 51, 52 and 54 of the Cybersecurity Act."*

on relevant international standards. In such a case, the Commission shall also submit a WTO TBT notification.

Next, the EC launches adoption of an implementing act by comitology under the examination procedure (CSA, Article 49 (7) and Article 66 (2)). This is done by submitting the draft implementing act to a committee of Member State representatives. The comitology procedure can be launched prior to the closing of the public consultation, and where applicable, the WTO TBT notification, however no opinion can be delivered by the committee before the closing of such consultation(s). The committee must deliver an opinion. If the opinion is positive, the EC may proceed with adoption. If the opinion is negative or not delivered, the EC may revise the draft or take other appropriate steps.

Once the implementing act is adopted, the EU certification scheme has a harmonisation effect across all Member States. The scheme is published in the Official Journal of the European Union and enters into force on the date specified in the act. From that point on, Conformity Assessment Bodies (CABs) and economic operators across the EU may apply the scheme (CSA, Article 56 (1)). The ECCF does not envisage maintenance of the schemes that have been adopted at the moment. Updates of schemes therefore require revision of the implementing act establishing the scheme, preparation and review of the documents is currently (informally) done by a ECCG sub-group of the willing Member States representatives and industry and subject to the ECCG agreement, before the comitology procedure.

Since the entry into force of the CSA, five schemes have been formally requested but only one has been adopted to date. The European Common Criteria-based Cybersecurity Certification Scheme (EUCC) was adopted on 31 January 2024 and entered into application on 27 February 2025 following several years of technical drafting and interinstitutional procedures. The table below summarizes the state of play at the end 2024:

| EUCC | EUCS | EU 5G | ID Wallet | *MSS* |
|---|---|---|---|---|
| Adopted<br>**4.5 years** | Ongoing<br>**5 years** | Ongoing<br>**4.5 years** | Ongoing<br>**5 months** | *Requested recently* |

## ANNEX 13: INTERVENTION LOGIC WITH LIST OF MEASURES PER POLICY OPTIONS

# Overview of policy options - ENISA

| ENISA's mandate | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Problem drivers | Problem | Policy option | Key measures | Specific objectives | | | | |
| | | | | SPO1 | SPO2 | SPO3 | SPO4 | SPO5 |
| **PD1:** Increasingly hostile and unpredictable threat landscape in a rapidly evolving technological environment (horizontal driver).<br><br>**PD2:** Regulatory gaps (horizontal driver)<br><br>**PD4:** Unsuitable ENISA mandate and resources to evolve with EU cyber ecosystem's and regulatory needs<br><br>**PD5:** Complex and fragmented collaboration on cybersecurity among EU agencies, governance bodies and stakeholders | **P1:** Misalignment between the Union's cybersecurity policy framework and stakeholders' needs in an increasingly hostile threat landscape | A.1: Clarifying ENISA's mandate and providing for prioritisation | **M1:** Align with NIS 2, CRA, DORA, CSoA, DORA and NCCS. | ☑ | | | | |
| | | | **M2:** Ensure for synergies with the ECCC and the Network of NCCs | ☑ | | | | |
| | | | **M3:** Prioritise tasks, focusing on policy implementation and sectoral guidelines | | ☑ | | | |
| | | | **M4:** Facilitating operational cooperation between Member States and CSIRTs network and EU CyCLONe (cross-border incidents and information flows) | ± | | | | |
| | | | **M5:** Adjust budget to reflect additional tasks; limit ad hoc contribution agreements. | ± | | | | |
| | | **A.2:** Reforming of ENISA's mandate | **M1, M2, M5** | ☑ | | | | |
| | | | **M6:** Structure the mandate into 3 priority pillars<br>Pillar 1: supporting implementation of general and sector -specific cybersecurity policies and legislation.<br>Pillar 2: providing operational support for MS and enhancing contribution to shared situational awareness and exchange of information.<br>Pillar 3: cybersecurity certification and standardisation. | ☑ | ☑ | ☑ | | |
| | | | **M7:** Provide vulnerability management services. | ☑ | ☑ | | | |
| | | | **M8:** Clarify the role and principles of international cooperation | | ☑ | | | |
| | | | **M9:** Contribute to the development and maintenance of European individual skills attestations schemes | | ☑ | | | |
| | | | **M10**: Resourcing based on EU budget, liaison officers, own resourcing | ☑ | ☑ | | | |
| | | **A.3:** Reforming of ENISA's mandate with a strong operational support focus | **M1, M2, M5, M8, M9** | | ☑ | | | |
| | | | **M6, M7, M10** | ☑ | ☑ | | | |
| | | | **M11:** Providing direct operational support to NIS 2 entities. | ☑ | ± | | | |
| | | | **M12:** Create 24/7 operational team with ENISA staff, liaison officers and service providers. | ☑ | ± | | | |

# Overview of policy options - ECCF

| European Cybersecurity Certification Framework | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Problem drivers** | **Problems** | **Policy option** | **Key measures** | **Specific objectives** | | | | |
| | | | | SPO1 | SPO2 | SPO3 | SPO4 | SPO5 |
| **PD1:** Increasingly hostile and unpredictable threat landscape in a rapidly evolving technological environment (horizontal driver).<br><br>**PD2:** Regulatory gaps (horizontal driver)<br><br>**PD6:** Implementation failure: The practical experience of the development and adoption process of first schemes<br><br>**PD7:** Legislative developments not factored in the current ECCF | **P2:** Stalled implementation of the ECCF | **B.1:** Clarifying the ECCF's scope, elements and objectives and introducinga maintenance mechanism | **M1:** Clarifying that ECCF covers technical risk factors only | | | ☑ | | |
| | | | **M2:** Formalising maintenance procedure of applicable certification schemes. | | ☑ | ☑ | | |
| | | | **M3**: Aligning the ECCF with the CRA, particularly on vulnerability handling. | | | ☑ | | |
| | | **B.2:** Reforming the ECCF by revising its procedures and extending the scope to facilitate simplification of regulatory compliance | **M1 – M2** | | ☑ | ☑ | | |
| | | | **M4:** Revising procedure for request, development, and adoption of Certification schemes | | ☑ | ☑ | ☑ | |
| | | | **M5:** New Strategic planning and with strengthened stakeholder engagement | | | ☑ | | |
| | | | **M6:** Strengthening ENISA's role as 'scheme manager'. | | | ☑ | | |
| | | | **M7:** Solidifying synergies between the ECCF and CRA / NIS2 | | ☑ | ☑ | ☑ | |
| | | | **M8:** Extending scope to cater for future certification of organisation-wide security posture. | | ☑ | ☑ | ☑ | |
| | | **B.3:** Reforming the ECCF as envisaged under option B.2 and introduce mandatory certification for cyber posture | **M1 – M2; M4 – M8** | | ☑ | ☑ | ☑ | |
| | | | **M9**: Empowering the Commission to mandate certification in specific risk-based scenarios and adjust the list | | | | | |

# Overview of policy options - Simplification

| Simplification | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Problem drivers** | **Problem** | **Policy option** | **Key measures** | **Specific objectives** | | | | |
| | | | | SPO1 | SPO2 | SPO3 | SPO4 | SPO5 |
| **PD2:** Regulatory gaps (horizontal driver)<br><br>**PD3:** Vulnerabilities linked to non-technical risks (horizontal driver)<br><br>**PD8:** Fragmented compliance landscape and complexity of horizontal and sectoral frameworks | **P3:** Complexity and diversity of the cybersecurity-related policies impacting the Union's cyber posture | **C.1:** Taking a soft law and non-legislative instruments approach, including the use of existing empowerments (adoption of implementing acts under Article 21(5) and Article 23(11) of the NIS 2 Directive) | **M1:** Harmonise cybersecurity risk-management measures, incident reporting thresholds, as well as information, formats and procedures of notifications.to facilitate compliance | | | | ☑ | |
| | | | **M2:** Commission to adopt guidelines:<br>• easing the burden on suppliers by clarifying the application of supply chain obligations,<br>• on the scope include NIS 2 definitions to support a more harmonised interpretation,<br>• to streamline ransomware reporting | | | | ☑ | |
| | | **C.2:** Targeted intervention – further simplification of compliance with relevant Union cybersecurity legislative framework | **M3:** Introduce possibility to demonstrate compliance based on organisational cybersecurity certification schemes in the ECCF. | | | ☑ | ☑ | |
| | | | **M4:** New role for ENISA to support competent authorities in supervision of cross-border entities | | ☑ | | ☑ | |
| | | | **M5:** Ensure harmonised collection of data on ransomware attacks. | ☑ | | | ☑ | |
| | | | **M6:** Clarifying the scope, definitions and introducing small mid-caps category in NIS2 Directive | | ☑ | | ☑ | |
| | | | **M7:** Enable maximum harmonisation for NIS2 Directive implementing acts. | | | | ☑ | |
| | | | **M8:** Guidelines easing the burden on suppliers by clarifying the application of supply chain obligations | | ☑ | | ☑ | |
| | | **C.3:** Harmonising cybersecurity-related measures set out in Union legislation | **M3-M8** | ☑ | ☑ | | ☑ | |
| | | | **M9:** Remove all sector-specific risk-management provisions and centralise requirements within NIS 2 Directive ecosystem. | | | | ☑ | |

# Overview of policy options – ICT supply chain security

| ICT supply chain security | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Problem drivers** | **Problems** | **Policy option** | **Key measures** | **Specific objectives** | | | | |
| | | | | SPO1 | SPO2 | SPO3 | SPO4 | SPO5 |
| **PD1:** Increasingly hostile and unpredictable threat landscape in a rapidly evolving technological environment (horizontal driver).<br><br>**PD2:** Regulatory gaps (horizontal driver)<br><br>**PD3:** Vulnerabilities linked to non-technical risks (horizontal driver)<br><br>**PD9:** Inadequate measures to address ICT supply chain cybersecurity risks | **P4:** Increasing ICT supply chains security risks | **D.1:** Taking a soft law approach to address cybersecurity risks for ICT supply chains | **M1:** Use of soft law measures within the existing EU regulatory framework to address non-technical risks, with Commission communications, guidance and recommendations | | | | | |
| | | | **M2:** Continuation of coordinated risk assessments under NIS2, with non-binding mitigating measures | | | | | |
| | | | **M3:** Introduction of security requirements on an ad hoc basis in public procurement tenders or auctions. | | | | | |
| | | **D.2:** Ad hoc regulatory intervention codifying the 5G Toolbox | **M4:** Codification of the 5G Toolbox measures, i.e. mandatory obligation for Member States not to use components from high-risk suppliers in key assets of the network as defined in the EU coordinated risk assessment on 5G security | | | | | ± |
| | | **D.3:** Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks | **M4** | | | | | ± |
| | | | **M5:** Horizontal, technology and sector-neutral regulatory framework to address cybersecurity risks, in particular non-technical risks, in ICT supply chains, which would entail:<br>• Identification of key ICT assets and technologies for entities operating in sectors of high criticality and other critical sectors listed in Annex I and II of the NIS2 Directive, through a set of objective and harmonised criteria<br>• Identification of a list of high-risk suppliers or countries of concern, through a set of objective and harmonised criteria<br>• Set of proportionate and risk-based measures to mitigate the risks linked to the high-risk suppliers, e.g. storage or processing of data, prohibition to install equipment from high-risk suppliers | | | ☑ | | ☑ |

# ANNEX 14: COMPARISON OF THE OPTIONS – CRITERIA EFFICIENCY, COHERENCE

## 1. EFFICIENCY

The table below represents a detailed overview of the net value of policy options, where quantitative data is available, and, where this is not the case, it compares in a qualitative expected costs and benefits presented in sections 6.1 and 6.2. The net values are summarized in the table under *section 7.3* of the impact assessment, under the section related to compliance costs and cost savings.

*Table 33: Overview of the net value of policy options*

Legend: * broad estimate

| Benefits/Costs analysis | **Policy options** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ENISA mandate | | | Certification | | | Simplification | | | Supply chain | | |
| | A.1 | A.2 (preferred option) | A.3 | B.1 | B.2 (preferred option) | B.3 | C.1 | C.2 (preferred option) | C.3 | D.1 | D.2 | D.3 (preferred option) |
| **Citizens** | | | | | | | | | | | | |
| Costs | 0 | 0/- | 0/- | 0 | 0 | - | 0 | 0 | 0 | 0/- | - If transferred (not expected) : EUR 6.5 to 8.3 per mobile subscriber per year for 3 years | - - < D2 |
| Benefits | 0 | + | ++ | + | ++ | +++ | 0 | 0 | 0 | 0/+ | ++ | +++ |
| **Net Value (5 years)** | 0 | 0/+ | +/++ | + | ++ | +++ | 0 | 0 | 0 | 0 | + | ++ |
| **Businesses** | | | | | | | | | | | | |
| Costs | 0 | 0/- | 0/- | 0 /- | 0/- | - - - EUR 501 M | 0/- | - | - EUR 5,2n bn | 0/- | **-3.4 bn to 4.3 bn EUR per year** for 3 | < D2 |

| Benefits/Costs analysis | **Policy options** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | ENISA mandate | | | Certification | | | Simplification | | | Supply chain | | |
| | A.1 | A.2 (preferred option) | A.3 | B.1 | B.2 (preferred option) | B.3 | C.1 | C.2 (preferred option) | C.3 | D.1 | D.2 | D.3 (preferred option) |
| | | | | | | (one-off) | | | | | years | |
| Benefits | + | ++ **EUR 3.7 to 4.4 bn over five years *** | +++ **EUR 3.7 to 4.4 bn over five years *** | 0/+ | +/++ | ++ | + | EUR 14.6 bn | EUR 37.1 bn | + | **EUR 2bn /year** ++ | >D2 +++ |
| **Net Value (5 years)** | + | +/++ | +/++ | **0** | + | **- EUR 501 M (one-off)** | **0/+** | **EUR 14.6 bn -** | **EUR 31.9 bn** | -0/+ | **- EUR 1.4 to 2.3 bn** per year over 3 years ++ | **< D2** +++ |
| **National authorities** | | | | | | | | | | | | |
| Costs | 0 | EUR 11.3 M | EUR 12.7 M | EUR 0-61 M | EUR 13,7 to 74,7 M | EUR 22,8 to 83,9 M | 0/- | - | - EUR 0,16 M | 0/- | - | -- |
| Benefits | 0/+ | + | ++ | 0/+ | +/ ++ | ++/ +++ | 0 | EUR 7,5 M | EUR 15 M | + | ++ | +++ |
| **Net Value (5 years)** | **0/+** | **- EUR 11.3 M** + | **- EUR 12.7 M** ++ | **- EUR 0 to 61 M** 0/+ | **- EUR 13,7 to 74,7** M (D3) + | **- EUR 13,7 to 74,7** M (D3) ++ | 0/- | **+ 7.5 M** | **+ 14,8 M** | **0/+** | **+** | **+** |
| **ENISA** | | | | | | | | | | | | |
| Costs | 0 | **- EUR 148.12 M** | **-EUR 165.3 M** | EUR 6.8 to 10.5 M | EUR 9.5 to 13.1 M | EUR 9.5 to 13.1 M | 0 | N.A (A2/3) | N.A (A2/3) | N.A | N.A | N.A |
| Benefits | 0/+ | + | + | + | ++ | ++ | 0 | 0 | 0 | N.A | N.A | N.A |
| **Net Value (5 years)** | 0/+ | **- EUR 148.12 M** | **- EUR 165.3 M** | **EUR 6.8 to 10.5 M +** | **EUR 9.5 to 13.1 M** ++ | **EUR 9.5 to 13.1 M** ++ | | (A2/3) | (A2/3) | N.A | N.A | N.A |

## 2. COHERENCE

The assessment of coherence focuses on alignment with the EU's overarching policy framework, including the EU Cybersecurity Strategy and key existing and future legislative instruments. It also considers whether the options are coherent with the international developments, namely:

- **NIS2 Directive:** Option A.1, streamlines ENISA's mandate and continue implementing tasks prescribed by the NIS 2 in particular in the area of support for policy implementation and operational cooperation (medium coherence). Options A.2 further reinforces NIS 2 Directive objectives on cooperation in information exchange to prevent or mitigate incidents, within the CSIRTs network and EU-CyCLONe. It also delivers on the NIS 2 provision on coordinated vulnerability disclosure (high coherence). Option A.3 by going further in the support of operational cooperation is least coherent with the NIS 2 Directive that acknowledges national CSIRTs clear role in the support of the entities in incident response. Options B.2 and B.3 in combination with options C.2 and C.3 are assessed to have high coherence with the NIS 2 by proposing the certification of entities that would demonstrate compliance with the Directive (possibly other relevant Union legal acts, such as GDPR). Option B.1 is assessed to be neutral. Options C provide for targeted amendments of NIS2 Directive to clarify the scope, adjust the coverage of certain categories of entities under the scope, introducing the mid-size cap to narrow the coverage of ex ante supervision, therefore they are assessed to be coherent with the NIS 2 Directive. Similarly, options D are coherent with the NIS 2 Directive as provide for covering non-technical risks for supply chain, also covered by the Directive, with option D.3 assessed as of high coherence, as providing the best solutions to address non-technical risks.
- **CER Directive:** it requires from Member States to identify the critical entities from the list of sectors, while NIS2 Directive applies to all entities from the list of sectors where these meet a certain threshold. While enhancing the legal clarity to the NIS 2 Directive, options C.1 and C.2 will not affect the CER Directive, making them coherent with the CER. Option C.3 is of low coherence as would repeal cybersecurity measures from the Directive. Additionally, options D and particular option D.3 will complement the CER Directive insofar as it provides for supply chain aspects as part of resilience measures of critical entities, making this option highly coherent.
- **Cyber Resilience Act and the New Legislative Framework (NLF):** options B are assessed as coherent with the CRA, as they will support demonstrating compliance with the CRA. Options B.2 and B.3 are assessed as highly coherent as they will also look to align with the NLF. Similarly, options A.2 and A.3 are highly coherent as they strengthen the mandate of ENISA to ensure delivering of tasks prescribed by the CRA. Options D and in particular option D.3 was assessed as highly coherent as it will complement the market surveillance mechanism foreseen in the CRA that tackles technical risks. Coherence of option D.2 is assessed as medium as it only covers 5G networks.
- **MFF:** The proposals for Multiannual Financial Framework (MFF) programmes include a horizontal provision which mandates the exclusion of high-risk suppliers identified under EU law, in order to protect the integrity of the EU budget and ensure

that Union expenditure does not contradict essential Union security interest. Option D.3 is highly coherent with this proposal as it will identify high-risk suppliers in the ICT supply chains and option D.2 can be assessed as of medium coherence (as only covers 5G networks),

Given the international character of cybersecurity, when designing the measures, international developments and solutions were also studied to compare the proposed solutions with trends in other jurisdictions. The proposed measures are therefore also in line with the international developments and in particular:

- Options B.2 and B.3 are coherent with the developments in the US, as regards the US Cyber Trust Mark programme, an IoT cybersecurity labelling scheme by the National Institute of Standards and Technology[329]; the US Cybersecurity and Infrastructure Security Agency (CISA) technical recommendations on software security, including security by design[330] and related concepts such as 'Software Bill Of Materials' [331] and the US FedRAMP provides a standardized, reusable approach to security assessment and authorization for cloud service offerings[332]. In Japan, the Cyber STAR (JC-STAR), a cybersecurity labelling scheme for IoT products, was launched in March 2025. Other jurisdictions such as Singapore[333] have taken similar initiatives on cybersecurity certification or labelling schemes for products, mostly of voluntary nature with the exception of the United Kingdom[334].
- Options C are coherent with the initiatives regarding reporting of the ransomware, such as an international Counter-Ransomware Initiative (CRI)[335]. Other countries are taking further initiatives to gain more insights into ransomware attack, such as the UK[336] and Australia[337] .

[329] NIST, *Consumer IoT Cybersecurity*, https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity.
[330] CISA, *Secure by Design*, https://www.cisa.gov/securebydesign.
[331] CISA, *2025 Minimum Elements for a Software Bill of Materials (SBOM)*, https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom.
[332] See FedRAMP Marketplace: https://marketplace.fedramp.gov/products?status=authorized.
[333] CSA, *About Cybersecurity Labelling Scheme for IoT - CLS(IoT)*, https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about.
[334] GOV.UK, *The UK Product Security and Telecommunications Infrastructure (Product Security) regime*, https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime.
[335] Counter Ransomware Initiative (CRI), *About Us*, https://counter-ransomware.org/aboutus.
[336] GOV.UK, *Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting*, https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible#proposal-3-a-ransomware-incident-reporting-regime.
[337] Australian Department of Home Affairs, *Mandatory ransomware and cyber extortion payment reporting is active from 30 May 2025*, https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-ransomware-payment-reporting.pdf.

- Options D.2 and D.3 are coherent with initiatives in the US[338], the UK[339], Australia[340] and Canada[341] with legislation allowing the government to take measures to safeguard from, restrict or control presence of high-risk suppliers in the telecommunication infrastructure. In addition, the US introduced prohibitions as regards the sale of connected vehicles and related hardware and software from China and Russia[342]. Within the G7, member countries are working on the issue of the supply chain security and notably to address non-technical risks in Internet of things[343].

The result of the assessment of the options shows that options A.2, combination of B.2/B.3 with C.2/C.3 3 are option D.3 of the highest coherence with other legal instruments and international developments.

[338] The Secure Equipment Act (2021) requires the US Federal Communications Commission (FCC) to issue rules stating that it will no longer review or approve any authorization application for equipment that poses an unacceptable risk to national security.
[339] The Telecommunications (Security) Act (2021) Act gives the government powers to control the presence of high-risk vendors in UK public telecoms networks where necessary in the interests of national security.
[340] The Security Legislation Amendment (Critical Infrastructure) Bill 2020 allows the government to take measures regarding entities that are likely subject to extrajudicial directions from a foreign government that conflict with Australian law.
[341] The proposed law on cybersecurity would allow the government to take measures to safeguard the security of telecommunications infrastructure, including measures related to high-risk suppliers.
[342] U.S. Commerce Department final rule implementing Executive Order 13873, effective March 17, 2025, aims to prevent unauthorized access to U.S. vehicle data by entities under the jurisdiction of these foreign governments. This rule bans vehicles with connected vehicle systems (VCS) or automated driving systems (ADS) software and hardware linked to China or Russia.
[343] G7 Cybersecurity Working Group Statement on IoT Security (2025), https://www.nisc.go.jp/pdf/press/G7_Statement_on_IoT_Security.pdf.

# ANNEX 15: MONITORING AND EVALUATION INDICATORS

*Table 34: Monitoring and evaluation indicators per Specific Objective*

| *Specific Objective* | *Indicator* | *Baseline* | *Frequency* | *Target* | *Source* |
|---|---|---|---|---|---|
| 1. Create the capacity to effectively implement Union cybersecurity policies and regular/continuous operational cooperation enabling more structured cooperation between Member States. | Number of relevant contributions from ENISA to the implementation of EU and national policies and legislative initiatives<br><br>Positive feedback by stakeholders regarding the relevant ENISA contributions | 2023 | Annual | Increase by 25 % compared to 2023 baseline as reported in ENISA Annual Activity Report (for the number of relevant contributions) and as per ENISA's annual satisfaction survey (for the positive feedback) | ENISA Annual Activity Report<br><br>ENISA's annual satisfaction survey |
| | Usage statistics of EU Vulnerability Database | 2025 | Annual | Increase by 25 % of number of users compared to 2025 | EU Vulnerability Database |
| | Number of alerts issued by ENISA to the CSIRTs network | 2029 | Annual | Increase by 25% of alerts compared to baseline of 2029 | ENISA |
| 2. Develop and implement the means and mechanisms to effectively support and address the needs | Number of stakeholders supported by ENISA and quality of the provided | 2025 | Annual | Increased by 10% number of supported stakeholders and increased by 10% satisfaction | European Commission's stakeholder consultation ENISA's annual satisfaction |

| | | | | | |
|---|---|---|---|---|---|
| of Member States, industry and other stakeholders. | support<br><br>Number of measures deployed to support stakeholders | | | level of supported stakeholders | survey |
| 3. Create the prerequisites for faster delivery of cybersecurity certification schemes driven by market needs by broadening the scope of the ECCF, ensuring effective maintenance and agile procedures and increasing transparency. | Number of adopted schemes | 2025 | Biennial | Decreased time to develop a scheme by 50% | ENISA |
| | Number of valid certificates issued annually | 2025 | Annual | Increase by 25 % over 2025 baseline | Annual reporting by NCCAs |
| | Positive feedback of stakeholders regarding their involvement in scheme development and transparency of the ECCF | 2025 | Annual | Increase by 25 % over baseline in ENISA's annual satisfaction survey | ENISA's annual satisfaction survey |
| 4. Create mechanisms and conditions to facilitate compliance with cybersecurity requirements, thereby making their implementation more coherent and effective. | Percentage of SMEs cost for compliance with NIS2 and cybersecurity rules, as a proportion of all compliance costs | 2025 | Biennial | <70 % SMEs reporting reduction in compliance costs for cybersecurity | SME Survey,<br><br>ENISA Investment Reports |
| | Number of ransomware attacks and | 2027 | Annual | | |

| | | | | | |
|---|---|---|---|---|---|
| | amount of damages in EUR | | | Reduce number of ransomware attacks by > 1% | ENISA NIS2 incident reports |
| | Percentage of cross-border incidents during or after which Member States' authorities used mutual assistance mechanisms | 2025 | Annual | Increase proportion of cases where mutual assistance was used by >20 percentage points | Information made available via NIS Cooperation Group (cf. NIS2 Article 14(4)(j)-(k)), and information directly made available to ENISA |
| 5. De-risk critical ICT supply chains from entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers) and reduce critical dependencies by developing a coherent and effective framework at EU level to address ICT supply chain security risks | Number of measures adopted<br><br>Decrease of dependency on high-risk suppliers | 2025 | Biennial | Increase by 25% of number of measures adopted and key assets identified compared to adoption date + 6 months<br><br>Decrease of dependencies on high-risk suppliers in key assets by 25%. | European Commission independent reports |