Council of the
European Union

Brussels, 20 December 2018
(OR. en)

15786/18

Interinstitutional File:
2017/0225(COD)

CYBER 336
TELECOM 502
CODEC 2420
COPEN 464
COPS 490
COSI 328
CSC 391
CSCI 181
IND 425
JAI 1335
JAIEX 175
POLMIL 232
RELEX 1124

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for 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")

Following the Coreper meeting on 19 December 2018, delegations will find attached the final version of the text agreed with the European Parliament on the above-mentioned proposal.

ANNEX

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "European Union Agency for Cybersecurity", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

Whereas:

(1) Network and information systems and telecommunications networks and services play a vital role for society and have become the backbone of economic growth. Information and communications technology (ICT) underpins the complex systems which support everyday societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and in particular support the functioning of the internal market.

(2) The use of network and information systems by citizens, businesses and governments across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the Internet of Things (IoT) millions, if not billions, of connected digital devices are expected to be deployed across the EU during the next decade. While an increasing number of devices are connected to the Internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In this context, the limited use of certification leads to insufficient information for organisational and individual users about the cybersecurity features of ICT products and services, undermining trust in digital solutions.

Network and information systems have the potential to support all aspects of our lives, drive the Union’s economic growth. They are the backbone to achieve the digital single market.

(3) Increased digitisation and connectivity lead to increased cybersecurity risks, thus making society at large more vulnerable to cyber threats and exacerbating dangers faced by individuals, including vulnerable persons such as children. In order to mitigate this risk to society, all necessary actions need to be taken to improve cybersecurity in the EU to better protect network and information systems, telecommunication networks, digital products, services and devices used by citizens, governments and business – from SMEs to operators of critical infrastructures – from cyber threats.

(3b) By providing and making available relevant information to the public, ENISA contributes to the development of the cybersecurity industry in the EU, in particular SMEs and start-ups. ENISA should strive for a closer cooperation with universities and research entities in order to contribute to a strategic approach to reducing dependencies on cybersecurity products and services from outside the Union and on supply chains inside the Union.

(4) Cyber-attacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyber-attacks are often cross-border, policy responses by cybersecurity authorities and law enforcement competences are predominantly national. Large-scale cyber incidents could disrupt the provision of essential services across the EU. This requires effective, coordinated EU level response and crisis management, building upon dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of cybersecurity and resilience in the Union, based on reliable Union data, as well as systematic forecast of future developments, challenges and threats, both at Union and global level, is therefore important for policy makers, industry and users.

(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation including information sharing and coordination cross Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises, while underlining the importance of maintaining and further enhancing the national capabilities to respond to cyber threats of all scales.

Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, given that cyber incidents undermine trust in digital service providers and in the digital single market itself, especially among consumers, trust should be further improved by offering transparent information on the level of security of ICT products, processes and services stressing that even a high level of cybersecurity certification cannot guarantee an ICT product or service is completely secure. This can be facilitated by EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors.

(5a) Cybersecurity is not just a technology issue, but human behaviour is equally important. Therefore, 'cyber hygiene', understood as simple routine measures that when implemented and carried out regularly by citizens, organisations and businesses minimise their exposure to risks from cyber threats, should be strongly promoted.

(5b) For the purpose of strengthening European cybersecurity structures, it is important to maintain and develop the capabilities of Member States to comprehensively respond to cyber threats, including cross-border incidents.

(5c) Businesses as well as individual consumers should have accurate information regarding with what level assurance the security of their ICT products, processes and services have been certified. At the same time, it has to be understood that no product is cyber secure and that basic rules of cyber hygiene have to be promoted and prioritised.

Given the growing availability of IoT devices, there are a range of voluntary measures that the private sector can take to reinforce trust in the security of ICT products, processes and services.

(5d) Organizations, manufacturers or providers should be encouraged to implement measures, at the earliest stages of the design and development of the ICT products, processes and services in such a way that the security of those products, processes and service is protected to the highest possible degree from the start, that the occurrence of attacks is presumed and their impact is anticipated and minimised ('security by design'). Security should be addressed throughout the lifetime of the product with the design and development processes constantly evolving to reduce the harm from malicious exploitation.

(5e) Security by default should not require extensive configuration to work, nor specific technical understanding or non-obvious behaviour from the user, and should simply work reliably where implemented. Undertakings, organisations and the public sector should configure the ICT products, services or process designed by them in a way that ensures a higher degree of security which should enable the first user to receive a default configuration with the most secure settings possible ('security by default') and reducing the burden on users to have to configure a product appropriately. If, on a case-by-case basis, risk and usability analysis lead to the conclusion that such a setting by default is not feasible, users should be prompted to opt for the most secure setting.

(6) In 2004, the European Parliament and the Council adopted Regulation (EC) No 460/2004 establishing ENISA with the purpose of contributing to the goals of ensuring a high level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. In 2008, the European Parliament and the Council adopted Regulation (EC) No 1007/2008 extending the mandate of the Agency until March 2012.

Regulation (EC) No 580/2011 extended further the mandate of the Agency until 13 September 2013. In 2013, the European Parliament and the Council adopted Regulation (EU) No 526/2013 concerning ENISA and repealing Regulation (EC)No 460/2004, which extended the Agency's mandate until June 2020.

(7) The Union has already taken important steps to ensure cybersecurity and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to cybersecurity threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive").

The NIS Directive put in place requirements concerning national capabilities in the area of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for economy and society such as energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces). Other legal instruments such as the Directive establishing the European Electronic Communications Code, the Regulation (EU) 2016/679 and the Directive 2002/58/EC also contribute to a high level of cybersecurity in the Digital Single Market.

A key role was attributed to ENISA in supporting implementation of this Directive. In addition, effective fight against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity.

(8) It is recognised that, since the adoption of the 2013 EU Cybersecurity Strategy and the last revision of the Agency's mandate, the overall policy context has changed significantly, also in relation to a more uncertain and less secure global environment. In this context and in the context of the positive development of the role of the Agency as reference point of advice and expertise, as a facilitator of cooperation and of capacity building as well as within the framework of the new Union cybersecurity policy, it is necessary to review the mandate of ENISA to define its role in the changed cybersecurity ecosystem and ensure it contributes effectively to the Union's response to cybersecurity challenges emanating from this radically transformed threat landscape, for which, as recognised by the evaluation of the Agency, the current mandate is not sufficient.

(9) The Agency established by this Regulation should succeed ENISA as established by Regulation (EU) No 526/2013. The Agency should carry out the tasks conferred on it by this Regulation and legal acts of the Union in the field of cybersecurity by, among other things, providing expertise and advice and acting as a Union centre of information and knowledge. It should promote the exchange of best practices between Member States and private stakeholders, offering policy suggestions to the European Commission and Member States, acting as a reference point for Union sectoral policy initiatives with regard to cybersecurity matters, fostering operational cooperation between the Member States and between the Member States and the Union institutions, agencies and bodies.

(10) Within the framework of Decision 2004/97/EC, Euratom, adopted at the meeting of the European Council on 13 December 2003, the representatives of the Member States decided that ENISA would have its seat in a town in Greece to be determined by the Greek Government. The Agency's host Member State should ensure the best possible conditions for the smooth and efficient operation of the Agency. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and to enhance the efficiency of networking activities that the Agency be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of the Agency. The necessary arrangements should be laid down in an agreement between the Agency and the host Member State concluded after obtaining the approval of the Management Board of the Agency.

(11) Given the increasing cybersecurity risks and challenges the Union is facing, the financial and human resources allocated to the Agency should be increased to reflect its enhanced role and tasks, and its critical position in the ecosystem of organisations defending the European digital ecosystem, allowing ENISA to effectively carry out the tasks conferred on it by this Regulation.

(12) The Agency should develop and maintain a high level of expertise and operate as a point of reference establishing trust and confidence in the single market by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in carrying out its tasks. The Agency should actively support national and proactively contribute to Union efforts while carrying out its tasks in full cooperation with the Union institutions, agencies and bodies and the Member States, avoiding any duplication of work and promoting synergy. In addition, the Agency should build on input from and cooperation with the private sector as well as other relevant stakeholders.

A set of tasks should establish how the Agency is to accomplish its objectives while allowing flexibility in its operations.

(12b) In order to be able to provide adequate support to the operational cooperation of the Member States, ENISA should further strengthen its technical and human capabilities and skills. ENISA should increase its know-how and capacities. ENISA and Member States, on a voluntary basis, could develop programmes for seconding national experts to the Agency, creating pools of experts and staff exchange.

(13) The Agency should assist the Commission by means of advice, opinions and analyses on all the Union matters related to policy and law development, update and review in the area of cybersecurity and its sector-specific aspects in order to enhance relevance of EU policies and law with cybersecurity dimension and enable consistency in their implementation at national level. The Agency should act as a reference point of advice and expertise for Union sector-specific policy and law initiatives where matters related to cybersecurity are involved. The Agency should regularly update the European Parliament on its activities.

(13a) The public core of the open internet, meaning its main protocols and infrastructure, which are a global public good, provides the essential functionality of the Internet as a whole and underpins its normal operation. ENISA should support the security and stability of its functioning including, but not limited to key protocols (in particular DNS, BGP, and IPv6), the operation of the Domain Name System (including those of all Top Level Domains), and the operation of the Root Zone.

(14) The underlying task of the Agency is to promote the consistent implementation of the relevant legal framework, in particular the effective implementation of the NIS Directive and other relevant legal instruments containing cybersecurity aspects, which is essential in order to increase cyber resilience. In view of the fast evolving cybersecurity threat landscape, it is clear that Member States must be supported by more comprehensive, cross-policy approach to building cyber resilience.

(15) The Agency should assist the Member States and Union institutions, agencies and bodies in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cyber threats and incidents and in relation to the security of network and information systems. In particular, the Agency should support the development and enhancement of national and Union CSIRTs with a view of achieving a high common level of their maturity in the Union. Activities carried out by ENISA relating to the operational capacities of Member States should actively support actions taken by Member States in order to fulfil their obligations arising from the NIS Directive and thus should not supersede them.

(15a) The Agency should also assist with the development and update of Union and upon request, Member States strategies on the security of network and information systems, in particular on cybersecurity, promote their dissemination and follow the progress of their implementation. The Agency should also offer contribute to cover the need for trainings and training material including to public bodies, and where appropriate to a high extent "train the trainers" building on the Digital Competence Framework for Citizens and with a view to assisting Member States and Union institutions, bodies and agencies in developing their own training capabilities.

(15b) The Agency should support Member States in the area of cybersecurity education and awareness raising by facilitating closer coordination and exchange of best practices amongst them. Such support could consist, amongst others, in development of a network of national education points of contact and of a cybersecurity training platform. The network of national education points of contact could operate within the National Liaison Officers Network and enable a starting point for future coordination within the Members States.

(16) The Agency should assist the Cooperation Group established in the NIS Directive in the execution of its tasks, in particular by providing expertise, advice and facilitate the exchange of best practices, notably with regard to the identification of operators of essential services by Member States, including in relation to cross-border dependencies, regarding risks and incidents.

(17) With a view to stimulating cooperation between public and private sector and within the private sector, in particular to support the protection of the critical infrastructures, the Agency should support information sharing in and between sectors, in particular in the sectors listed in Annex II of Directive (EU) 2016/1148, by providing best practices and guidance on available tools, procedure, as well as providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral Information Sharing and Analysis Centres (ISACs).

(17a) Whereas the potential negative impact of vulnerabilities in ICT products and services is constantly increasing, finding and remedying such vulnerabilities plays an important role in reducing the overall cybersecurity risk. Cooperation between the organizations, manufacturers or providers of vulnerable products and services, and members of the cybersecurity research community and governments who find such vulnerabilities has been proven to significantly increase both the rate of discovery and remedy of vulnerabilities in ICT products and services. Coordinated vulnerability disclosure specifies a structured process of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organization the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or the public. The process also provides for coordination between the finder and the organization as regards the publication of said vulnerabilities. Coordinated vulnerability disclosure management processes can play an important role in Member States' efforts to enhance cybersecurity.

(18) The Agency should aggregate and analyse voluntary shared national reports from CSIRTs and CERT-EU, for the purpose of contributing to the setting up common procedures, language and terminology for exchange of information. The Agency should also involve the private sector, within the framework of the NIS Directive which laid down the grounds for voluntary technical information exchange at the operational level within the CSIRTs Network.

(19) The Agency should contribute to an EU level response in case of large-scale cross-border cybersecurity incidents and crises. This function should be performed in accordance with its mandate pursuant to this Regulation and an approach to be agreed by Member States in the context of the Commission Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises and the Council conclusions on EU coordinated response to large scale cybersecurity incidents and crises. It could include gathering relevant information and acting as facilitator between the CSIRTs Network and the technical community as well as decision makers responsible for crisis management. Furthermore, the Agency could support the operational cooperation among Member States by, upon request of one or more Member States, the handling of incidents from a technical perspective facilitating relevant technical exchange of solutions between Member States and by providing input into public communications. The Agency should support the process by testing modalities of such cooperation through regular cybersecurity exercises.

(20) In supporting operational cooperation, the Agency should make use of the available technical and operational expertise of CERT-EU through a structured cooperation. The structured cooperation can build-up of ENISA's expertise. Where appropriate, dedicated arrangements between the two organisations should be established to define the practical implementation of such cooperation and avoid duplication of activities.

(21) In compliance with its tasks to support operational cooperation within the CSIRTs Network, the Agency should be able to provide support to Member States at their request, such as by providing advice on how to improve their capabilities to prevent, detect and respond to incidents, by facilitating the technical handling of incidents having a significant or substantial impact or by ensuring analyses of threats and incidents. ENISA should facilitate the technical handling of incidents having a significant or substantial impact in particular by supporting the voluntary sharing of technical solutions between Member States or produces combined technical information - such as technical solutions voluntarily shared by the Member States.

The Commission's Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises recommends that Member States cooperate in good faith and share amongst themselves and with ENISA information on large-scale cybersecurity incidents and crises without undue delay. Such information should further help ENISA in performing its tasks of supporting operational cooperation.

(22) As part of the regular cooperation at technical level to support Union situational awareness, the Agency should on regular basis and in close cooperation with Member States prepare in-depth EU Cybersecurity Technical Situation Reports on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs or NIS Directive Single Points of Contact (both on a voluntary basis), European Cybercrime Centre (EC3) at Europol, CERT-EU and, where appropriate, European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission, the High Representative of the Union for Foreign Affairs and Security Policy and the CSIRTs Network.

(23) The support by the Agency to ex-post technical inquiries of incidents with significant or substantial impact undertaken upon request the Member States concerned should be focused on the prevention of future incidents. The Member States concerned should provide the necessary information and assistance in order to enable the Agency to effectively support the technical enquiry.

(25) Member States may invite undertakings concerned by the incident to cooperate by providing necessary information and assistance to the Agency without prejudice to their right to protect commercially sensitive information and information relevant to public security.

(26) To understand better the challenges in the field of cybersecurity, and with a view to providing strategic long term advice to Member States and Union institutions, the Agency needs to analyse current and emerging risks. For that purpose, the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant publicly available or voluntary shared information and perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on network and information security, in particular cybersecurity. The Agency should furthermore support Member States and Union institutions, agencies and bodies in identifying emerging risks and preventing cybersecurity incidents, by performing analyses of threats, vulnerabilities and incidents.

(27) In order to increase the resilience of the Union, the Agency should develop excellence on the subject of cybersecurity of infrastructures supporting in particular the sectors listed in Annex II of the NIS Directive and those used by the digital service providers listed in Annex III of that Directive, by providing advice, guidance and best practices. With a view to ensuring easier access to better structured information on cybersecurity risks and potential remedies, the Agency should develop and maintain the "information hub" of the Union, a one-stop-shop portal providing the public with information on cybersecurity deriving from the EU and national institutions, agencies and bodies. Facilitating access to better structured information on cybersecurity risks and potential remedies can also help Member States bolster their capacities and align their practices, hence increasing their overall resilience in the face of cyber-attacks.

(28) The Agency should contribute towards raising the awareness of the public, including by an EU-wide awareness raising campaign, by promoting education, about cybersecurity risks and provide guidance on good practices for individual users aimed at citizens, organisations and businesses. The Agency should also contribute to promote best practices and solutions, including cyber hygiene and cyber literacy, at the level of individuals, organisations and businesses by collecting and analysing publicly available information regarding significant incidents, and by compiling and publishing reports and guides with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. ENISA should also strive to provide consumers with relevant information on applicable certification schemes, for example by providing guidelines and recommendations.

The Agency should furthermore organise, in line with the Digital Education Action Plan and in cooperation with the Member States and the Union institutions, agencies and bodies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour, digital literacy and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, data fraud incidents and, as well as promoting basic multi-factor authentication, patching, encryption, anonymization and data protection advice.

The Agency should play a central role in accelerating end-user awareness on security of devices and secure use of services, promoting at EU level security-by-design and privacy-by-design. In achieving this objective, the Agency should make best use of available best practices and experience, especially from academic institutions and IT security researchers.

(29) In order to support the businesses operating in the cybersecurity sector, as well as the users of cybersecurity solutions, the Agency should develop and maintain a "market observatory" by performing regular analyses and dissemination of the main trends in the cybersecurity market, both on the demand and supply side.

(29a) The Agency should contribute to the Union's efforts for cooperation with international organisations as well as within relevant international cooperation frameworks in the area of cybersecurity. In particular, the Agency should contribute, where appropriate, to the cooperation with organisations such as OECD, OSCE and NATO. Such cooperation could include, amongst others, joint cybersecurity exercises and joint cyber incident response coordination. This shall be in full respect of the principles of inclusiveness, reciprocity and decision making autonomy of the Union, without prejudice to the specific character of the security and defence policy of any Member State.

(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant EU supervisory and other competent authorities, Union institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Global Navigation Satellite Systems Agency (GNSS Agency), Body of European Regulators for Electronic Communications (BEREC), European Agency for the operational management of large-scale IT systems (eu-LISA), European Central Bank (ECB), European Banking Authority (EBA), European Data Protection Board (EDPB), EU Agency for the Cooperation of Energy Regulators (ACER), European Aviation Safety Agency (EASA) and any other EU Agency that is involved in cybersecurity.

It should also liaise with authorities dealing with data protection in order to exchange know-how and best practices and provide advice on cybersecurity aspects that might have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the ENISA Advisory Group. In liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks.

Partnerships could be established with academic institutions that have research initiatives in the relevant areas, while the input from consumer organisations and other organisations should have appropriate channels and should be taken into consideration.

(31) The Agency, in its role as a Secretariat of the CSIRTs Network, should support Member State CSIRTs and the CERT-EU in operational cooperation further to all the relevant tasks of the CSIRTs Network, as defined by the NIS Directive. Furthermore, the Agency should promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or protected by the CSIRTs and involving or potentially involving at least two CERTs while taking due account of the Standard Operating Procedures of the CSIRTs Network.

(32) With a view to increasing Union preparedness in responding to cybersecurity incidents, the Agency should organise regular cybersecurity exercises at Union level, and, at their request, support Member States and EU institutions, agencies and bodies in organising exercises. Once every two years a large-scale comprehensive exercise should be organised which includes technical, operational or strategic elements. In addition, the Agency can organise regularly less comprehensive exercises with the same goal of increasing Union preparedness in responding to cybersecurity incidents

(33) The Agency should further develop and maintain its expertise on cybersecurity certification with a view to supporting the Union policy in this field. The Agency should build upon existing best practices and promote the uptake of cybersecurity certification within the Union, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthening trust in the digital internal market.

(34) Efficient cybersecurity policies should be based on well-developed risk assessment methods, both in the public and private sector. Risk assessment methods are used at different levels with no common practice regarding how to apply them efficiently. Promoting and developing best practices for risk assessment and for interoperable risk management solutions in public- and private-sector organisations will increase the level of cybersecurity in the Union. To this end, the Agency should support cooperation between stakeholders at Union level, facilitating their efforts relating to the establishment and take-up of European and international standards for risk management and for measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems.

(35) The Agency should encourage Member States, product manufacturers and service providers to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal cybersecurity and be incentives to do so. In particular, service providers and product manufacturers should provide necessary updates and recall, withdraw or recycle products and services that do not meet cybersecurity standards, while importers and distributors should make sure that ICT products, processes, services they place on the EU market comply with the applicable requirements and do not present a risk to European consumers.

In cooperation with competent authorities, ENISA may disseminate information regarding the level of cybersecurity of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the security, including cybersecurity, of their products.

(36) The Agency should take full account of the ongoing research, development and technological assessment activities, in particular those carried out by the various Union research initiatives to advise the Union institutions, agencies and bodies and where relevant, the Member States, at their request, on research needs in the area of cybersecurity. In order to identify the research needs and priorities, the Agency should also consult the relevant user groups. More specifically, a cooperation with the European Research Council (ERC) and the European Institute for Innovation and Technology (EIT) as well as with the European Union Institute for Security Studies (EUISS) could be established.

(36a) The Agency should regularly consult standardisation organisations, in particular European standardisation organisations, when preparing the European Cybersecurity Certification Schemes.

(37) Cybersecurity threats are global issues. There is a need for closer international cooperation to improve cybersecurity standards, including the definition of common norms of behaviour and codes of conduct, use of international standards, and information sharing, promoting swifter international collaboration in response to, as well as a common global approach to, network and information security issues. To that end, the Agency should support further Union involvement and cooperation with third countries and international organisations by providing, where appropriate, the necessary expertise and analysis to the relevant Union institutions, agencies and bodies.

(38) The Agency should be able to respond to ad hoc requests for advice and assistance by Member States and EU institutions, agencies and bodies falling within the Agency's objectives.

(39) It is sensible and recommended to implement certain principles regarding the governance of the Agency from the Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agencies, the purpose of which statement and approach is to streamline the activities of agencies and improve their performance. The Joint Statement and Common Approach's guidance to the Agency's Work Programmes, evaluations of the Agency, and the Agency's reporting and administrative practice should be also reflected, as appropriate.

(40) The Management Board, composed of the Member States and the Commission, should define the general direction of the Agency's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, adopt the Agency's Single Programming Document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.

(41) In order for the Agency to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Management Board have appropriate professional expertise and appropriate experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Management Board in order to ensure continuity in its work.

(42) The smooth functioning of the Agency requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence. The Executive Director should prepare a proposal for the Agency's work programme, after prior consultation with the Commission, and take all necessary steps to ensure the proper execution of the work programme of the Agency. The Executive Director should prepare an annual report including the implementation of the Agency's annual work programme to be submitted to the Management Board, draw up a draft statement of estimates of revenue and expenditure for the Agency, and implement the budget. Furthermore, the Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific, technical, legal or socioeconomic nature. Notably in relation to the preparation of a specific candidate scheme, the establishment of an ad hoc working group is considered necessary.

The Executive Director should ensure that the ad hoc Working Groups' members are selected according to the highest standards of expertise, taking due account of a representative and gender balance, as appropriate according to the specific issues in question, between the public administrations of the Member States, the Union institutions and the private sector, including industry, users, and academic experts in network and information security.

(43) The Executive Board should contribute to the effective functioning of the Management Board. As part of its preparatory work related to Management Board decisions, it should examine in detail relevant information and explore available options and offer advice and solutions to prepare relevant decisions of the Management Board.

(44) The Agency should have a ENISA Advisory Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The ENISA Advisory Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the attention of the Agency. The composition of the Permanent Stakeholders Group and the tasks assigned to this Group, to be consulted in particular regarding the draft work programme, should ensure sufficient representation of stakeholders in the work of the Agency.

(44a) The Stakeholder Cybersecurity Certification Group should be established in order to help the Agency and the Commission facilitating consultation with relevant stakeholders. The Group should be composed of members representing in balanced proportion industry, both on the demand as well as the supply side of ICT products and services and including in particular small and medium-sized enterprises, digital service providers, European and international standardisation bodies, accreditation bodies, data protection supervisory authorities and conformity assessment bodies pursuant to Regulation (EC) 765/2008, academia as well as consumer organisations.

(45) The Agency should have in place rules regarding the prevention and the management of conflict of interest. The Agency should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council. Processing of personal data by the Agency should be subject to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The Agency should comply with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information.

(46) In order to guarantee the full autonomy and independence of the Agency and to enable it to perform additional and new tasks, including unforeseen emergency tasks, the Agency should be granted a sufficient and autonomous budget whose revenue comes primarily from a contribution from the Union and contributions from third countries participating in the Agency's work. An appropriate budget is paramount for ensuring that the Agency has sufficient capacities to fulfil all its growing tasks and objectives. The majority of the Agency staff should be directly engaged in the operational implementation of the Agency's mandate. The host Member State, or any other Member State, should be allowed to make voluntary contributions to the revenue of the Agency. The Union's budgetary procedure should remain applicable as far as any subsidies chargeable to the general budget of the Union are concerned. Moreover, the Court of Auditors should audit the Agency's accounts to ensure transparency and accountability.

(48) Cybersecurity certification plays an important role in increasing trust and security in ICT products, services and processes. The digital single market, and particularly the data economy and the Internet of Things, can only thrive if there is general public trust that such products, services and processes provide a certain level of cybersecurity assurance. Connected and automated cars, electronic medical devices, industrial automation control systems or smart grids are only some examples of sectors in which certification is already widely used or is likely to be used in the near future. The sectors regulated by the NIS Directive are also sectors in which cybersecurity certification is critical.

(49) In the 2016 Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", the Commission outlined the need for high-quality, affordable and interoperable cybersecurity products and solutions. The supply of ICT products, services and processes within the single market remains very fragmented geographically. This is because the cybersecurity industry in Europe has developed largely on the basis of national governmental demand. In addition, the lack of interoperable solutions (technical standards), practices and EU-wide mechanisms of certification are among the other gaps affecting the single market in cybersecurity. On the one hand, this makes it difficult for European companies to compete at national, European and global level. On the other, it reduces the choice of viable and usable cybersecurity technologies that individuals and enterprises have access to.

Similarly, in the Mid-Term Review on the implementation of the Digital Single Market Strategy, the Commission highlighted the need for safe connected products and systems, and indicated that the creation of a European ICT security framework setting rules on how to organise ICT security certification in the Union could both preserve trust in the internet and tackle the current fragmentation of the cybersecurity market.

(50) Currently, the cybersecurity certification of ICT products, services and processes is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In this context, a certificate issued by one national cybersecurity authority is not in principle recognised by other Member States. Companies thus may have to certify their products, services and processes in several Member States where they operate, for example with a view to participating in national procurement procedures, thereby adding to their costs. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach with regard to horizontal cybersecurity issues, for instance in the field of the Internet of Things.

Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual utilisation, impeding mutual recognition mechanisms within the Union.

(51) Some efforts have been made in the past in order to lead to a mutual recognition of certificates in Europe. However, they have been only partly successful. The most important example in this regard is the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA). While it represents the most important model for cooperation and mutual recognition in the field of security certification, SOG-IS includes only part of the Union Member States. This has limited the effectiveness of SOG-IS MRA from the point of view of the internal market.

(52) In view of the above, it is necessary to adopt a common approach and establish a European cybersecurity certification framework laying down the main horizontal requirements for European cybersecurity certification schemes to be developed and allowing certificates and EU statements of conformity for ICT products and services to be recognised and used in all Member States. In so doing, it is essential to build on existing national and international schemes, as well as on mutual recognition systems, in particular SOG-IS, and to make possible a smooth transition from existing schemes under such systems to schemes under the new European framework. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products, services and processes that have been certified according to such schemes.

On the other hand, it should avoid the multiplication of conflicting or overlapping national cybersecurity certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should be non-discriminatory and based on international and / or European standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.

(52a) The European cybersecurity certification framework should be established in a uniform manner in all Member States in order to prevent 'certification shopping' based on differences in levels of stringency between Member States.

(52b) European cybersecurity certification schemes should be built upon what already exists at international and national level and, if necessary, on technical specifications from fora and consortia, learning from current strong points and assessing and correcting weaknesses.

(52c) Flexible cybersecurity solutions are necessary for the industry to stay ahead of cyber threats and therefore any certification scheme should avoid the risk of being outdated quickly.

(53) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products, services and processes. These schemes should be implemented and supervised by national cybersecurity certification authorities and certificates issued within these schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or other private organisations should fall outside the scope of the Regulation. However, the bodies operating such schemes may propose to the Commission to consider such schemes as a basis for approving them as a European scheme.

(54) The provisions of this Regulation should be without prejudice to Union legislation providing specific rules on certification of ICT products, services and processes. In particular, the General Data Protection Regulation (GDPR) lays down provisions for the establishment of certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with that Regulation of processing operations by controllers and processors. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of relevant products and services. The present Regulation is without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR.

(55) The purpose of European cybersecurity certification schemes should be to ensure that ICT products, services and processes certified under such a scheme comply with specified requirements with the aim to protect the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems throughout their life cycle within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products, services and processes. ICT products, services and processes and related cybersecurity needs are so diverse that it is very difficult to come up with general cybersecurity requirements valid across the board.

It is, therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, complemented by a set of specific cybersecurity objectives that need to be taken into account when designing European cybersecurity certification schemes. The modalities with which such objectives will be achieved in specific ICT products, services and processes should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications where no appropriate standards are available.

(55a) The technical specifications to be used in a European cybersecurity certification scheme should be identified by respecting the principles laid down in Annex II of Regulation (EU) 1025/2012. Some deviations from these principles could be however considered necessary in duly justified cases where those technical specifications are to be used in a European cybersecurity certification scheme referring to assurance level high. The reasons for such deviations need to be made publicly available.

(55b) The certified conformity assessment is the process of evaluating whether specified requirements relating to an ICT process, product or service have been fulfilled. This process is carried out by an independent third party, other than the product manufacturer or service provider. The process of issuing a certificate follows the process of successful evaluation of an ICT product, service or process. It should be considered as a confirmation that the respective evaluation has been properly carried out. Depending on the assurance level, the European cybersecurity scheme should provide whether the certificate is being issued by a private or public body.

Conformity assessment and certification cannot guarantee per se that certified ICT products and services are cyber secure. It is rather a procedure and technical methodology to attest that ICT products and services have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example as specified in technical standards.

(55c) The choice, by the users of certificates, of the appropriate level of certification and associated security requirements should be based on a risk analysis on the use of the ICT products, services or processes. The level of assurance should be thus commensurate with the level of the risk associated with the intended use of an ICT product, service or process.

(55d) A European cybersecurity certification scheme could provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products and services (conformity self-assessment). In such cases, it is sufficient that the manufacturer or provider carries out himself all checks in order to ensure the conformity of the ICT products, services or processes with the certification scheme. This type of conformity assessment should be considered appropriate for low complexity ICT products and services (e.g. simple design and production mechanism) that present a low risk for the public interest. Moreover, only ICT products and services corresponding to assurance level basic could become subject to conformity self-assessment.

(55e) A European cybersecurity certification scheme could allow for both certification and conformity self-assessment of ICT products and services. In this case, the scheme should provide for clear and understandable means for consumers or other users to differentiate between products and services that are assessed under the responsibility of the manufacturer or provider and products and services that are certified by a third party.

(55f) The manufacturer or provider of ICT products and services carrying out a conformity self-assessment should draw up and sign the EU statement of conformity as part of the conformity assessment procedure. The EU statement of conformity is the document that states that particular ICT product or service complies with the requirements of the scheme. By drawing up and signing up of the EU statement of conformity, the manufacturer or provider assumes responsibility for the compliance of the ICT product or service with the legal requirements of the scheme. A copy of the EU statement of conformity should be submitted to the national cybersecurity certification authority and to ENISA.

(55g) The manufacturer or provider of ICT products and services should keep the EU statement of conformity and technical documentation of all relevant information relating to the conformity of the ICT products or services with a scheme at the disposal of the competent national cybersecurity certification authority for a period defined in the particular European cybersecurity certification scheme. The technical documentation should specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the ICT product or service. The technical documentation should be so compiled to enable the assessment of the conformity of an ICT product or service with the relevant requirements.

(55h) The governance of the Framework takes into account the involvement of Member States as well as appropriate involvement stakeholders and defines the role of the European Commission throughout the planning and proposing, requesting, preparing, adopting and reviewing of a European cybersecurity certification scheme.

(56) The Commission should prepare with the support of the European Cybersecurity Certification Group and the Stakeholder Cybersecurity Certification Group and after an open and wide consultation a Union rolling work programme for European Cybersecurity Certification schemes and publish it in the form of a legally non-binding instrument. The Union work programme should be a strategic document allowing in particular industry, national authorities and standardisation bodies to prepare in advance for future cybersecurity certification schemes.

The Union rolling work programme should include a multiyear overview of the requests for candidate schemes which the Commission intends to submit to ENISA for preparation based on justified grounds. The Commission should take into account this Union rolling work programme while preparing their Rolling Plan for ICT Standardisation, standardisation mandates. In view of the rapid introduction and uptake by users and companies of new technologies, the emergence of previously unknown cybersecurity risks or legislative and market developments, the Commission or the European Cybersecurity Certification Group should be entitled to request ENISA to prepare candidate schemes which were not be included in the Union rolling work programme. In such cases, the Commission and the European Cybersecurity Certification Group should also assess the necessity of such request by taking into account the overall aims and objectives of this Regulation and by ensuring the continuity as regards the Agency's planning and use of resources.

Following a request, ENISA should prepare without undue delay candidate schemes for specific ICT processes, products or services. The Commission should evaluate the positive and negative impact of its request on the specific market under the scope, especially on SMEs, innovation, barriers for entry and cost for end users. The Commission, based on the candidate scheme proposed by ENISA, should then be empowered to adopt the European cybersecurity certification scheme by means of implementing acts. Taking account of the general purpose and security objectives identified in this Regulation, European cybersecurity certification schemes adopted by the Commission should specify a minimum set of elements concerning the subject-matter, the scope and functioning of the individual scheme. ENISA can, under duly justified cases, refuse a request by the ECCG. Such decision should be made by the Management Board.

These should include among others the scope and object of the cybersecurity certification, including the categories of ICT products, services and processes covered, the detailed specification of the cybersecurity requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods, as well as the intended level of assurance: basic, substantial and/or high and the evaluation levels where applicable.

(56a) The assurance of a European certification scheme is the ground for confidence that an ICT process, product or service meets the security requirements of a specific European cybersecurity certification scheme. In order to ensure consistency of the framework on certified ICT processes, products and services, a European cybersecurity certification scheme could specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each certificate could refer to one of the assurance levels: basic, substantial or high, while the EU statement of conformity could only refer to the assurance level basic. The assurance levels provide a corresponding degree of efforts for the evaluation of and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent cybersecurity incidents.

Each assurance level should be consistent among the different sectorial domain where certification is applied.

(56b) A European cybersecurity certification scheme may specify several evaluations levels depending on the rigour and depth of the evaluation methodology used which should correspond to one of the assurance levels and should be associated with an appropriate combination of assurance components. For all assurance levels, the ICT product, service or process should contain a number of secure functions, as defined by the scheme, which may include: secure out of the box configuration, signed code, secure update and exploit mitigations and full stack/heap memory protections. Those functions should have been developed and be maintained, using security focused development approaches and associated tools to ensure that effective mechanisms (both software and hardware) are reliably incorporated.

For assurance level basic, the evaluation should be guided at least by the following assurance components: the evaluation should at least include a review of the technical documentations of the ICT product or service by the conformity assessment body. Where the certification includes ICT processes, subject to the technical review should also be the process used to design, develop and maintain an ICT product or service. In cases where a European cybersecurity certification scheme provides for a conformity self-assessment, it should be sufficient if the manufacturer or provider has carried out a self-assessment on the compliance of the ICT process, products or services with the certification scheme.

For assurance level substantial, the evaluation should in addition to assurance level basic be guided at least by the verification of the conformity of security functionalities of the ICT product or service to its technical documentation.

For assurance level high the evaluation should in addition to assurance level substantial be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product or service against those who perform elaborate cyber attacks having significant skills and resources.

(56d) ENISA should maintain a website providing information on, and publicity of, European cybersecurity certification schemes which should include, amongst others, the requests for the preparation of a candidate European cybersecurity certification scheme as well as the feedback received in the consultation process carried out by ENISA in the preparation phase. Such website should also provide information about certificates and EU statements of conformity issued under this Regulation including their withdrawn and expiration. The website should also indicate those national certification schemes that have been replaced by a European cybersecurity certification scheme.

(56e) Modern ICT products and systems often integrate and rely upon one or more third party technologies and components such as software modules, libraries or application programming interfaces (APIs). This reliance, referred to as a "dependency", may present additional cybersecurity risks as vulnerabilities found in third party components may also affect the security of the ICT product and services. In many cases, identifying and documenting such dependencies enables end users of ICT products and services to improve their cybersecurity risk management activities by improving, for examples, users' cybersecurity vulnerability management and remediation procedures.

(57) Recourse to European cybersecurity certification and EU statement of conformity should remain voluntary, unless otherwise provided in Union or Member States legislation adopted in accordance with Union law. In the absence of harmonised legislation, Member States may adopt national technical regulations in accordance with Directive (EU) 2015/1535 providing for mandatory certification under a European cybersecurity certification scheme. Member States could also use the recourse to European cybersecurity certification in the context of public procurement and Directive 2014/214/EU. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products, services and processes covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act.

(57aa) The certification according to this regulation should be voluntary. In some areas, it could be necessary in the future to make specific cybersecurity requirements and the certification thereof mandatory in certain products, processes or services to improve the level of cyber security in the Union. The Commission should regularly follow the impacts of adopted certification schemes on availability of secure ICT products, processes and services in the internal market and assess the level of utilization of the certification schemes by the manufacturers and service providers in the EU. The efficiency of the certification schemes and whether any particular schemes should be made mandatory should be assessed in the light of the cyber security related legislation of the Union, in particular Directive 2016/1148 considering security of network and information systems used by operators of essential services.

(57a) Certificates and self-assessment should help end users to do founded choices. Therefore, certified and self assessed products, processes and services should be accompanied by structure information adapted to the expected technical level of the intended user. All information should be available on line and appropriate information could be available in physical form. In concrete, the end user should be able to know the reference to the certification scheme, the assurance level, the description of the risks, the issuing body or a copy of the certificate. In addition, the end user should be informed of the cybersecurity support policy (i.e. for how long the end user can expect to receive cybersecurity updates or patches) of the manufacturer or provider; where applicable guidance on actions or settings the end user can perform to maintain or increase its cybersecurity, a single point of contact to report and receive support in case of a cyberattacks (in addition to automatic reporting). Information should be regularly updated and available in a website.

(57a) With a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme should cease to be effective from the date established by the Commission by means of the implementing act. Moreover, Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme. However, Member States should not be prevented to adopt or maintain national certification schemes for national security purposes.

Member States should communicate to the Commission and to the European Cybersecurity Group any intent to draw up new national cybersecurity certification schemes. The Commission and the European Cybersecurity Group should evaluate the impacts of the new national cybersecurity certification scheme on the proper functioning of the internal market and in light of the strategic interest to request a European cybersecurity certification scheme instead.

(57c) European cybersecurity schemes will help to harmonise cybersecurity practices within the Union. They must contribute to increase the level of cybersecurity within the Union. The design of European cybersecurity schemes should also take into account and allow for development of new innovations in the field of cybersecurity.

(57d) Cybersecurity certification schemes should take into account current software and hardware development methods and in particular, the impact of frequent software or firmware updates on individual certificates. Certification schemes should specify the conditions under which an update may require that an ICT product or service be recertified or that the scope of the particular certificate be reduced taking into account any possible adverse effect of the update on compliance with the security requirements of the certificate.

(58) Once a European cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services should be able to submit an application for certification of their products or services to a conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by an accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements.

Accreditation bodies should restrict, suspend or revoke an accreditation of a conformity assessment body where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation.

(58a) The certification according to this regulation should be voluntary. In some areas, it could be necessary in the future to make specific cybersecurity requirements and the certification thereof mandatory in certain products, processes or services to improve the level of cyber security in the Union. The Commission should regularly follow the impacts of adopted certification schemes on availability of secure ICT products, processes and services in the internal market and assess the level of utilization of the certification schemes by the manufacturers and service providers in the EU. The efficiency of the certification schemes and whether any particular schemes should be made mandatory should be assessed in the light of existing provisions of Union law related to cyber security, in particular Directive 2016/1148 considering security of network and information systems used by operators of essential services.

(58) References in national legislation to national standards which have ceased to be effective due to the entry into force of a European Certification scheme can be a potential source of confusion for manufacturers and end users. Member States should reflect the adoption of an European Certification scheme in their national legislation.

(59) Member States should designate one or more cybersecurity certification authorities to supervise compliance with obligations arising from this Regulation. If a Member State considers it appropriate, the tasks may be assigned also to already existing authorities. Member States should also be able to decide, upon mutual agreement with another Member State, to designate one or more supervisory authorities in the territory of that other Member State.

The authority should in particular monitor and enforce the obligations of the manufacturer or provider of ICT products and services established in their respective territories relating to the EU statement of conformity, assist the national accreditation bodies in the monitoring and supervision of activities of conformity assessment bodies by providing them with expertise and relevant information, authorise conformity assessment bodies to carry out its tasks when they meet additional requirements set out in a scheme and monitor relevant developments in the field of cybersecurity certification.

National cybersecurity certification authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by them or certificates issued by conformity assessment bodies referring to assurance level high, investigate to the extent appropriate the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable time period. Moreover, they should cooperate with other national cybersecurity certification authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.

The Commission should facilitate that exchange of information by making available a general electronic information support system, for example the Information and Communication System on Market Surveillance (ICSMS) and the rapid alert system for dangerous non-food products (RAPEX) already used by market surveillance authorities pursuant to Regulation (EC) No 765/2008.

(60) With a view to ensuring the consistent application of the European cybersecurity certification framework, a European Cybersecurity Certification Group (the 'Group') consisting of representatives of national cybersecurity certification authorities or other relevant national authorities should be established. The main tasks of the Group should be to advise and assist the Commission in its work to ensure a consistent implementation and application of the European cybersecurity certification framework; to assist and closely cooperate with the Agency in the preparation of candidate cybersecurity certification schemes; recommend that the Commission request the Agency to prepare a candidate European cybersecurity certification scheme; and to adopt opinions addressed to the Agency on candidate schemes and to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

(60a) The Group should facilitate the exchange of good practices and expertise between the national cybersecurity certification authorities responsible for the authorisation of conformity assessment bodies and the issuance of certificates.

(60b) In order to achieve equivalent standards throughout the Union, to facilitate mutual recognition and to promote the overall acceptance of certificates and EU statements of conformity, it is necessary to put in place a system of peer review between national cybersecurity certification authorities. Peer review should cover procedures for supervising the compliance of ICT products, services and processes with certificates, for monitoring the obligations of manufacturers or providers who undertake self-assessment, for monitoring conformity assessment bodies, as well as the appropriateness of the expertise of the personnel of bodies issuing certificates for high assurance levels. The Commission should, by means of implementing act, establish at least a five-year plan for the peer review, as well as laying down criteria and methodologies for the operation of the peer review system.

(60c) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the certification framework, certain certification schemes may include a peer assessment mechanism for the bodies issuing European cybersecurity certificates at the high assurance level under such schemes.

The Group should support the implementation of such peer assessment mechanisms Such peer assessments should in particular assess whether the bodies concerned carry out their tasks in a harmonised way and may include judgement appeal mechanisms. The results of the peer assessments should be made publicly available. These bodies may adopt appropriate measures to adapt their practices and expertise.

(61) In order to raise awareness and facilitate the acceptance of future EU cyber security schemes, the European Commission may issue general or sector-specific cyber security guidelines, e.g. on good cyber security practices or responsible cyber security behaviour highlighting the positive effect of the use of certified ICT products, services and processes.

(61a) In order to further facilitate trade and recognising that ICT supply chains are global, mutual recognition agreements concerning certificates issued by schemes established under the European Cybersecurity Certification Framework, may be concluded by the Union in accordance with Article 218 TFEU. The Commission, taking into account the advice from ENISA and the European Cybersecurity Certification Group, may recommend the initiation of relevant negotiations. Each scheme should provide specific conditions for mutual recognition with third countries.

(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

(65) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT products and services; on modalities of carrying inquiries by the Agency; on a plan for peer review of national cybersecurity certification authorities as well as on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national cybersecurity certification authorities to the Commission.

(66) The Agency's operations should be evaluated regularly and independently. The evaluation should have regard to the Agency achieving its objectives, its working practices and the relevance of its tasks, in particular its tasks relating to operational cooperation at Union level. In case of a review, the Commission should evaluate how its role as reference point for advice and expertise can be reinforced.

(66 a) The evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework. In the case of a review the Commission could evaluate a role for the Agency on supporting the assessment of third country products and services entering the Union that do not comply with Union rules.

(67) Regulation (EU) No 526/2013 should be repealed.

(68) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective,

HAVE ADOPTED THIS REGULATION

TITLE I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. With a view to ensuring the proper functioning of the internal market while aiming at a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation:

(a) lays down the objectives, tasks and organisational aspects of ENISA, the "European Union Agency for Cybersecurity", hereinafter ‘the Agency’; and

(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products, processes and services in the Union as well as avoiding market fragmentation with regard to certification schemes in the Union and which shall apply without prejudice to specific provisions in other Union acts regarding voluntary or mandatory certification.

2. This Regulation shall be without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the state in areas of criminal law.

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) ‘cybersecurity’ means all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;

(2) ‘network and information system’ means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;

(3) ‘national strategy on the security of network and information systems’ means a national strategy on the security of network and information systems as defined in of point (3) of Article 4 of Directive (EU) 2016/1148;

4) ‘operator of essential services’ means an operator of essential services as defined in point (4) of Article 4 of Directive (EU) 2016/1148;

(5) ‘digital service provider’ means a digital service provider as defined in point (6) of Article 4 of Directive (EU) 2016/1148;

(6) ‘incident’ means an incident as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

(7) ‘incident handling’ means incident handling as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

(8) ‘cyber threat’ means any potential circumstance, event or action that may damage, disrupt or otherwise adversely impact network and information systems, their users and affected persons.

(9) ‘European cybersecurity certification scheme’ means the comprehensive set, defined at Union level, of rules, technical requirements, standards and procedures applying to the certification or conformity assessment of Information and Communication Technology (ICT) products, services and processes falling under the scope of that specific scheme;

(9a) ‘national cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority applying to the certification or conformity assessment of ICT products, services and processes falling under the scope of that specific scheme;

(10) ‘European cybersecurity certificate’ means a document issued by the relevant body attesting that a given ICT product, service or process has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;

(11) ‘ICT product means any element or group of elements of network and information systems;

(11a) ‘ICT service’ means any service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

(11b) ‘ICT process’ means any set of activities performed to design, develop, deliver and maintain an ICT product or service;

(12) ‘accreditation’ means accreditation as defined in point (10), Article 2 of Regulation (EC) No 765/2008;

(13) ‘national accreditation body’ means a national accreditation body as defined in point (11), Article 2 of Regulation (EC) No 765/2008;

(14) ‘conformity assessment’ means conformity assessment as defined in point (12), Article 2 of Regulation (EC) No 765/2008;

(15) ‘conformity assessment body’ means conformity assessment body as defined in point (13), Article 2 of Regulation (EC) No 765/2008;

(16) ‘standard’ means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012,

(16a) ‘technical specification’ means a document that prescribes technical requirements to be fulfilled by ICT process, product, service or conformity assessment procedures;

(16b) ‘assurance level’ means a ground for confidence that an ICT process, product or service meets the security requirements of a specific European cybersecurity certification scheme and states at what level it has been evaluated; the assurance level does not measure the security of an ICT process, product or service themselves.

(16c) ‘self-assessment’ means an action carried out by manufacturer or provider of ICT services, products or processes which evaluates the fulfilment of the requirements set in a European cybersecurity certification scheme.

TITLE II

ENISA – the "European Union Agency for Cybersecurity"

CHAPTER I

MANDATE AND OBJECTIVES

Article 3

Mandate

1. The Agency shall undertake the task assigned to it by this Regulation for the purpose of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, agencies and bodies in improving cybersecurity. The Agency shall act as a reference point for advice and expertise on cybersecurity for Union institutions, agencies and bodies as well as other relevant Union stakeholders.

The Agency by carrying out the tasks conferred to it under this Regulation shall contribute to reducing fragmentation in the internal market.

2. The Agency shall carry out tasks conferred upon it by Union acts setting out measures for approximating the laws, regulations and administrative provisions of the Member States which are related to cybersecurity.

2a. When carrying out its tasks, the Agency shall act independently while avoiding duplication with Member States activities and considering already existing Member States expertise.

3. ENISA shall develop its own necessary resources, including technical and human capabilities and skills in order to perform the tasks mandated in this Regulation.

Article 4

Objectives

1. The Agency shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks.

2. The Agency shall assist the Union institutions, agencies and bodies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectorial policies on cybersecurity.

3. The Agency shall support capacity building and preparedness across the Union, by assisting the Union institutions, agencies and bodies, as well as Member States and public and private stakeholders in order to increase the protection of their network and information systems, develop and improve cyber resilience and response capacities, and develop skills and competencies in the field of cybersecurity.

4. The Agency shall promote cooperation including information sharing and coordination at Union level among Member States, Union institutions, agencies and bodies, and relevant private and public stakeholders on matters related to cybersecurity.

5. The Agency shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents.

6. The Agency shall promote the use of European certification, with a view to avoiding fragmentation. The Agency shall contribute to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products, processes and services and thus strengthen trust in the digital internal market and its competiveness.

7. The Agency shall promote a high level of cybersecurity awareness, including cyber hygiene and cyber literacy among of citizens and businesses on issues related to the cybersecurity.

CHAPTER IA

TASKS

Article 5

Development and implementation of Union policy and law

The Agency shall contribute to the development and implementation of Union policy and law, by:

1. assisting and advising, in particular by providing its independent opinion and analysis as well as supplying preparatory work, on the development and review of Union policy and law in the area of cybersecurity, as well as sector-specific policy and law initiatives where matters related to cybersecurity are involved;

2. assisting Member States to implement consistently the Union policy and law regarding cybersecurity notably in relation to Directive (EU) 2016/1148, including by means of opinions, guidelines, advice and best practices on topics such as risk management, incident reporting and information sharing, as well as facilitating the exchange of best practices between competent authorities in this regard.

2a. assisting Member States, Union Institutions, agencies and bodies in developing and promoting cyber security policies related to sustaining the general availability or integrity of the public core of the open internet.

3. contributing to the work of the Cooperation Group pursuant to Article 11 of Directive (EU) 2016/1148, by providing its expertise and assistance;

4. supporting:

(1) the development and implementation of Union policy in the area of electronic identity and trust services, in particular by providing advice and technical guidelines, as well as facilitating the exchange of best practices between competent authorities;

(2) the promotion of an enhanced level of security of electronic communications, including by providing expertise and advice, as well as facilitating the exchange of best practices between competent authorities;

(3) Assisting Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy as well as providing upon request an advice to the European Data Protection Board (EDPB).

5. supporting the regular review of Union policy activities by providing an annual report on the state of implementation of the respective legal framework regarding:

(a) Member States' incident notifications provided by the single point of contacts to the Cooperation Group pursuant to Article 10(3) of Directive (EU) 2016/1148;

(b) notifications of breach of security and loss of integrity regarding the trust service providers, provided by the supervisory bodies to the Agency, pursuant to Article 19(3) of Regulation (EU) 910/2014;

(c) notifications of security incidents transmitted by the undertakings providing public communications networks or publicly available electronic communications services, provided by the competent authorities to Agency, pursuant to Article 40 of [Directive establishing the European Electronic Communications Code].

Article 6

Capacity building

1. The Agency shall assist:

(a) Member States in their efforts to improve the prevention, detection and analysis, and the capacity to respond to, cyber threats and incidents by providing them with the necessary knowledge and expertise;

(aa) Member States and Union institutions, agencies and bodies in establishing and implementing vulnerability disclosure policies on voluntary basis.

(b) Union institutions, agencies and bodies, in their efforts to improve the prevention, detection and analysis of and the capability to respond to cyber threats and incidents in particular through appropriate support for the CERT for the Union institutions, agencies and bodies (CERT-EU);

(c) Member States, at their request, in developing national Computer Security Incident Response Teams (CSIRTs) pursuant to Article 9(5) of Directive (EU) 2016/1148;

(d) Member States, at their request, in developing national strategies on the security of network and information systems, pursuant to Article 7(2) of Directive (EU) 2016/1148; the Agency shall also promote dissemination and note the progress of the implementation of those strategies across the Union in order to promote best practices;

(e) Union institutions in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking progress of their implementation;

(f) national and Union CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CSIRT meets a common set of minimum capabilities and operates according to best practices;

(g) the Member States by organising regular and at least biennial cybersecurity exercises at the Union level referred to in Article 7(6) and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them;

(h) relevant public bodies by offering trainings regarding cybersecurity, where appropriate in cooperation with stakeholders;

(i) the Cooperation Group, in exchanging best practices, in particular with regard to the identification of operators of essential services by Member States, including in relation to cross-border dependencies, regarding risks and incidents, pursuant to Article 11(3)(l) of Directive (EU) 2016/1148.

2. The Agency shall support information sharing in and between sectors support, in particular in the sectors listed in Annex II of Directive (EU) 2016/1148, by providing best practices and guidance on available tools, procedure, as well as on how to address regulatory issues related to information sharing.

Article 7

Operational cooperation at Union level

1. The Agency shall support operational cooperation among Member States, Union institutions, agencies and bodies, and between stakeholders.

2. The Agency shall cooperate at operational level and establish synergies with Union institutions, agencies and bodies, including the CERT-EU, those services dealing with cybercrime and supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern, including:

(a) the exchange of know-how and best practices;

(b) the provision of advice and guidelines on relevant issues related to cybersecurity;

(c) the establishment, upon consultation of the Commission, of practical arrangements for the execution of specific tasks.

3. The Agency shall provide the secretariat of the CSIRTs network, pursuant to Article 12(2) of Directive (EU) 2016/1148 and in this capacity shall actively support the information sharing and the cooperation among its members.

4. The Agency shall support Member States in the operational cooperation within the CSIRTs Network by

(a) advising on how to improve their capabilities to prevent, detect and respond to incidents and, upon request of one or more Member States providing advice in relation to a specific threat;

(b) assisting, upon request of one or more Member States, in the assessment of incidents having a significant or substantial impact through the provision of expertise and facilitating the technical handling of such incidents including in particular by supporting the voluntary sharing of relevant information and technical solutions between Member States;

(c) analysing vulnerabilities and incidents on the basis of publically available information or information provided voluntarily by Member States for this purpose;

(ca) upon request of one or more Member States, providing support to ex-post technical inquiries of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148.

In performing these tasks, the Agency and CERT-EU shall engage in a structured cooperation in order to benefit from synergies and avoid duplication of activities.

6. The Agency shall organise regular cybersecurity exercises at Union level, and support Member States and EU institutions, agencies and bodies in organising exercises following their request(s). Such exercises at Union level may include technical, operational or strategic elements. Once every two years, a large-scale comprehensive exercise shall be organised.

The Agency shall also contribute to and help organise, where appropriate, sectoral cybersecurity exercises together with relevant organisations that may participate also in Union level cybersecurity exercises.

7. The Agency shall, in close cooperation with Member States, prepare a regular and in-depth EU Cybersecurity Technical Situation Report on incidents and threats based on open source information, its own analysis, and reports shared by, among others: Member States' CSIRTs or NIS Directive Single Points of Contact (both on a voluntary basis); European Cybercrime Centre (EC3) at Europol, CERT-EU.

8. The Agency shall contribute to develop a cooperative response, at Union and Member States level, to large-scale cross-border incidents or crises related to cybersecurity, mainly by:

(a) aggregating and analysing reports from national sources that are in the public domain or shared on a voluntary basis with a view to contribute to establishing common situational awareness;

(b) ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs Network and the technical and political decision-makers at Union level;

(c) facilitating, upon request the technical handling of an incident or crises, including in particular, by supporting the voluntary sharing of technical solutions between Member States;

(d) supporting EU institutions, agencies and bodies and, upon request, Member States in the public communication around the incident or crisis;

(e) testing the cooperation plans to respond to such incidents or crises at Union level and upon request supporting Member States in testing such plans at national level.

Article 8

Market, cybersecurity certification, and standardisation

The Agency shall:

(a) support and promote the development and implementation of the Union policy on cybersecurity certification of ICT products, services, and processes as established in Title III of this Regulation, by:

(-1) on an ongoing basis monitor developments in related areas of standardisation and recommend appropriate technical specifications for the use of the development of European cybersecurity certification schemes as referred in Article 47(1)(b) in cases where standards are not available;

(1) preparing candidate European cybersecurity certification schemes for ICT products and services and processes in accordance with Article 44 of this Regulation;

1a. evaluating adopted European cybersecurity schemes in accordance with Article 44(5).

1ab. participating in peer reviews pursuant to Article 50a(4);

(2) assisting the Commission in providing the secretariat to the European Cybersecurity Certification Group pursuant to Article 53 of this Regulation;

(2a) providing the secretariat to the Stakeholder Cybersecurity Certification Group pursuant to Article 20a of this Regulation;

(3) compiling and publishing guidelines and developing good practices, concerning the cybersecurity requirements of ICT products, processes and services, in cooperation with national cybersecurity certification authorities and the industry in a formal, structured and transparent way;

(3a) contributing to a sufficient capacity building related to evaluation and certification processes by compiling and issuing guidelines as well as by providing support to Member States at their request;

(b) facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT processes, products and services;

(ba) draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148;

(c) perform and disseminate regular analyses of the main trends in the cybersecurity market both on the demand and supply side, with a view of fostering the cybersecurity market in the Union.

Article 9

Knowledge and information

The Agency shall:

(a) perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on cybersecurity;

(b) perform long-term strategic analyses of cybersecurity threats and incidents in order to identify emerging trends and help prevent cybersecurity incidents;

(c) provide, in cooperation with experts from Member States authorities and relevant stakeholders, advice, guidance and best practices for the security of network and information systems, in particular for the security of the infrastructures supporting the sectors listed in Annex II of Directive (EU) 2016/1148 and those used by the digital service providers listed in Annex III of that Directive;

(d) pool, organise and make available to the public, through a dedicated portal, information on cybersecurity, provided by the Union institutions, agencies and bodies and, on a voluntary basis, by Member States and private and public stakeholders;

(f) collect and analyse publicly available information regarding significant incidents and compiling reports with a view to providing guidance to businesses and citizens across the Union;

Article 9a

Awareness raising and education

The Agency shall:

(a) raise awareness of the public about cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens and organisations, including cyber hygiene and cyber literacy;

(b) organise, in cooperation with the Member States, Union institutions, bodies, agencies and industry, regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate;

(c) assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education;

(d) support closer coordination and exchange of best practices among Member States on cybersecurity education and awareness.

Article 10

Research and innovation

In relation to research and innovation, the Agency shall:

(a) advise the Union and the Member States on research needs and priorities in the area of cybersecurity, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;

(b) participate, where the Commission has delegated the relevant powers to it, in the implementation phase of research and innovation funding programmes or as a beneficiary.

(ba) contribute in the area of cybersecurity to the strategic research and innovation agenda at Union level.

Article 11

International cooperation

The Agency shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity, by:

(a) engaging, where appropriate, as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

b) facilitating, upon the request of the Commission, the exchange of best practices;

(c) providing, upon request, the Commission with expertise;

(ca) providing advice and support to the Commission on matters concerning agreements for mutual recognition of cybersecurity certificates with third countries in collaboration with the Member States Certification Group established under Article 53.

CHAPTER II

ORGANISATION OF THE AGENCY

Article 12

Structure

The administrative and management structure of the Agency shall be composed of the following:

(a) a Management Board which shall exercise the functions set out in Article 14;

(b) an Executive Board which shall exercise the functions set out in Article 18;

(c) an Executive Director who shall exercise the responsibilities set out in Article 19;

(d) an ENISA Advisory Group which shall exercise the functions set out in Article 20.

(da) a National Liaison Officers Network which shall exercise the functions set out in Article 20a.

SECTION 1

MANAGEMENT BOARD

Article 13

Composition of the Management Board

1. The Management Board shall be composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives shall have voting rights.

2. Each member of the Management Board shall have an alternate member to represent the member in their absence.

3. Members of the Management Board and their alternates shall be appointed in light of their knowledge in the field of cybersecurity, taking into account relevant managerial, administrative and budgetary skills. The Commission and Member States shall make efforts to limit the turnover of their representatives in the Management Board, in order to ensure continuity of that Board's work. The Commission and Member States shall aim to achieve a balanced representation between men and women on the Management Board.

4. The term of office of members of the Management Board and of their alternates shall be four years. That term shall be renewable.

Article 14

Functions of the Management Board

1. The Management Board shall:

(a) define the general direction of the operation of the Agency and shall also ensure that the Agency works in accordance with the rules and principles laid down in this Regulation. It shall also ensure consistency of the Agency's work with activities conducted by the Member States as well as at Union level;

(b) adopt the Agency's draft single programming document referred to in Article 21, before its submission to the Commission for its opinion;

(c) adopt, taking into account the Commission opinion, the Agency's single programming document by a majority of two-thirds of members and in accordance with Article 17;

(ca) supervise the implementation of the multiannual and annual programming included in the single programming document;

(d) adopt, by a majority of two-thirds of members, the annual budget of the Agency and exercise other functions in respect of the Agency's budget pursuant to Chapter III;

(e) assess and adopt the consolidated annual report on the Agency's activities and send both the report and its assessment by 1 July of the following year, to the European Parliament, the Council, the Commission and the Court of Auditors. The annual report shall include the accounts and describe how the Agency has met its performance indicators. The annual report shall be made public;

(f) adopt the financial rules applicable to the Agency in accordance with Article 29;

(g) adopt an anti-fraud strategy that is proportionate to the fraud risks having regard to a cost-benefit analysis of the measures to be implemented;

(h) adopt rules for the prevention and management of conflicts of interest in respect of its members;

(i) ensure adequate follow-up to the findings and recommendations resulting from investigations of the European Anti-fraud Office (OLAF) and the various internal or external audit reports and evaluations;

(j) adopt its rules of procedure incl. the delegation of specific tasks subject to Article 18(7);

(k) in accordance with paragraph 2, exercise, with respect to the staff of the Agency, the powers conferred by the Staff Regulations of Officials on the Appointing Authority and the Conditions of Employment of Other Servants of the European Union on the Authority Empowered to Conclude a Contract of Employment ("the appointing authority powers");

(l) adopt rules implementing the Staff Regulations and the Conditions of Employment of Other Servants in accordance with the procedure provided for in Article 110 of the Staff Regulations;

(m) appoint the Executive Director and where relevant extend his term of office or remove him from office in accordance with Article 33 of this Regulation;

(n) appoint an Accounting Officer, who may be the Commission's Accounting Officer, who shall be totally independent in the performance of his/her duties;

(o) take all decisions on the establishment of the Agency's internal structures and, where necessary, their modification, taking into consideration the Agency's activity needs and having regard to sound budgetary management;

(p) authorise the conclusion of working arrangements in accordance with Articles 7 and 39.

2. The Management Board shall adopt, in accordance with Article 110 of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment of Other Servants, delegating relevant appointing authority powers to the Executive Director and defining the conditions under which this delegation of powers can be suspended. The Executive Director shall be authorised to sub-delegate those powers.

3. Where exceptional circumstances so require, the Management Board may by way of a decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and those sub-delegated by the latter and exercise them itself or delegate them to one of its members or to a staff member other than the Executive Director.

Article 15

Chairperson of the Management Board

The Management Board shall elect by a majority of two-thirds of members its Chairperson and a Deputy Chairperson from among its members for a period of four years, which shall be renewable once. If, however, their membership of the Management Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall ex officio replace the Chairperson if the latter is unable to attend to his or her duties.

Article 16

Meetings of the Management Board

1. Meetings of the Management Board shall be convened by its Chairperson.

2. The Management Board shall hold at least two ordinary meetings a year. It shall also hold extraordinary meetings at the request of the Chairperson, at the request of the Commission, or at the request of at least a third of its members.

3. The Executive Director shall take part, without voting rights, in the meetings of the Management Board

4. Members of the ENISA Advisory Group may take part, upon invitation from the Chairperson, in the meetings of the Management Board, without voting rights

5. The members of the Management Board and their alternates may, subject to its Rules of Procedure, be assisted at the meetings by advisers or experts.

6. The Agency shall provide the secretariat for the Management Board.

Article 17

Voting rules of the Management Board

1. The Management Board shall take its decisions by majority of its members.

2. A two-thirds majority of all Management Board members shall be required for the single programming document, the annual budget, the appointment, extension of the term of office or removal of the Executive Director.

3. Each member shall have one vote. In the absence of a member, their alternate shall be entitled to exercise the right to vote.

4. The Chairperson shall take part in the voting.

5. The Executive Director shall not take part in the voting.

6. The Management Board's rules of procedures shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.

SECTION 2

EXECUTIVE BOARD

Article 18

Executive Board

1. The Management Board shall be assisted by an Executive Board.

2. The Executive Board shall:

(a) prepare decisions to be adopted by the Management Board;

(b) ensure, together with the Management Board, the adequate follow-up to the findings and recommendations stemming from investigations of OLAF and the various internal or external audit reports and evaluations;

(c) without prejudice to the responsibilities of the Executive Director, as set out in Article 19, assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters pursuant to Article 19.

3. The Executive Board shall be composed of five members appointed from among the members of the Management Board amongst whom the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission. The Executive Director shall take part in the meetings of the Executive Board, but shall not have the right to vote. The appointments shall aim to achieve a balanced representation of genders on the Executive Board.

4. The term of office of the members of the Executive Board shall be four years. That term shall be renewable.

5. The Executive Board shall meet at least once every three months. The chairperson of the Executive Board shall convene additional meetings at the request of its members.

6. The Management Board shall lay down the rules of procedure of the Executive Board.

7. When necessary, because of urgency, the Executive Board may take certain provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters. The Executive Board shall not take such decision that must be passed by a two third majority of the Management Board. Such provisional decision shall be notified to the Management Board without undue delay and be approved by the latter no later than 3 months after the decision has been taken".

SECTION 3

EXECUTIVE DIRECTOR

Article 19

Responsibilities of the Executive Director

1. The Agency shall be managed by its Executive Director, who shall be independent in the performance of his or her duties. The Executive Director shall be accountable to the Management Board.

2. The Executive Director shall report to the European Parliament on the performance of his or her duties when invited to do so. The Council may invite the Executive Director to report on the performance of his or her duties.

3. The Executive Director shall be responsible for:

(a) the day-to-day administration of the Agency;

(b) implementing the decisions adopted by the Management Board;

(c) preparing the draft single programming document and submitting it to the Management Board for approval before its submission to the Commission;

(d) implementing the single programming document and reporting to the Management Board thereon;

(e) preparing the consolidated annual report on the Agency's activities including the implementation of the annual work programme and presenting it to the Management Board for assessment and adoption;

(f) preparing an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission;

(g) preparing an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Ant-fraud Office (OLAF) and reporting on progress twice a year to the Commission and regularly to the Management Board;

(h) preparing draft financial rules applicable to the Agency

(i) preparing the Agency's draft statement of estimates of revenue and expenditure and implementing its budget;

(j) protecting the financial interests of the Union by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative and financial penalties;

(k) preparing an anti-fraud strategy for the Agency and presenting it to the Management Board for approval;

(l) developing and maintaining contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;

(la) exchanging regularly with Union institutions, agencies and bodies regarding their activities on cybersecurity to ensure coherence in the development and the implementation of EU policy;

(m) other tasks assigned to the Executive Director by this Regulation.

4. Where necessary and within the Agency's mandate, and in accordance with the Agency's objectives and tasks, the Executive Director may set up ad hoc Working Groups composed of experts, including from the Member States' competent authorities. The Management Board shall be informed in advance. The procedures regarding in particular the composition of the Working Groups, the appointment of the experts of the Working Groups by the Executive Director and the operation of the Working Groups shall be specified in the Agency's internal rules of operation.

5. Where necessary, for the purpose of carrying out the Agency's tasks in an efficient and effective manner and based on an appropriate cost-benefit analysis, the Executive Director may decide to establish one or more local offices in one or more Member States. Before deciding to establish a local office the Executive Director shall seek the opinion of the Member State(s) concerned, including the Member State where the seat of the Agency is located, and obtain the prior consent of the Commission and the Management Board. In cases of disagreement during the consultation process between the Executive Director and the Member States concerned, the issue shall be brought to the Council for discussion. The number of the staff in all local offices shall be kept to a minimum and shall not exceed in total 40 % of the total number of the Agency's staff located in the Member State where the seat of the Agency is located. The number of the staff in each local office shall not exceed 10 % of the total number of the Agency's staff located in the Member State where the seat of the Agency is located.

The decision shall specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and duplication of administrative functions of the Agency.

SECTION 4

ENISA ADVISORY GROUP

Article 20

ENISA Advisory Group

1. The Management Board, acting on a proposal by the Executive Director, shall set up in a transparent manner a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, academic experts in the cybersecurity, and representatives of competent authorities notified under Directive 2016/0288, European Standards Organisations (ESOs), as well as of law enforcement and data protection supervisory authorities.

The Management Board shall strive to ensure an appropriate gender and geographical balance as well as balance between the different stakeholder groups.

2. Procedures for the ENISA Advisory Group, in particular regarding the number, composition, and the appointment of its members by the Management Board, the proposal by the Executive Director and the operation of the Group, shall be specified in the Agency's internal rules of operation and shall be made public.

The ENISA Advisory Group shall be chaired by the Executive Director or by any person the Executive Director appoints on a case-by-case basis

4. The term of office of the ENISA Advisory Group's members shall be two-and-a-half years. Members of the Management Board may not be members of the ENISA Advisory Group. Experts from the Commission and the Member States shall be entitled to be present at the meetings of the ENISA Advisory Group and to participate in its work. Representatives of other bodies deemed relevant by the Executive Director, who are not members of the ENISA Advisory Group, may be invited to attend the meetings of the ENISA Advisory Group and to participate in its work.

5. The ENISA Advisory Group shall advise the Agency in respect of the performance of its activities, except of the application of the title III of this Regulation. It shall in particular advise the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on issues related to the work programme.

5a. The Permanent Stakeholders' Group shall on a regular basis inform the Management Board of its activities.

Article 20a

Stakeholder Cybersecurity Certification Group

1. The Stakeholder Cybersecurity Certification Group shall be established.

2. The Group shall be composed of members selected among recognised experts representing relevant stakeholders. The European Commission shall select those members upon a proposal from ENISA through an transparent and open call ensuring balance between the different stakeholder groups as well as appropriate gender and geographical balance.

3. The Stakeholder Certification Group shall have the following tasks:

a) to advise the Commission on strategic issues regarding the European Cybersecurity Certification Framework;

(b) upon request, to advise the Agency on general and strategic matters concerning the Agency's tasks on market, cybersecurity certification, and standardisation;

(c) to assist the Commission in the preparation of the Union rolling work programme;

(d) to issue an opinion on the Union rolling work programme pursuant to Article 43a(4); and

(e) in urgent cases, to give advice to the Commission and the ECCG on the need to for additional certification schemes not included in the work programme, as outlined in Art 43 a and b;

4. The Group shall be co-chaired by the Commission and the Agency, and the secretariat shall be provided by the Agency.

Recital: The Cybersecurity Certification Stakeholder Group should be established in order to help the Agency and the Commission facilitating consultation with relevant stakeholders. The Group should be composed of members representing in balanced proportion industry, both on the demand as well as the supply side of ICT products and services and including in particular small and medium-sized enterprises, digital service providers, European and international standardisation bodies, accreditation bodies, data protection supervisory authorities and conformity assessment bodies pursuant to Regulation (EC) 765/2008, academia as well as consumer organisations.

SECTION 4A

NATIONAL LIAISON OFFICERS NETWORK

Article 20a

National Liaison Officers Network

1. The Management Board, acting on a proposal by the Executive Director, shall set up a National Liaison Officers Network composed of representatives of the Member States.

2. The National Liaison Officers Network shall compose of the representatives of all Member States. Each Member State shall appoint one representative. The meetings of the network may be held in different expert formats.

3. The National Liaison Officers Network shall in particular facilitate the exchange of information between ENISA and the Member States and support ENISA in disseminating its activities, findings and recommendations across the EU, to the relevant stakeholders.

4. National Liaison Officers shall act as a focal point of contact on a national level to facilitate cooperation between ENISA and national experts in the context of ENISA work programme implementation.

5. While National Liaison Officers shall closely cooperate with the Management Board Representatives of their respective countries, the Network itself shall not duplicate the work neither of the Management Board nor other EU fora.

6. Functions and procedures for the National Liaisons Officers Network, shall be specified in the Agency's internal rules of operation and shall be made public.

SECTION 5

OPERATION

Article 21

Single Programming Document

1. The Agency shall carry out its operations in accordance with a single programming document containing its multiannual and annual programming, which shall include all of its planned activities.

2. Each year, the Executive Director shall draw up a draft single programming document containing multiannual and annual programming with the corresponding human and financial resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) No 1271/2013 and taking into account guidelines set by the Commission.

3. By 30 November each year, the Management Board shall adopt the single programming document referred to in paragraph 1 and forward it to the European Parliament, the Council and the Commission no later than 31 January of the following year, as well as any later updated version of that document.

4. The single programming document shall become definitive after final adoption of the general budget of the Union and, if necessary, shall be adjusted accordingly.

5. The annual work programme shall comprise detailed objectives and expected results including performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be coherent with the multi-annual work programme referred to in paragraph 7. It shall clearly indicate tasks that have been added, changed or deleted in comparison with the previous financial year.

6. The Management Board shall amend the adopted annual work programme when a new task is given to the Agency. Any substantial amendment to the annual work programme shall be adopted by the same procedure as the initial annual work programme. The Management Board may delegate the power to make non-substantial amendments to the annual work programme to the Executive Director.

7. The multi-annual work programme shall set out overall strategic programming including objectives, expected results and performance indicators. It shall also set out resource programming including multi-annual budget and staff.

8. The resource programming shall be updated annually. The strategic programming shall be updated wherever appropriate and in particular where necessary to address the outcome of the evaluation referred to in Article 56.

Article 22

Declaration of interest

1. Members of the Management Board, the Executive Director and officials seconded by Member States on a temporary basis shall each make a declaration of commitments and a declaration indicating the absence or presence of any direct or indirect interest which might be considered prejudicial to their independence. The declarations shall be accurate and complete, made annually in writing and updated whenever necessary.

2. Members of the Management Board, the Executive Director, and external experts participating in ad hoc Working Groups shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting upon such points.

3. The Agency shall lay down, in its internal rules of operation, the practical arrangements for the rules on declarations of interest referred to in paragraphs 1 and 2.

Article 23

Transparency

1. The Agency shall carry out its activities with a high level of transparency and in accordance with Article 25.

2. The Agency shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 22.

3. The Management Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of the Agency's activities.

4. The Agency shall lay down, in its internal rules of operation, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.

Article 24

Confidentiality

1. Without prejudice to Article 25, the Agency shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.

2. Members of the Management Board, the Executive Director, the members of the ENISA Advisory Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union (TFEU), even after their duties have ceased.

3. The Agency shall lay down, in its internal rules of operation, the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.

4. If required for the performance of the Agency's tasks, the Management Board shall decide to allow the Agency to handle classified information. In that case the Management Board shall, in agreement with the Commission services, adopt internal rules of operation applying the security principles set out in Commission Decisions (EU, Euratom) 2015/443 and 2015/444 . Those rules shall include provisions for the exchange, processing and storage of classified information.

Article 25

Access to documents

1. Regulation (EC) No 1049/2001 shall apply to documents held by the Agency.

2. The Management Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the Agency.

3. Decisions taken by the Agency pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the Ombudsman under Article 228 TFEU or of an action before the Court of Justice of the European Union under Article 263 TFEU.

CHAPTER III

ESTABLISHMENT AND STRUCTURE OF THE BUDGET

Article 26

Establishment of the budget

1. Each year, the Executive Director shall draw up a draft statement of estimates of the Agency's revenue and expenditure for the following financial year, and shall forward it to the Management Board, together with a draft establishment plan. Revenue and expenditure shall be in balance.

2. Each year, the Management Board shall, on the basis of the draft statement of estimates of revenue and expenditure referred to in paragraph 1, produce a statement of estimates of revenue and expenditure for the Agency for the following financial year.

3. The Management Board shall, by 31 January each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document, to the Commission and the third countries with which the Union has concluded agreements in accordance with Article 39.

4. On the basis of that statement of estimates, the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Article 313 and 314 TFEU.

5. The European Parliament and the Council shall authorise the appropriations for the contribution to the Agency.

6. The European Parliament and the Council shall adopt the establishment plan for the Agency.

7. Together with the single programming document, the Management Board shall adopt the Agency's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Management Board shall adjust the Agency's budget and single programming document in accordance with the general budget of the Union.

Article 27

Structure of the budget

1. Without prejudice to other resources, the Agency's revenue shall be composed of:

(a) a contribution from the Union budget;

(b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 29;

(c) Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in Article 29 and with the provisions of the relevant instruments supporting the policies of the Union;

(d) contributions from third countries participating in the work of the Agency as provided for in Article 39;

(e) any voluntary contributions from Member States in money or in kind; Member States that provide voluntary contributions may not claim any specific right or service as a result thereof.

2. The expenditure of the Agency shall include staff, administrative and technical support, infrastructure and operational expenses, and expenses resulting from contracts entered into with third parties.

Article 28

Implementation of the budget

1. The Executive Director shall be responsible for the implementation of the Agency’s budget.

2. The Commission’s internal auditor shall exercise the same powers over the Agency as over Commission departments.

3. By 1 March following each financial year (1 March of year N + 1), the Agency’s accounting officer shall send the provisional accounts to the Commission’s accounting officer and to the Court of Auditors.

4. Upon receipts of the Court of Auditors' observations on the Agency's provisional accounts, the Agency's accounting officer shall draw up the Agency's final accounts under his or her responsibility.

5. The Executive Director shall submit the final accounts to the Management Board for an opinion.

6. The Executive Director shall send, by 31 March of year N + 1, the report on the budgetary and financial management to the European Parliament, the Council, the Commission and the Court of Auditors.

7. The accounting officer shall, by 1 July of year N + 1, transmit the final accounts to the European Parliament, the Council, the accounting officer of the Commission and the Court of Auditors, together with the Management Board's opinion.

8. At the same date as the transmission of his or her final accounts, the accounting officer shall also send to the Court of Auditors a representation letter covering those final accounts, with a copy to the accounting officer of the Commission.

9. The Executive Director shall publish the final accounts by 15 November of the following year.

10. The Executive Director shall send the Court of Auditors a reply to its observations by 30 September of year N + 1 and shall also send a copy of that reply to the Management Board and to the Commission.

11. The Executive Director shall submit to the European Parliament, at the latter’s request, all the information necessary for the smooth application of the discharge procedure for the financial year in question, as laid down in Article 165(3) of the Financial Regulation.

12. The European Parliament, acting on a recommendation from the Council, shall, before 15 May of year N + 2, give a discharge to the Executive Director in respect of the implementation of the budget for the year N.

Article 29

Financial Rules

The financial rules applicable to the Agency shall be adopted by the Management Board after consulting the Commission. They shall not depart from Regulation (EU) 1271/2013 unless such a departure is specifically required for the Agency's operation and the Commission has given its prior consent.

Article 30

Combating fraud

1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EC) 883/2013 of the European Parliament and of the Council , the Agency shall, within six months from the day it becomes operational, accede to the Interinstitutional Agreement of 25 May, 1999 concerning internal investigations by the European Anti-fraud Office (OLAF) and shall adopt the appropriate provisions applicable to all the employees of the Agency, using the template set out in the Annex to that Agreement.

2. The Court of Auditors shall have the power of audit, on the basis of documents and on-the-spot checks and inspections, over all grant beneficiaries, contractors and subcontractors who have received Union funds from the Agency.

3. OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Regulation 883/2013 of the European Parliament and of the Council and Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the Union' financial interests against fraud and other irregularities with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by the Agency.

4. Without prejudice to paragraphs 1, 2 and 3, cooperation agreements with third countries and international organisations, contracts, grant agreements and grant decisions of the Agency shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct such audits and investigations, according to their respective competences.

CHAPTER IV

AGENCY STAFF

Article 31

General provisions

The Staff Regulations and the Conditions of Employment of Other Servants and the rules adopted by agreement between the Union institutions for giving effect to those Staff Regulations shall apply to the staff of the Agency.

Article 32

Privileges and immunity

Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the TFEU shall apply to the Agency and its staff.

Article 33

Executive Director

1. The Executive Director shall be engaged as a temporary agent of the Agency under Article 2(a) of the Conditions of Employment of Other Servants.

2. The Executive Director shall be appointed by the Management Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.

3. For the purpose of concluding the contract of the Executive Director, the Agency shall be represented by the Chairperson of the Management Board.

4. Before appointment, the candidate selected by the Management Board shall be invited to make a statement before the relevant committee of the European Parliament and to answer Members' questions.

5. The term of office of the Executive Director shall be five years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Agency's future tasks and challenges.

6. The Management Board shall reach decisions on appointment, extension of the term of office or removal from office of the Executive Director on the basis of a two-thirds majority of its members with voting rights.

7. The Management Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for five years.

8. The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office. Within three months before any such extension, the Executive Director shall, if invited, make a statement before the relevant committee of the European Parliament and answer Members' questions.

9. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.

10. The Executive Director may be removed from office only by decision of the Management Board acting on a proposal from the Commission.

Article 34

Seconded national experts and other staff

1. The Agency may make use of seconded national experts or other staff not employed by the Agency. The Staff Regulations and the Conditions of Employment of Other Servants shall not apply to such staff.

2. The Management Board shall adopt a decision laying down rules on the secondment to the agency of national experts.

CHAPTER V

GENERAL PROVISIONS

Article 35

Legal status of the Agency

1. The Agency shall be a body of the Union and shall have legal personality.

2. In each Member State, the Agency shall enjoy the most extensive legal capacity accorded to legal persons under national law. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings, or both.

3. The Agency shall be represented by its Executive Director.

Article 36

Liability of the Agency

1. The contractual liability of the Agency shall be governed by the law applicable to the contract in question.

2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the Agency.

3. In the case of non-contractual liability, the Agency shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by it or its servants in the performance of their duties.

4. The Court of Justice of the European Union shall have jurisdiction in any dispute relating to compensation for such damage.

5. The personal liability of its servants towards the Agency shall be governed by the relevant conditions applying to the staff of the Agency.

Article 37

Language arrangements

1. Council Regulation No 1 shall apply to the Agency. The Member States and the other bodies appointed by them may address the Agency and receive a reply in the official language of the institutions of the Union of their choice.

2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union.

Article 38

Protection of personal data

1. The processing of personal data by the Agency shall be subject to Regulation (EU) No xz/2018 of the European Parliament and of the Council.

2. The Management Board shall adopt implementing measures referred to in Article 45(3) of Regulation (EU) 2018/1725. The Management Board may adopt additional measures necessary for the application of Regulation (EU) No xz/2018 by the Agency.

Article 39

Cooperation with third countries and international organisations

1. In so far as is necessary in order to achieve the objectives set out in this Regulation, the Agency may cooperate with the competent authorities of third countries or with international organisations or both. To this end, the Agency may, subject to prior approval by the Commission, establish working arrangements with the authorities of third countries and international organisations. These arrangements shall not create legal obligations incumbent on the Union and its Member States.

2. The Agency shall be open to the participation of third countries that have entered into agreements with the Union to this effect. Under the relevant provisions of these agreements, arrangements shall be made specifying in particular the nature, extent and manner in which those countries will participate in the Agency's work, including provisions relating to participation in the initiatives undertaken by the Agency, financial contributions and staff. As regards staff matters, those arrangements shall, in any event, comply with the Staff Regulations.

3. The Management Board shall adopt a strategy for relations with third countries or international organisations concerning matters for which the Agency is competent. The Commission shall ensure that the agency operates within its mandate and the existing institutional framework by concluding an appropriate working arrangement with the agency's Executive Director.

Article 40

Security rules on the protection of classified and sensitive non-classified information

In consultation with the Commission, the Agency shall adopt its security rules applying the security principles contained in the Commission's security rules for protecting European Union Classified Information (EUCI) and sensitive non-classified information, as set out in Commission Decisions (EU, Euratom) 2015/443 and 2015/444. This shall cover, inter alia, provisions for the exchange, processing and storage of such information.

Article 41

Headquarters Agreement and operating conditions

1. The necessary arrangements concerning the accommodation to be provided for the Agency in the host Member State and the facilities to be made available by that Member State together with the specific rules applicable in the host Member State to the Executive Director, members of the Management Board, Agency staff and members of their families shall be laid down in a Headquarters Agreement between the Agency and Member State where the seat is located, concluded after obtaining the approval of the Management Board.

2. The Agency's host Member State shall provide the best possible conditions to ensure the proper functioning of the Agency, including the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses.

Article 42

Administrative control

The operations of the Agency shall be supervised by the Ombudsman in accordance with Article 228 TFEU.

TITLE III

CYBERSECURITY CERTIFICATION FRAMEWORK

Article 43

European cybersecurity certification framework

1. The European cybersecurity certification framework is established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at EU level of European cybersecurity certification schemes, in view of creating a digital single market for ICT products, services and processes.

2. The European cybersecurity certification framework defines a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, processes and services that have been evaluated in accordance with such schemes comply with specified security requirements with the aim to protect the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, and services throughout their life cycle.

Article 43a

The Union rolling work programme for European Cybersecurity Certification

1. The Commission shall publish a Union rolling work programme for European Cybersecurity Certification (hereinafter 'the programme') that shall identify strategic priorities for future European Cybersecurity Certification schemes.

2. The programme shall in particular include a list of ICT products, services and processes or categories thereof that may benefit from being included in the scope of a European Cybersecurity Certification Scheme.

3. Inclusion of any particular ICT products, services and processes or categories in the Programme shall be justified on one of the following grounds:

(a) the availability and the development of national certification schemes covering any particular category of ICT products, services or processes and in particular as regards the risk of fragmentation

(b) relevant Union and / or national policy or legislation;

(c) market demand

d) developments in cyber threat landscape

e) request for preparation of specific candidate scheme proposed by the ECCG referred to in Article 53.

4. The Commission shall take in due account the opinions issued by the European Cybersecurity Certification Group referred to in Article 53 and the Stakeholder Certification Group referred to in Article 20a on the draft Programme.

5. The first programme shall be published no later than twelve months after entry into force of this Regulation. The Programme shall be updated as necessary and at least every three years.

Article 43b

Request for a European cybersecurity certification scheme

1. The Commission may request the Agency to prepare a candidate European cybersecurity certification scheme or review an existing scheme on the basis of the Programme.

2. In duly justified cases, the Commission or the ECCG referred to in Article 53 may request the Agency to prepare a candidate European cybersecurity scheme or review an existing scheme which is not included in the Union rolling work programme referred to in Article 43a. The Programme will be updated accordingly.

Article 44

Preparation, adoption and review of a European cybersecurity certification schemes

1. Following a request from the Commission pursuant to Article 43b, the Agency shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation.

1a. Following a request from the European Cybersecurity Certification Group pursuant to Article 43b.2, ENISA may prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. If the agency refuses such request, it shall give a justification. Any refusal decision shall be taken by the management board.

2. When preparing candidate schemes referred to in paragraph 1 of this Article, the Agency shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation processes.

2a. For each candidate scheme, the Agency shall establish an ad hoc working group in accordance with Article 19(4) of this Regulation with the purpose of providing the Agency with specific advice and expertise.

2b. The Agency shall closely cooperate with the ECCG referred to in Article 53. The Group shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme and shall adopt an opinion on the candidate scheme prepared by ENISA.

3. ENISA shall take utmost account of the opinion of the Group before transmitting the candidate scheme prepared in accordance with paragraph 2 and 2b of this Article to the Commission. The opinion is not binding nor is the absence thereof blocking ENISA to transmit the candidate scheme.

4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(2), providing for European cybersecurity certification schemes for ICT processes, products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.

5. The Agency shall at least every 5 years evaluate the adopted European cybersecurity certification schemes taking into account feedback received from interested parties. If considered necessary, the Commission or European Cybersecurity Certification Group may request the Agency to start the process of developing a revised candidate scheme in accordance with Article 43b and 44.

Article 44a

Website on European cybersecurity certification schemes

1. The Agency shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes, certificates and EU statements of conformity including with regard to withdrawn and expired cybersecurity certification schemes and certificates and the repository of links to cybersecurity information provided online by manufacturers and providers in accordance to Article 47a.

2. Where applicable, the website shall also indicate the national certifications schemes that have been replaced by a European cybersecurity certification scheme.

Article 45

Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme shall be so designed as to achieve, as applicable, at least the following security objectives:

(a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure during the entire process, product or service lifecycle;

(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire process, product or service lifecycle;

(c) authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;

(ca) identify and document known dependencies and vulnerabilities;

(d) record which data, functions or services have been accessed, used or otherwise processed, at what times and by whom;

(da) verify that ICT products, processes and services do not contain known vulnerabilities;

(e) it is possible to check which data, services or functions have been accessed, or used or otherwise processed, at what times and by whom;

(f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;

(fa) that ICT products, services and processes are secure by default and by design;

(g) ICT processes, products and services are provided with up to date software and hardware that do not contain publicly known vulnerabilities, and are provided mechanisms for secure updates.

Article 46

Assurance levels of European cybersecurity certification schemes

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels: basic, substantial and/or high, for ICT products, services and processes. The level of assurance shall be commensurate with the level of the risk, in terms of the probability and impact of an incident, associated with the intended use of an ICT process, product or service

2. The assurance levels basic, substantial and high shall refer to a certificate or an EU statement of conformity issued in the context of a European cybersecurity certification scheme, which provides for each assurance level respective security requirements including security functionalities and the corresponding degree of effort for the evaluation of an ICT process, product or service. The certificate or the EU statement of conformity is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents as follows:

(a) a European cybersecurity certificate or EU statement of conformity that refers to assurance level “basic” provides assurance that the ICT products, services and processes meet the respective security requirements including security functionalities and they have been evaluated to a level which aims to minimise the known basic risks for cyber incidents and cyber attacks. The evaluation activities shall include at least a review of a technical documentation, or where not applicable they shall include substitute activities with equivalent effect.

(b) a European cybersecurity certificate that refers to assurance level “substantial” provides assurance that the ICT products, services and processes meet the respective security requirements including security functionalities and they have been evaluated to a level which aims to minimise known cyber risks, cyber incidents and cyber attacks carried out by actors with limited skills and resources. The evaluation activities shall include at least: reviewing the non-applicability of publicly known vulnerabilities and testing that the ICT products, processes or services correctly implement the necessary security functionality; or where not applicable they shall include substitute activities with equivalent effect.

(c) a European cybersecurity certificate that refers to assurance level “high” provides assurance that the ICT products, services and processes meet the respective security requirements including security functionalities and they have been evaluated to a level which aims to minimise the risk of state-of-the-art cyber attacks carried out by actors with significant skills and resources. The evaluation activities shall include at least: reviewing the non-applicability of publicly known vulnerabilities, testing that the ICT products, processes or services correctly implement the necessary security functionality, at the state-of-the-art, and assessing their resistance to skilled attackers via penetration testing; or where not applicable they shall include substitute activities

2a. A European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation methodology. Each one of the evaluation levels shall correspond to one of the assurance levels and be defined by an appropriate combination of assurance components.

Article 46a

Conformity self-assessment

1. A European cybersecurity certification scheme may allow for carrying out a conformity assessment under the sole responsibility of the manufacturer or provider of ICT products and services. Such conformity assessment shall be applicable only to ICT products and services of low risk corresponding to assurance level basic.

2. The manufacturer or provider of ICT products and services may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By drawing up such a statement, the manufacturer or provider of ICT products and services shall assume responsibility for the compliance of the ICT product or service with the requirements set out in the scheme.

3. The manufacturer or provider of ICT products and services shall keep the EU statement of conformity and technical documentation of all relevant information relating to the conformity of the ICT products or services with a scheme at the disposal of the national cybersecurity certification authority referred to in Article 50(1) for a period defined in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

4. The issuing of EU statement of conformity is voluntary unless otherwise specified in the Union law or in Member States law.

5. The EU statement of conformity issued pursuant to this Article shall be recognised in all Member States.

Article 47

Elements of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall include at least the following elements:

(a) subject-matter and scope of the certification scheme, including the type or categories of ICT processes, products and services covered;

(aa) a clear description of the purpose of the scheme and how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme.

(b) reference to international, European or national standards followed in the evaluation. Where standards are not available or appropriate, a reference shall be made to technical specifications that meet the requirements of Annex II of Regulation 1025/2012 or, if such are not available, to technical specifications or other cybersecurity requirements defined in the scheme;

(c) where applicable, one or more assurance levels;

(c aa) an indication of whether self-assessment of conformity is permitted under the scheme;

(ca) where applicable, specific or additional requirements applicable to conformity assessment bodies in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(d) specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved;

(e) where applicable, information to be supplied or otherwise be made available to the conformity assessment bodies by an applicant which is necessary for certification;

(f) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(g) rules for monitoring compliance with the requirements of the certificates or the EU statement of conformity, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;

(h) where applicable, conditions for granting, maintaining, continuing and renewing a certificate, as well as conditions for extending or reducing the scope of certification;

(i) rules concerning the consequences of non-conformity of certified or self-assessed ICT products, services and processes with the requirements of the scheme;

(j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT processes, products and services are to be reported and dealt with;

(k) where applicable, rules concerning the retention of records by conformity assessment bodies;

(l) identification of national or international cybersecurity certification schemes covering the same type or categories of ICT processes, products and services, security requirements, evaluation criteria and methods, and assurance levels;

(m) the content and the format of the issued certificate or the EU statement of conformity;

(ma) the period of the availability of the EU statement of conformity and the technical documentation of all relevant information by the manufacturer or provider of ICT products and services;

(mb) maximum period of validity of certificates;

(mc) disclosure policy for granted, amended and withdrawn certificates;

(md) conditions for the mutual recognition of certification schemes with third countries;

(me) where applicable, rules concerning any peer assessment mechanism established in the scheme for the bodies issuing European cybersecurity certificates for high assurance levels pursuant to Article 48(4a). Such mechanism shall be without prejudice to the peer review provided for in Article 50a;

(mf) format and procedures to be followed by manufacturers and providers in supplying and updating the supplementary cybersecurity information in accordance with Article 47a (EP).

2. The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.

3. Where a specific Union act so provides, certification or the EU statement of conformity under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that act.

4. In the absence of harmonised Union legislation, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

Article 47 a

Cybersecurity information for certified products, process and services

1. The manufacturer or provider of certified or self-assessed ICT products, services and processes shall provide the following supplementary information:

a) guidance and recommendations to assist end users with secure configuration, installation, deployment, operation and maintenance of the products or services;

b) the period during which security support will be offered to end users in particular as regards the availability of cybersecurity related updates;

c) contact information and accepted methods for receiving vulnerability information from end users or security researchers;

d) a reference to online repositories listing publicly disclosed vulnerabilities related to the product or service and relevant cybersecurity advisories.

2. The information referred to in paragraph 1 of this Article shall be available in electronic form and remain available and updated as necessary at least until the expiry of the corresponding certificate or EU statement of conformity.

Article 48

Cybersecurity certification

1. ICT processes, products and services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 44 shall be presumed to be compliant with the requirements of such scheme.

2. The certification shall be voluntary, unless otherwise specified in Union law or in Member States law.

2a. The Commission shall assess regularly and latest by 31 December 2023 and at least every 2 years after the efficiency and utilization of the adopted certification schemes and whether any particular schemes shall be made mandatory through relevant Union legislation to ensure an adequate level of cybersecurity of ICT products, processes and services in the Union and improve the functioning of the internal market.

The Commission shall, based on the outcome of the assessment, identify the ICT products, processes and services covered by an existing certification scheme which should be covered by a mandatory scheme.

As a priority, the Commission shall focus on the sectors listed in Annex II of the Directive 2016/1148 which shall be assessed latest two years after the adoption of the first scheme.

When preparing the assessment the Commission shall:

a) consider the impact of the measures on the manufacturers or providers of such ICT product and services and the users in terms of costs, and the (societal and/or economic) benefits stemming from the anticipated enhanced level of security for the targeted products and services;

b) take into account the availability and uptake of existing relevant national and international legislation;

c) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;

d) consider implementation deadlines, transitional measures or periods, taking in particular into account the possible impact of the measure on the providers or manufacturers, including SMEs.

e) propose the most speedy and efficient way in which the transition from a voluntary to mandatory certification schemes is going to be implemented.

3. A European cybersecurity certificate pursuant to this Article referring to assurance level basic or substantial shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44.

4. By way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity certification scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such body shall be one of the following:

(a) a national cybersecurity certification authority referred to in Article 50(1);

(b) a public body that is accredited as conformity assessment body pursuant to Article 51(1).

4a. In cases where a European cybersecurity certification scheme pursuant to Article 44 requires an assurance level high, the certificate can only be issued by a national cybersecurity certification authority referred to in Article 50(1) or, under the following conditions, by a conformity assessment body referred to in Article 51:

(a) upon prior approval by the national cybersecurity certification authority for each individual certificate issued by a conformity assessment body; or

(b) upon prior general delegation of this task to a conformity assessment body by the national cybersecurity certification authority.

5. The natural or legal person which submits its ICT processes, products or services to the certification mechanism shall make available to the conformity assessment body referred to in Article 51 or the national cybersecurity certification authority referred to in Article 50, where this authority is the body issuing the certificate, all information necessary to conduct the certification procedure.

5a. The holder of a certificate shall inform the body issuing the certificate about any later detected vulnerabilities or irregularities concerning the security of the certified ICT process, product or service that may have an impact on the requirements related to the certification. The body shall forward this information without undue delay to the national cybersecurity certification authority.

6. Certificates shall be issued for the period defined by the particular certification scheme and may be renewed, provided that the relevant requirements continue to be met.

7. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.

Article 49

National cybersecurity certification schemes and certificates

1. Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products, processes and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant Article 44(4). National cybersecurity certification schemes and the related procedures for the ICT products, processes and services not covered by a European cybersecurity certification scheme shall continue to exist.

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, processes and services covered by a European cybersecurity certification scheme in force.

3. Existing certificates issued under national cybersecurity certification schemes and covered by a European cybersecurity certification scheme shall remain valid until their expiry date.

3a. With a view to avoiding fragmentation of the internal market, Member States shall communicate initiatives to draw up new national cybersecurity certification schemes to the Commission and the European Cybersecurity Certification Group.

Article 50

National cybersecurity certification authorities

1. Each Member State shall designate one or more national cybersecurity certification authorities in its territory, or upon mutual agreement with another Member State, designate one or more authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State.

2. Each Member State shall inform the Commission of the identity of the authorities designated, where a Member State designates more than one authority, it shall also inform about the tasks assigned to each of these authorities.

3. Without prejudice to Article 48(4)(a) and Article 48 (4a), each national cybersecurity certification authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise.

3a. Member States shall ensure that the activities of the national cybersecurity certification authority related to the issuance of certificates in accordance with Article 48(4)(a) and Article 48(4a) adhere to a strict separation of roles and responsibilities with the supervisory activities in this article and that both activities function independently from each other.

4. Member States shall ensure that national cybersecurity certification authorities have adequate resources to exercise their powers and to carry out, in an effective and efficient manner, the tasks assigned to them.

5. For the effective implementation of the regulation, it is appropriate that these authorities participate in the European Cybersecurity Certification Group established pursuant to Article 53 in an active, effective, efficient and secure manner.

6. National cybersecurity certification authorities shall:

(a) supervise and enforce rules included in schemes pursuant to Article 47(1)(g) for monitoring compliance of ICT products, processes and services with the requirements of the certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;

(aa) monitor and enforce the obligations of the manufacturer or provider/manufacturers and providers of ICT products, processes or services that are established in their respective territories and that carry out conformity self-assessment, in particular the obligations set out in Article 46(2) and (3) and in the corresponding European cybersecurity certification scheme;

(b) without prejudice to Article 51(1b), actively assist and support the national accreditation bodies in the monitoring and supervision of activities of conformity assessment bodies for the purpose of this Regulation,

(ba) monitor and supervise the activities of the public bodies referred to in Article 48(4);

(bb) where applicable, authorise conformity assessment bodies in accordance with Article 51(1b) and restrict, suspend or withdraw existing authorisation in cases of non-compliance of conformity assessment bodies with the requirements of this Regulation;

(c) handle complaints lodged by natural or legal persons in relation to certificates issued by the national cybersecurity certification authority or, in accordance with Article 48(4a) by conformity assessment bodies or to self-assessment of conformity made, investigate, to the extent appropriate, the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation within a reasonable time period;

(ca) provide an annual summary report on the activities undertaken, under points (aa), (b) and (ba) of this paragraph and under paragraph 7 to the Agency and the European Cybersecurity Certification Group;

(d) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on possible non-compliance of ICT processes, products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;

(e) monitor relevant developments in the field of cybersecurity certification.

7. Each national cybersecurity certification authority shall have at least the following powers:

(a) to request conformity assessment bodies, European cybersecurity certificate holders and issuers of EU statement of conformity to provide any information it requires for the performance of its task;

(b) to carry out investigations, in the form of audits, of conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statement of conformity, for the purpose of verifying compliance with the provisions under Title III;

(c) to take appropriate measures, in accordance with national law, in order to ensure that conformity assessment bodies, certificate holders and issuers of EU statement of conformity comply with this Regulation or with a European cybersecurity certification scheme;

(d) to obtain access to any premises of conformity assessment bodies and European cybersecurity certificates' holders for the purpose of carrying out investigations in accordance with Union or Member State procedural law;

(e) to withdraw, in accordance with national law, certificates issued by the national cybersecurity certification authority or, in accordance with Article 48(4a) by conformity assessment bodies, that are not compliant with this Regulation or a European cybersecurity certification scheme;

(f) to impose penalties, as provided for in Article 54, in accordance with national law, and to require the immediate cessation of the breaches of obligations set out in this Regulation.

8. National cybersecurity certification authorities shall cooperate amongst each other and the Commission and, in particular, exchange information, experiences and good practices as regards cybersecurity certification and technical issues concerning cybersecurity of ICT processes, products and services.

Article 50 a

Peer review

1. With a view to achieving equivalent standards throughout the Union in respect of certificates issued and EU statements of conformity, national cybersecurity certification authorities shall be subject to peer review.

2. Peer review shall be operated on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints.

3. Peer review shall cover the assessments of:

a) where applicable, whether the activities of the national cybersecurity certification authority related to the issuance of certificates in accordance with Article 48(4)(a) and Article 48(4a) adhere to a strict separation of roles and responsibilities with the supervisory activities according to Article 50 and that both activities function independently from each other,

b) the procedures for supervising and enforcing the rules of monitoring compliance of ICT products, services and processes with certificates in accordance with Article 50(6)(a),

c) the procedures for monitoring and enforcing the obligations of manufacturers and providers of ICT products or services in accordance with Article 50(6)(aa),

d) the procedures for monitoring, authorizing and supervising the activities of conformity assessment bodies;

e) where applicable, whether the personnel of bodies issuing certificates for high assurance levels pursuant to Article 48(4a) has the appropriate expertise.

4. Peer review shall be carried out by at least two national certification cybersecurity authorities of other Member States and the Commission and shall be carried out at least once every five years. The Agency may participate in the peer review.

5. The Commission may adopt implementing acts, in accordance with Article 55(2), establishing a plan for the peer review covering a period of at least five years, laying down criteria concerning the composition of the peer review team, the methodology used for the peer review, the schedule, periodicity and the other tasks related to the peer review. When adopting those implementing acts, the Commission shall take due account of the considerations of the European Cybersecurity Certification Group.

6. The outcomes of the peer review shall be examined by the European Cybersecurity Certification Group, which shall draw up a summary that may be made publicly available and which shall, when necessary, issue guidelines or recommendations on actions or measures to be taken by the entities concerned.

Article 51

Conformity assessment bodies

1. The conformity assessment bodies shall be accredited by the national accreditation body named pursuant to Regulation (EC) No 765/2008 only when they meet the requirements set out in the Annex to this Regulation.

1a. In cases where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to Article 48(4)(a) and Article 48(4a), the certification body of the national cybersecurity certification authority shall be accredited as conformity assessment body pursuant to paragraph 1 of this Article.

1b. Where European certification schemes set out specific or additional requirements pursuant to Article 47(1)(ca), only CABs authorised by the NCCA as meeting those requirements shall carry out tasks under such schemes.

2. Accreditation shall be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements set out in this Article. Accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke an accreditation of a conformity assessment body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation.

Article 52

Notification

1. For each European cybersecurity certification scheme adopted pursuant to Article 44, national cybersecurity certification authorities shall notify the Commission of the conformity assessment bodies accredited and where applicable, authorised pursuant to Article 51(1b) to issue certificates at specified assurance levels as referred to in Article 46 and, without undue delay, of any subsequent changes thereto.

2. One year after the entry into force of a European cybersecurity certification scheme, the Commission shall publish a list of notified conformity assessment bodies in the Official Journal.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 21, it shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A national cybersecurity certification authority may submit to the Commission a request to remove a conformity assessment body notified by that Member State from the list referred to in paragraph 2 of this Article. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the national cybersecurity certification authority's request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Article 53

European Cybersecurity Certification Group

1. The European Cybersecurity Certification Group (the 'Group') shall be established.

2. The Group shall be composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. Any member of the Group may represent not more than one other Member State.

Stakeholders and relevant third parties may be invited to meetings of the Group and to participate in its work.

3. The Group shall have the following tasks:

(a) to advise and assist the Commission in its work to ensure a consistent implementation and application of the present Title, in particular regarding the Union rolling work programme, cybersecurity certification policy issues, coordination of policy approaches, and the preparation of European cybersecurity certification schemes;

(b) to assist, advise and cooperate with the Agency in relation to the preparation of a candidate scheme in accordance with Article 44 of this Regulation;

(ba) to adopt an opinion on the candidate scheme pursuant to Article 44 of this Regulation;

(c) to request to the Agency to prepare a candidate European cybersecurity certification scheme in accordance with Article 43b(2) of this Regulation;

(d) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;

(e) to examine the relevant developments in the field of cybersecurity certification and exchange information and good practices on cybersecurity certification schemes;

(f) to facilitate the cooperation between national cybersecurity certification authorities under this Title through capacity building, the exchange of information, in particular by establishing methods for the efficient exchange of information relating to all issues concerning cybersecurity certification;

(fa) to provide support to the implementation of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to Article 47(1)(me) of this Regulation.

(f a) to facilitate the alignment of European cybersecurity schemes with internationally recognised standards, including by reviewing existing European cybersecurity schemes and, where appropriate, making recommendations to the Agency to engage with relevant international standardisation organisations to address insufficiencies or gaps in available internationally recognised standards;

4. The Commission shall chair the Group and provide the secretariat to it, with the assistance of ENISA as provided for in Article 8(a).

Article 53a

Right to lodge a complaint

1. Natural or legal persons shall have the right to lodge a complaint with the issuer of a certificate or, when related to a certificate issued by a conformity assessment body when acting in accordance with Article 48(4a), with the relevant national cybersecurity certification authority.

2. The body with which the complaint had been lodged shall inform the complainant of the progress of the proceedings and of the decision taken, including of the possibility of a judicial remedy as referred to in Article 53b.

Article 53b

Right to an effective judicial remedy

1. Notwithstanding any administrative or other non-judicial remedies, natural and legal persons shall have the right to an effective judicial remedy with regard to:

(a) decisions by a body referred to in Article 53a(1) including, where applicable, in relation to the issuing, non-issuing or recognition of a European cybersecurity certificate held by those natural and legal persons;

(b) failure to act on a complaint lodged with a body referred to in Article 53a(1).

2. Proceedings pursuant to this Article shall be brought before the courts of the Member State where the body that is the subject of the judicial proceedings is located.

Article 54

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Title and European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall [by …/without delay] notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.

TITLE IV

FINAL PROVISIONS

Article 55

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5(4)(b) of Regulation (EU) No 182/2011 shall apply.

Article 56

Evaluation and review

1. Not later than five years after the date referred to in Article 58, and every five years thereafter, the Commission shall assess the impact, effectiveness and efficiency of the Agency and its working practices and the possible need to modify the mandate of the Agency and the financial implications of any such modification. The evaluation shall take into account any feedback made to the Agency in response to its activities. Where the Commission considers that the continuation of the Agency is no longer justified with regard to its assigned objectives, mandate and tasks, it may propose that this Regulation be amended with regard to the provisions related to the Agency.

2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, processes and services in the Union and improving the functioning of the internal market.

2 a. The evaluation shall assess whether cybersecurity essential requirements for access to the internal market are necessary in order to prevent products, services and processes entering the Union market which do not meet basic cybersecurity requirements.

3. The Commission shall forward the evaluation report together with its conclusions to the European Parliament, the Council and the Management Board. The findings of the evaluation report shall be made public.

Article 57

Repeal and succession

1. Regulation (EC) No 526/2013 is repealed with effect from [….].

2. References to Regulation (EC) No 526/2013 and to ENISA shall be construed as references to this Regulation and to the Agency.

3. The Agency succeeds the Agency that was established by Regulation (EC) No 526/2013 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities. All existing decisions of the Management Board and Executive Board remain valid, providing they are not in conflict with the provisions of this Regulation.

4. The Agency shall be established for an indefinite period of time starting from […]

5. The Executive Director appointed pursuant to Article 24(4) of Regulation (EC) No 526/2013 shall be the Executive Director of the Agency for the remaining part of his term of office.

6. The Members and their alternates of the Management Board appointed pursuant to Article 6 of Regulation (EC) No 526/2013 shall be the Members and their alternates of the Management Board of the Agency for the remaining part of their term of office.

Article 58

Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

1a. This Regulation shall apply from […] except for the Articles 50, 51, 52, 53a, 53b and 54 which shall apply from [24 months after the date of its publication in the Official Journal of the European Union].

2. This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

Conformity assessment bodies that wish to be accredited shall meet the following requirements:

1. A conformity assessment body shall be established under national law and have legal personality.

2. A conformity assessment body shall be a third-party body independent of the organisation or the ICT products or services it assesses.

3. A body belonging to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products or services which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered a conformity assessment body.

4. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall neither be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product or service which is assessed, nor shall it be the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.

5. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of those ICT products or services, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall apply, in particular, to consultancy services.

5a. If a conformity assessment body is owned or operated by a public entity or institution, independence and absence of any conflict of interest shall be ensured and documented between, on the one hand, the certification supervisory authority and, on the other hand, the conformity assessment body.

6. Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

7. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, including of a financial nature, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.

8. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting or consultation of external personnel shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.

9. At all times and for each conformity assessment procedure and each kind, category or sub-category of ICT products or services, a conformity assessment body shall have at its disposal the necessary:

(a) personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a notified body and other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the ICT product or service technology in question and the mass or serial nature of the production process.

10. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.

11. The personnel responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all the conformity assessment activities;

(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the applicable requirements and testing standards;

(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

12. The impartiality of the conformity assessment bodies, of their top-level management and of the assessment personnel and subcontractors shall be guaranteed.

13. The remuneration of the top-level management and of the assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.

14. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.

15. The conformity assessment body and its personnel, committees, subsidiaries, subcontractors, and any associated body or personnel of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation or pursuant to any provision of national law giving effect to it, except where disclosure is required by Union or Member Stat law to which such persons are subject except in relation to the competent authorities of the Member States in which its activities are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this Section 15.

15a. With the exception of Section 15, the requirements of this Annex in no way preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person applying, or considering whether to apply, for certification.

15b. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of small and medium-sized enterprises as defined in Recommendation 2003/361/EC in relation to fees.

16. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) 765/2008 for the accreditation of conformity assessment bodies performing certification of processes, products or services.

17. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) 765/2008 for the accreditation of laboratories performing testing.