REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 17 April 2019

on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

Acting in accordance with the ordinary legislative procedure [3],

Whereas:

(1) Network and information systems and electronic communications networks and services play a vital role in 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, organisations and businesses 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) an extremely high number of connected digital devices are expected to be deployed across the Union during the next decade. While an increasing number of devices is connected to the internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In that context, the limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions. Network and information systems are capable of supporting all aspects of our lives and drive the Union's economic growth. They are the cornerstone for achieving the digital single market.

(3) Increased digitisation and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats and exacerbating the dangers faced by individuals, including vulnerable persons such as children. In order to mitigate those risks, all necessary actions need to be taken to improve cybersecurity in the Union so that network and information systems, communications networks, digital products, services and devices used by citizens, organisations and businesses – ranging from small and medium-sized enterprises (SMEs), as defined in Commission Recommendation 2003/361/EC [4], to operators of critical infrastructure – are better protected from cyber threats.

[1] OJ C 227, 28.6.2018, p. 86.
[2] OJ C 176, 23.5.2018, p. 29.
[3] Position of the European Parliament of 12 March 2019 (not yet published in the Official Journal) and decision of the Council of 9 April 2019.
[4] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(4) By making the relevant information available to the public, the European Union Agency for Network and Information Security (ENISA), as established by Regulation (EU) No 526/2013 of the European Parliament and of the Council ([5]) contributes to the development of the cybersecurity industry in the Union, in particular SMEs and start-ups. ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union.

(5) Cyberattacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyberattacks often take place across borders, the competence of, and policy responses by, cybersecurity and law enforcement authorities are predominantly national. Large-scale incidents could disrupt the provision of essential services across the Union. This necessitates effective and coordinated responses and crisis management at Union level, building on 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 forecasts of future developments, challenges and threats, at Union and global level, are important for policy makers, industry and users.

(6) 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 would foster mutually reinforcing objectives. Those objectives include further increasing the capabilities and preparedness of Member States and businesses, as well as improving cooperation, information sharing and coordination across Member States and Union institutions, bodies, offices and agencies. 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 cases of large-scale cross-border incidents and crises, while taking into account the importance of maintaining and further enhancing the national capabilities to respond to cyber threats of all scales.

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

(8) Cybersecurity is not only an issue related to technology, but one where human behaviour is equally important. Therefore, 'cyber-hygiene', namely, simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to risks from cyber threats, should be strongly promoted.

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

(10) Businesses and individual consumers should have accurate information regarding the assurance level with which the security of their ICT products, ICT services and ICT processes has been certified. At the same time, no ICT product or ICT service is wholly cyber-secure and basic rules of cyber-hygiene have to be promoted and prioritised. Given the growing availability of IoT devices, there is a range of voluntary measures that the private sector can take to reinforce trust in the security of ICT products, ICT services and ICT processes.

(11) Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. In many cases, identifying and documenting such dependencies enables end users of ICT products, ICT services and ICT processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures.

([5]) Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

(12) Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design'). Security should be ensured throughout the lifetime of the ICT product, ICT service or ICT process by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation.

(13) Undertakings, organisations and the public sector should configure the ICT products, ICT services or ICT processes designed by them in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible ('security by default'), thereby reducing the burden on users of having to configure an ICT product, ICT service or ICT process appropriately. Security by default should not require extensive configuration or specific technical understanding or non-intuitive behaviour on the part of the user, and should work easily and reliably when implemented. If, on a case-by-case basis, a risk and usability analysis leads to the conclusion that such a setting by default is not feasible, users should be prompted to opt for the most secure setting.

(14) Regulation (EC) No 460/2004 of the European Parliament and of the Council ([6]) established ENISA with the purposes of contributing to the goals of ensuring a high and effective 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. Regulation (EC) No 1007/2008 of the European Parliament and of the Council ([7]) extended ENISA's mandate until March 2012. Regulation (EU) No 580/2011 of the European Parliament and of the Council ([8]) further extended ENISA's mandate until 13 September 2013. Regulation (EU) No 526/2013 extended ENISA's mandate until 19 June 2020.

(15) The Union has already taken important steps to ensure cybersecurity and to increase trust in digital technologies. In 2013, the Cybersecurity Strategy of the European Union was adopted to guide the Union's policy response to cyber threats and risks. In an effort to better protect citizens online, the Union's first legal act in the field of cybersecurity was adopted in 2016 in the form of Directive (EU) 2016/1148 of the European Parliament and of the Council ([9]). Directive (EU) 2016/1148 put in place requirements concerning national capabilities in the field 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 the economy and society, such as energy, transport, drinking water supply and distribution, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces).

A key role was attributed to ENISA in supporting the implementation of that Directive. In addition, fighting effectively against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity. Other legal acts such as Regulation (EU) 2016/679 of the European Parliament and of the Council ([10]) and Directives 2002/58/EC ([11]) and (EU) 2018/1972 ([12]) of the European Parliament and of the Council also contribute to a high level of cybersecurity in the digital single market.

([6]) Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1).

([7]) Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (OJ L 293, 31.10.2008, p. 1).

([8]) Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (OJ L 165, 24.6.2011, p. 3).

([9]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

([10]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([11]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

([12]) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

(16) Since the adoption of the Cybersecurity Strategy of the European Union in 2013 and the last revision of ENISA's mandate, the overall policy context has changed significantly as the global environment has become more uncertain and less secure. Against that background and in the context of the positive development of the role of ENISA as a reference point for 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 ENISA's mandate, to establish its role in the changed cybersecurity ecosystem and to ensure that it contributes effectively to the Union's response to cybersecurity challenges emanating from the radically transformed cyber threat landscape, for which, as recognised during the evaluation of ENISA, the current mandate is not sufficient.

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

(18) Within the framework of Decision 2004/97/EC, Euratom taken by common agreement between the Representatives of the Member States, meeting at Head of State or Government level ([13]), 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. ENISA's host Member State should ensure the best possible conditions for the smooth and efficient operation of ENISA. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and for enhancing the efficiency of networking activities that ENISA be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of ENISA. The necessary arrangements should be laid down in an agreement between ENISA and the host Member State concluded after obtaining the approval of the Management Board of ENISA.

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

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

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

(22) ENISA should assist the Commission by means of advice, opinions and analyses regarding all Union matters related to policy and law development, updates and reviews in the field of cybersecurity and sector-specific aspects thereof in order to enhance the relevance of Union policies and laws with a cybersecurity dimension and to enable consistency in the implementation of those policies and laws at national level. ENISA should act as a reference point for advice and expertise for Union sector-specific policy and law initiatives where matters related to cybersecurity are involved. ENISA should regularly inform the European Parliament about its activities.

([13]) Decision 2004/97/EC, Euratom taken by common agreement between the Representatives of the Member States, meeting at Head of State or Government level, of 13 December 2003 on the location of the seats of certain offices and agencies of the European Union (OJ L 29, 3.2.2004, p. 15).

(23) The public core of the open internet, namely 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 of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone.

(24) The underlying task of ENISA is to promote the consistent implementation of the relevant legal framework, in particular the effective implementation of Directive (EU) 2016/1148 and other relevant legal instruments containing cybersecurity aspects, which is essential to increasing cyber resilience. In light of the fast evolving cyber threat landscape, it is clear that Member States have to be supported by more comprehensive, cross-policy approach to building cyber resilience.

(25) ENISA should assist the Member States and Union institutions, bodies, offices and agencies 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, ENISA should support the development and enhancement of national and Union computer security incident response teams ('CSIRTs') provided for in Directive (EU) 2016/1148, with a view to 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 to comply with their obligations under Directive (EU) 2016/1148 and therefore should not supersede them.

(26) ENISA should also assist with the development and updating of strategies on the security of network and information systems at Union level and, upon request, at Member State level, in particular on cybersecurity, and should promote the dissemination of such strategies and follow the progress of their implementation. ENISA should also contribute to covering the need for training and training materials, including the needs of public bodies, and where appropriate, to a high extent, 'train the trainers', building on the Digital Competence Framework for Citizens with a view to assisting Member States and Union institutions, bodies, offices and agencies in developing their own training capabilities.

(27) ENISA should support Member States in the field of cybersecurity awareness-raising and education by facilitating closer coordination and the exchange of best practices between Member States. Such support could consist in the development of a network of national education points of contact and the development of a cybersecurity training platform. The network of national education points of contact could operate within the National Liaison Officers Network and be a starting point for future coordination within the Members States.

(28) ENISA should assist the Cooperation Group created by Directive (EU) 2016/1148 in the execution of its tasks, in particular by providing expertise, advice and by facilitating the exchange of best practices, inter alia, with regard to the identification of operators of essential services by Member States, as well as in relation to cross-border dependencies, regarding risks and incidents.

(29) With a view to stimulating cooperation between the public and private sector and within the private sector, in particular to support the protection of the critical infrastructures, ENISA should support information sharing within and among sectors, in particular the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available tools and on procedure, as well as by 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.

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

(31) ENISA should aggregate and analyse voluntarily shared national reports from CSIRTs and the inter-institutional computer emergency response team for the Union's institutions, bodies and agencies established by the Arrangement between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) ([14]) in order to contribute to the setting up of common procedures, language and terminology for the exchange of information. In that context ENISA should involve the private sector within the framework of Directive (EU) 2016/1148 which lays down the grounds for the voluntary exchange of technical information at the operational level, in the computer security incident response teams network ('CSIRTs network') created by that Directive.

(32) ENISA should contribute to responses at Union level in the case of large-scale cross-border incidents and crises related to cybersecurity. That task should be performed in accordance with ENISA's mandate under this Regulation and an approach to be agreed by Member States in the context of Commission Recommendation (EU) 2017/1584 ([15]) and the Council conclusions of 26 June 2018 on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises. That task could include gathering relevant information and acting as a facilitator between the CSIRTs network and the technical community, as well as between decision makers responsible for crisis management. Furthermore, ENISA should support operational cooperation among Member States, where requested by one or more Member States, in the handling of incidents from a technical perspective, by facilitating relevant exchanges of technical solutions between Member States, and by providing input into public communications. ENISA should support operational cooperation by testing the arrangements for such cooperation through regular cybersecurity exercises.

(33) In supporting operational cooperation, ENISA should make use of the available technical and operational expertise of CERT-EU through structured cooperation. Such structured cooperation could build on ENISA's expertise. Where appropriate, dedicated arrangements between the two entities should be established to define the practical implementation of such cooperation and to avoid the duplication of activities.

(34) In performing its task to support operational cooperation within the CSIRTs network, ENISA 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 that cyber threats and incidents are analysed. 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 by producing combined technical information, such as technical solutions voluntarily shared by the Member States. Recommendation (EU) 2017/1584 recommends that Member States cooperate in good faith and share among themselves and with ENISA information on large-scale incidents and crises related to cybersecurity without undue delay. Such information would further help ENISA in performing its task of supporting operational cooperation.

(35) As part of the regular cooperation at technical level to support Union situational awareness, ENISA, in close cooperation with the Member States, should prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs or the national single points of contact on the security of network and information systems ('single points of contact') provided for in Directive (EU) 2016/1148, both on a voluntary basis, the European Cybercrime Centre (EC3) at Europol, CERT-EU and, where appropriate, the European Union Intelligence and Situation Centre (EU INTCEN) at the European External Action Service. That report should be made available to the Council, the Commission, the High Representative of the Union for Foreign Affairs and Security Policy and the CSIRTs network.

(36) The support by ENISA for *ex-post* technical inquiries of incidents having a significant or substantial impact undertaken at the request of the Member States concerned should focus on the prevention of future incidents. The Member States concerned should provide the necessary information and assistance in order to enable ENISA to support the *ex-post* technical inquiry effectively.

([14]) OJ C 12, 13.1.2018, p. 1.
([15]) Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

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

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

(39) In order to increase the resilience of the Union, ENISA should develop expertise in the field of cybersecurity of infrastructures, in particular to support the sectors listed in Annex II to Directive (EU) 2016/1148 and those used by the providers of the digital services listed in Annex III to that Directive, by providing advice, issuing guidelines and exchanging best practices. With a view to ensuring easier access to better-structured information on cybersecurity risks and possible remedies, ENISA should develop and maintain the 'information hub' of the Union, a one-stop-shop portal providing the public with information on cybersecurity originating in Union and national institutions, bodies, offices and agencies. Facilitating access to better-structured information on cybersecurity risks and possible remedies could also help Member States bolster their capacities and align their practices, thus increasing their overall resilience to cyberattacks.

(40) ENISA should contribute to raising the public's awareness of cybersecurity risks, including through an EU-wide awareness-raising campaign by promoting education, and to providing guidance on good practices for individual users aimed at citizens, organisations and businesses. ENISA should also contribute to promoting best practices and solutions, including cyber-hygiene and cyber-literacy at the level of citizens, organisations and businesses by collecting and analysing publicly available information regarding significant incidents, and by compiling and publishing reports and guidance for citizens, organisations and businesses, to improve their 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. ENISA should furthermore organise, in line with the Digital Education Action Plan established in the Commission Communication of 17 January 2018 and in cooperation with the Member States and Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed at end users, to promote safer online behaviour by individuals and digital literacy, to raise awareness of potential cyber threats, including online criminal activities such as phishing attacks, botnets, financial and banking fraud, data fraud incidents, and to promote basic multi-factor authentication, patching, encryption, anonymisation and data protection advice.

(41) ENISA should play a central role in accelerating end-user awareness of the security of devices and the secure use of services, and should promote security-by-design and privacy-by-design at Union level. In pursuing that objective, ENISA should make use of available best practices and experience, especially the best practices and experience of academic institutions and IT security researchers.

(42) In order to support the businesses operating in the cybersecurity sector, as well as the users of cybersecurity solutions, ENISA should develop and maintain a 'market observatory' by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides.

(43) ENISA should contribute to the Union's efforts to cooperate with international organisations as well as within relevant international cooperation frameworks in the field of cybersecurity. In particular, ENISA should contribute, where appropriate, to cooperation with organisations such as the OECD, the OSCE and NATO. Such cooperation could include joint cybersecurity exercises and joint incident response coordination. Those activities are to be carried out in full respect of the principles of inclusiveness, reciprocity and the decision-making autonomy of the Union, without prejudice to the specific character of the security and defence policy of any Member State.

(44) In order to ensure that it fully achieves its objectives, ENISA should liaise with the relevant Union supervisory authorities and with other competent authorities in the Union, Union institutions, bodies, offices and agencies, including CERT-EU, EC3, the European Defence Agency (EDA), the European Global Navigation Satellite Systems Agency (European GNSS Agency), the Body of European Regulators for Electronic Communications (BEREC), the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), the European Central Bank (ECB), the European Banking Authority (EBA), the European Data Protection Board, the Agency for the Cooperation of Energy Regulators (ACER), the European Union Aviation Safety Agency (EASA) and any other Union agency involved in cybersecurity. ENISA should also liaise with authorities that deal with data protection in order to exchange know-how and best practices and should provide advice on cybersecurity issues 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 authorities regarding network and information security issues that might have an impact on their work, ENISA should respect existing channels of information and established networks.

(45) Partnerships could be established with academic institutions that have research initiatives in relevant fields, and there should be appropriate channels for input from consumer organisations and other organisations, which should be taken into consideration.

(46) ENISA, in its role as the secretariat of the CSIRTs network, should support Member States' CSIRTs and the CERT-EU in the operational cooperation in relation to the relevant tasks of the CSIRTs network, as referred to in Directive (EU) 2016/1148. Furthermore, ENISA 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 being capable of involving at least two CSIRTs while taking due account of the Standard Operating Procedures of the CSIRTs network.

(47) With a view to increasing Union preparedness in responding to incidents, ENISA should regularly organise cybersecurity exercises at Union level, and, at their request, support Member States and Union institutions, bodies, offices and agencies in organising such exercises. Large-scale comprehensive exercises which include technical, operational or strategic elements should be organised on a biennial basis. In addition, ENISA should be able to regularly organise less comprehensive exercises with the same goal of increasing Union preparedness in responding to incidents.

(48) ENISA should further develop and maintain its expertise on cybersecurity certification with a view to supporting the Union policy in that area. ENISA should build on existing best practices and should 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 (European cybersecurity certification framework) with a view to increasing the transparency of the cybersecurity assurance of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

(49) Efficient cybersecurity policies should be based on well-developed risk assessment methods, in both the public and private sectors. 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-sector and private-sector organisations will increase the level of cybersecurity in the Union. To that end, ENISA should support cooperation between stakeholders at Union level and facilitate their efforts relating to the establishment and take-up of European and international standards for risk management and for the measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems.

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

(51) In cooperation with competent authorities, ENISA should be able to disseminate information regarding the level of the cybersecurity of the ICT products, ICT services and ICT processes offered in the internal market, and should issue warnings targeting manufacturers or providers of ICT products, ICT services or ICT processes and requiring them to improve the security of their ICT products, ICT services and ICT processes, including the cybersecurity.

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

(53) ENISA should regularly consult standardisation organisations, in particular European standardisation organisations, when preparing the European cybersecurity certification schemes.

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

(55) ENISA should be able to respond to ad hoc requests for advice and assistance by Member States and Union institutions, bodies, offices and agencies on matters falling within ENISA's mandate.

(56) It is sensible and recommended to implement certain principles regarding the governance of ENISA in order to comply with 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 is to streamline the activities of decentralised agencies and improve their performance. The recommendations in the Joint Statement and Common Approach should also be reflected, as appropriate, in ENISA's work programmes, evaluations of ENISA, and ENISA's reporting and administrative practice.

(57) The Management Board, composed of the representatives of the Member States and of the Commission, should establish the general direction of ENISA'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 the execution of the budget, adopt appropriate financial rules, establish transparent working procedures for decision making by ENISA, adopt ENISA's single programming document, adopt its own rules of procedure, appoint the Executive Director and decide on the extension and termination of the Executive Director's term of office.

(58) In order for ENISA 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 experience. 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.

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

Executive Director should ensure that the members of ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure gender balance and an appropriate balance, according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies and the private sector, including industry, users, and academic experts in network and information security.

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

(61) ENISA should have an 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, established by the Management Board on a proposal from the Executive Director, should focus on issues relevant to stakeholders and should bring them to the attention of ENISA. The ENISA Advisory Group should be consulted in particular with regard to ENISA's draft annual work programme. The composition of the ENISA Advisory Group and the tasks assigned to it should ensure sufficient representation of stakeholders in the work of ENISA.

(62) The Stakeholder Cybersecurity Certification Group should be established in order to help ENISA and the Commission facilitate the consultation of relevant stakeholders. The Stakeholder Cybersecurity Certification Group should be composed of members representing industry in balanced proportions, both on the demand side and the supply side of ICT products and ICT services, and including, in particular, SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies pursuant to Regulation (EC) No 765/2008 of the European Parliament and of the Council ([16]), and academia as well as consumer organisations.

(63) ENISA should have rules in place regarding the prevention and the management of conflicts of interest. ENISA 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 ([17]). The processing of personal data by ENISA should be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council ([18]). ENISA should comply with the provisions applicable to the Union institutions, bodies, offices and agencies, and with national legislation regarding the handling of information, in particular sensitive non-classified information and European Union classified information (EUCI).

(64) In order to guarantee the full autonomy and independence of ENISA and to enable it to perform additional tasks, including unforeseen emergency tasks, ENISA should be granted a sufficient and autonomous budget whose revenue should primarily come from a contribution from the Union and contributions from third countries participating in ENISA's work. An appropriate budget is paramount for ensuring that ENISA has sufficient capacity to perform all of its growing tasks and to achieve its objectives. The majority of ENISA's staff should be directly engaged in the operational implementation of ENISA's mandate. The host Member State, and any other Member State, should be allowed to make voluntary contributions to ENISA's budget. 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 ENISA's accounts to ensure transparency and accountability.

(65) Cybersecurity certification plays an important role in increasing trust and security in ICT products, ICT services and ICT processes. The digital single market, and in particular the data economy and the IoT, can thrive only if there is general public trust that such products, services and processes provide a certain level of cybersecurity. Connected and automated cars, electronic medical devices, industrial automation control systems and 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 Directive (EU) 2016/1148 are also sectors in which cybersecurity certification is critical.

([16]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

([17]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

([18]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(66) 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, ICT services and ICT 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 Union-wide mechanisms of certification are among the other gaps affecting the single market in the field of cybersecurity. This makes it difficult for European businesses to compete at national, Union and global level. It also reduces the choice of viable and usable cybersecurity technologies that individuals and businesses have access to. Similarly, in the 2017 Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy – A Connected Digital Single Market for All, 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 internal market.

(67) Currently, the cybersecurity certification of ICT products, ICT services and ICT 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 that context, a certificate issued by a national cybersecurity certification authority is not in principle recognised in other Member States. Companies thus may have to certify their ICT products, ICT services and ICT processes in several Member States where they operate, for example, with a view to participating in national procurement procedures, which thereby adds to their costs. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach to horizontal cybersecurity issues, for instance in the field of the IoT. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual use, impeding mutual recognition mechanisms within the Union.

(68) Some efforts have been made in order to ensure the mutual recognition of certificates within the Union. 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 some of the Member States. That fact has limited the effectiveness of SOG-IS MRA from the point of view of the internal market.

(69) Therefore, it is necessary to adopt a common approach and to establish a European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognised and used in all Member States. In doing so, 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 the existing schemes under such systems to schemes under the new European cybersecurity certification framework. The European cybersecurity certification framework should have a twofold purpose. First, it should help increase trust in ICT products, ICT services and ICT processes that have been certified under European cybersecurity certification schemes. Second, it should help avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for undertakings operating in the digital single market. The European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, unless those standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in that regard.

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

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

(72) Flexible cybersecurity solutions are necessary for the industry to stay ahead of cyber threats, and therefore any certification scheme should be designed in a way that avoids the risk of being outdated quickly.

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

(74) The provisions of this Regulation should be without prejudice to Union law providing specific rules on the certification of ICT products, ICT services and ICT processes. In particular, Regulation (EU) 2016/679 lays down provisions for the establishment of certification mechanisms and of data protection seals and marks, for the purpose of demonstrating the compliance of processing operations by controllers and processors with that Regulation. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of the relevant ICT products, ICT services and ICT processes. This Regulation is without prejudice to the certification of data processing operations under Regulation (EU) 2016/679, including when such operations are embedded in ICT products, ICT services and ICT processes.

(75) The purpose of European cybersecurity certification schemes should be to ensure that ICT products, ICT services and ICT processes certified under such schemes comply with specified requirements that aim to protect the availability, authenticity, integrity and confidentiality of stored, transmitted or processed data or of the related functions of or services offered by, or accessible via those products, services and processes throughout their life cycle. It is not possible to set out in detail the cybersecurity requirements relating to all ICT products, ICT services and ICT processes in this Regulation. ICT products, ICT services and ICT processes and the cybersecurity needs related to those products, services and processes are so diverse that it is very difficult to develop general cybersecurity requirements that are valid in all circumstances. It is therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, which should be complemented by a set of specific cybersecurity objectives that are to be taken into account when designing European cybersecurity certification schemes. The arrangements by which such objectives are to be achieved in specific ICT products, ICT services and ICT 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 if no appropriate standards are available.

(76) The technical specifications to be used in European cybersecurity certification schemes should respect the requirements set out in Annex II to Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([19]). Some deviations from those requirements could, however, be considered to be 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 should be made publicly available.

(77) A conformity assessment is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service or ICT process have been fulfilled. That procedure is carried out by an independent third party that is not the manufacturer or provider of the ICT products, ICT services or ICT processes that are being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service or ICT process. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out. Depending on the assurance level, the European cybersecurity certification scheme should indicate whether the European cybersecurity certificate is to be issued by a private or public body. Conformity assessment and certification cannot guarantee per se that certified ICT products, ICT services and ICT processes are cyber secure. They are instead procedures and technical methodologies for attesting that ICT products, ICT services and ICT processes have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example in technical standards.

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

([19]) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

(79) European cybersecurity certification schemes could provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes itself carry out all of the checks to ensure that the ICT products, ICT services or ICT processes conform with the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for low complexity ICT products, ICT services or ICT processes that present a low risk to the public, such as simple design and production mechanisms. Moreover, conformity self-assessment should be permitted for ICT products, ICT services or ICT processes only where they correspond to assurance level 'basic'.

(80) European cybersecurity certification schemes could allow for both conformity self-assessments and certifications of ICT products, ICT services or ICT processes. In such a case, the scheme should provide for clear and understandable means for consumers or other users to differentiate between ICT products, ICT services or ICT processes with regard to which the manufacturer or provider of ICT products, ICT services or ICT processes is responsible for the assessment, and ICT products, ICT services or ICT processes that are certified by a third party.

(81) The manufacturer or provider of ICT products, ICT services or ICT processes who carry out a conformity self-assessment should be able to issue and sign the EU statement of conformity as part of the conformity assessment procedure. An EU statement of conformity is a document that states that a specific ICT product, ICT service or ICT process complies with the requirements of the European cybersecurity certification scheme. By issuing and signing the EU statement of conformity, the manufacturer or provider of ICT products, ICT services or ICT processes assumes responsibility for the compliance of the ICT product, ICT service or ICT process with the legal requirements of the European cybersecurity certification scheme. A copy of the EU statement of conformity should be submitted to the national cybersecurity certification authority and to ENISA.

(82) Manufacturers or providers of ICT products, ICT services or ICT processes should make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services or ICT processes with a European cybersecurity certification scheme available to the competent national cybersecurity certification authority for a period provided for in the relevant European cybersecurity certification scheme. The technical documentation should specify the requirements applicable under the scheme and should cover the design, manufacture and operation of the ICT product, ICT service or ICT process to the extent relevant to the conformity self-assessment. The technical documentation should be so compiled as to enable the assessment of whether an ICT product or ICT service complies with the requirements applicable under that scheme.

(83) The governance of the European cybersecurity certification framework takes into account the involvement of Member States as well as the appropriate involvement of stakeholders, and establishes the role of the Commission during the planning and proposing, requesting, preparing, adopting and reviewing of European cybersecurity certification schemes.

(84) The Commission should prepare, with the support of the European Cybersecurity Certification Group (the 'ECCG') and the Stakeholder Cybersecurity Certification Group and after an open and wide consultation, a Union rolling work programme for European cybersecurity certification schemes and should publish it in the form of a non-binding instrument. The Union rolling work programme should be a strategic document that allows industry, national authorities and standardisation bodies, in particular, to prepare in advance for future European cybersecurity certification schemes. The Union rolling work programme should include a multiannual overview of the requests for candidate schemes which the Commission intends to submit to ENISA for preparation on the basis of specific grounds. The Commission should take into account the Union rolling work programme while preparing its Rolling Plan for ICT Standardisation and standardisation requests to European standardisation organisations. In light of the rapid introduction and uptake of new technologies, the emergence of previously unknown cybersecurity risks, and legislative and market developments, the Commission or the ECCG should be entitled to request ENISA to prepare candidate schemes which have not been included in the Union rolling work programme. In such cases, the Commission and the ECCG should also assess the necessity of such a request, taking into account the overall aims and objectives of this Regulation and the need to ensure continuity as regards ENISA's planning and use of resources.

Following such a request, ENISA should prepare the candidate schemes for specific ICT products, ICT services and ICT processes without undue delay. The Commission should evaluate the positive and negative impact of its request on the specific market in question, especially its impact on SMEs, on innovation, on barriers to entry to that market and on costs to end users. The Commission, on the basis of the candidate scheme prepared by ENISA, should be empowered to adopt the European cybersecurity certification scheme by means of implementing acts. Taking account of the general purpose and security objectives laid down in this Regulation, European cybersecurity certification schemes adopted by the Commission should specify a minimum set of elements concerning the subject matter, scope and functioning of the individual scheme. Those elements should include, among other things, the scope and object of the cybersecurity certification, including the categories of ICT products, ICT services and ICT 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 assurance level ('basic', 'substantial' or 'high') and the evaluation levels where applicable. ENISA should be able to refuse a request by the ECCG. Such decisions should be taken by the Management Board and should be duly reasoned.

(85) ENISA should maintain a website providing information on and publicising European cybersecurity certification schemes, which should include, among other things, the requests for the preparation of a candidate scheme as well as the feedback received in the consultation process carried out by ENISA in the preparation phase. The website should also provide information about the European cybersecurity certificates and EU statements of conformity issued under this Regulation including information regarding the withdrawal and expiry of such European cybersecurity certificates and EU statements of conformity. The website should also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

(86) The assurance level of a European certification scheme is a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme. In order to ensure the consistency of the European cybersecurity certification framework, a European cybersecurity certification scheme should be able to specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. Each European cybersecurity certificate might refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity might only refer to the assurance level 'basic'. The assurance levels would provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service or ICT process and would be characterised by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent incidents. Each assurance level should be consistent among the different sectorial domains where certification is applied.

(87) A European cybersecurity certification scheme might specify several evaluation levels depending on the rigour and depth of the evaluation methodology used. Evaluation levels 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, ICT service or ICT process should contain a number of secure functions, as specified by the scheme, which may include: a secure out-of-the-box configuration, a signed code, secure update and exploit mitigations and full stack or heap memory protections. Those functions should have been developed, and be maintained, using security-focused development approaches and associated tools to ensure that effective software and hardware mechanisms are reliably incorporated.

(88) 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 documentation of the ICT product, ICT service or ICT process by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product or ICT service should also be subject to the technical review. Where a European cybersecurity certification scheme provides for a conformity self-assessment, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes has carried out a self-assessment of the compliance of the ICT product, ICT service or ICT process with the certification scheme.

(89) For assurance level 'substantial', the evaluation, in addition to the requirements for assurance level 'basic', should be guided at least by the verification of the compliance of the security functionalities of the ICT product, ICT service or ICT process with its technical documentation.

(90) For assurance level 'high', the evaluation, in addition to the requirements for assurance level 'substantial', should be guided at least by an efficiency testing which assesses the resistance of the security functionalities of ICT product, ICT service or ICT process against elaborate cyberattacks performed by persons who have significant skills and resources.

(91) Recourse to European cybersecurity certification and to EU statements of conformity should remain voluntary, unless otherwise provided for in Union law, or in Member State law adopted in accordance with Union law. In the absence of harmonised Union law, Member States are able to adopt national technical regulations providing for mandatory certification under a European cybersecurity certification scheme in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council ([20]). Member States also have recourse to European cybersecurity certification in the context of public procurement and of Directive 2014/24/EU of the European Parliament and of the Council ([21]).

(92) In some areas, it could be necessary in the future to impose specific cybersecurity requirements and make the certification thereof mandatory for certain ICT products, ICT services or ICT processes, in order to improve the level of cybersecurity in the Union. The Commission should regularly monitor the impact of adopted European cybersecurity certification schemes on the availability of secure ICT products, ICT services and ICT processes in the internal market and should regularly assess the level of use of the certification schemes by the manufacturers or providers of ICT products, ICT services or ICT processes in the Union. The efficiency of the European cybersecurity certification schemes, and whether specific schemes should be made mandatory, should be assessed in light of the cybersecurity-related legislation of the Union, in particular Directive (EU) 2016/1148, taking into consideration the security of the network and information systems used by operators of essential services.

(93) European cybersecurity certificates and EU statements of conformity should help end users to make informed choices. Therefore, ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued should be accompanied by structured information that is adapted to the expected technical level of the intended end user. All such information should be available online, and, where appropriate, in physical form. The end user should have access to information regarding the reference number of the certification scheme, the assurance level, the description of the cybersecurity risks associated with the ICT product, ICT service or ICT process, and the issuing authority or body, or should be able to obtain a copy of the European cybersecurity certificate. In addition, the end user should be informed of the cybersecurity support policy, namely for how long the end user can expect to receive cybersecurity updates or patches, of the manufacturer or provider of ICT products, ICT services or ICT processes. Where applicable, guidance on actions or settings that the end user can implement to maintain or increase the cybersecurity of the ICT product or of the ICT service and contact information of a single point of contact to report and receive support in the case of cyberattacks (in addition to automatic reporting) should be provided. That information should be regularly updated and made available on a website providing information on European cybersecurity certification schemes.

(94) 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 ICT products, ICT services or ICT processes covered by a European cybersecurity certification scheme should cease to be effective from a date established by the Commission by means of implementing acts. Moreover, Member States should not introduce new national cybersecurity certification schemes for ICT products, ICT services or ICT processes already covered by an existing European cybersecurity certification scheme. However, Member States should not be prevented from adopting or maintaining national cybersecurity certification schemes for national security purposes. Member States should inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes. The Commission and the ECCG should evaluate the impact of the new national cybersecurity certification schemes on the proper functioning of the internal market and in light of any strategic interest in requesting a European cybersecurity certification scheme instead.

(95) European cybersecurity certification schemes are intended to help harmonise cybersecurity practices within the Union. They need to contribute to increasing the level of cybersecurity within the Union. The design of the European cybersecurity certification schemes should take into account and allow for the development of innovations in the field of cybersecurity.

([20]) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

([21]) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

(96) European 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 European cybersecurity certificates. European cybersecurity certification schemes should specify the conditions under which an update may require that an ICT product, ICT service or ICT process be recertified or that the scope of a specific European cybersecurity certificate be reduced, taking into account any possible adverse effects of the update on compliance with the security requirements of that certificate.

(97) Once a European cybersecurity certification scheme is adopted, manufacturers or providers of ICT products, ICT services or ICT processes should be able to submit applications for certification of their ICT products or ICT services to the conformity assessment body of their choice anywhere in the Union. Conformity assessment bodies should be accredited by a national 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 should be renewable on the same conditions provided that the conformity assessment body still meets the requirements. National accreditation bodies should restrict, suspend or revoke the accreditation of a conformity assessment body where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.

(98) References in national legislation to national standards which have ceased to be effective due to the entry into force of a European cybersecurity certification scheme can be a source of confusion. Therefore, Member States should reflect the adoption of a European cybersecurity certification scheme in their national legislation.

(99) In order to achieve equivalent standards throughout the Union, to facilitate mutual recognition and to promote the overall acceptance of European cybersecurity 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, ICT services and ICT processes with European cybersecurity certificates, for monitoring the obligations of manufacturers or providers of ICT products, ICT services or ICT processes who carry out the conformity self-assessment, for monitoring conformity assessment bodies, as well as the appropriateness of the expertise of the staff of bodies issuing certificates for assurance level 'high'. The Commission should be able, by means of implementing acts, to establish at least a five-year plan for peer reviews, as well as lay down criteria and methodologies for the operation of the peer review system.

(100) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the European cybersecurity certification framework, certain European cybersecurity certification schemes may include a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services and ICT processes with an assurance level 'high' under such schemes. The ECCG should support the implementation of such peer-assessment mechanisms. The peer assessments should assess in particular whether the bodies concerned carry out their tasks in a harmonised way, and may include appeal mechanisms. The results of the peer assessments should be made publicly available. The bodies concerned may adopt appropriate measures to adapt their practices and expertise accordingly.

(101) Member States should designate one or more national cybersecurity certification authorities to supervise compliance with obligations arising from this Regulation. A national cybersecurity certification authority may be an existing or new authority. A Member State should also be able to designate, after agreeing with another Member State, one or more national cybersecurity certification authorities in the territory of that other Member State.

(102) National cybersecurity certification authorities should in particular monitor and enforce the obligations of manufacturers or providers of ICT products, ICT services or ICT processes established in its respective territory in relation to the EU statement of conformity, should assist the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies by providing them with expertise and relevant information, should authorise conformity assessment bodies to carry out their tasks where such bodies meet additional requirements set out in a European cybersecurity certification scheme, and should monitor relevant developments in the field of cybersecurity certification. National cybersecurity certification authorities should also handle complaints lodged by natural or legal persons in relation to European cybersecurity certificates issued by those authorities or in relation to European cybersecurity certificates issued by conformity assessment bodies,

where such certificates indicate assurance level 'high', should investigate, to the extent appropriate, the subject matter of the complaint and should inform the complainant of the progress and the outcome of the investigation within a reasonable period. Moreover, national cybersecurity certification authorities should cooperate with other national cybersecurity certification authorities or other public authorities, including by the sharing of information on the possible non-compliance of ICT products, ICT services and ICT processes with the requirements of this Regulation or with specific European cybersecurity certification schemes. The Commission should facilitate that sharing 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.

(103) With a view to ensuring the consistent application of the European cybersecurity certification framework, an ECCG that consists of representatives of national cybersecurity certification authorities or other relevant national authorities should be established. The main tasks of the ECCG should be to advise and assist the Commission in its work towards ensuring the consistent implementation and application of the European cybersecurity certification framework, to assist and closely cooperate with ENISA in the preparation of candidate cybersecurity certification schemes, in duly justified cases to request ENISA to prepare a candidate scheme, to adopt opinions addressed to ENISA on candidate schemes and to adopt opinions addressed to the Commission on the maintenance and review of existing European cybersecurity certifications schemes. The ECCG should facilitate the exchange of good practices and expertise between the various national cybersecurity certification authorities that are responsible for the authorisation of conformity assessment bodies and the issuance of European cybersecurity certificates.

(104) In order to raise awareness and to facilitate the acceptance of future European cybersecurity certification schemes, the Commission may issue general or sector-specific cybersecurity guidelines, for example on good cybersecurity practices or responsible cybersecurity behaviour highlighting the positive effect of the use of certified ICT products, ICT services and ICT processes.

(105) In order to further facilitate trade, and recognising that ICT supply chains are global, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). The Commission, taking into account the advice from ENISA and the European Cybersecurity Certification Group, may recommend the opening of relevant negotiations. Each European cybersecurity certification scheme should provide specific conditions for such mutual recognition agreements with third countries.

(106) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([22]).

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

(108) ENISA's operations should be subject to regular and independent evaluation. That evaluation should have regard to ENISA's objectives, its working practices and the relevance of its tasks, in particular its tasks relating to the operational cooperation at Union level. That evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework. In the event of a review, the Commission should evaluate how ENISA's role as a reference point for advice and expertise can be reinforced and should also evaluate the possibility of a role for ENISA in supporting the assessment of third country ICT products, ICT services and ICT processes that do not comply with Union rules, where such products, services and processes enter the Union.

([22]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(109) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, 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 (TEU). 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 those objectives.

(110) Regulation (EU) No 526/2013 should be repealed,

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 to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:

(a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and

(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

The framework referred to in point (b) of the first subparagraph applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.

2. This Regulation is 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 the activities necessary to protect network and information systems, the users of such systems, and other persons affected by 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 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 could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(9) 'European cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

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

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

(12) 'ICT product' means an element or a group of elements of a network or information system;

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

(14) 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

(15) 'accreditation' means accreditation as defined in point (10) of Article 2 of Regulation (EC) No 765/2008;

(16) 'national accreditation body' means a national accreditation body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008;

(17) 'conformity assessment' means a conformity assessment as defined in point (12) of Article 2 of Regulation (EC) No 765/2008;

(18) 'conformity assessment body' means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008;

(19) 'standard' means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012;

(20) 'technical specification' means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service or ICT process;

(21) 'assurance level' means a basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned;

(22) 'conformity self-assessment' means an action carried out by a manufacturer or provider of ICT products, ICT services or ICT processes, which evaluates whether those ICT products, ICT services or ICT processes meet the requirements of a specific European cybersecurity certification scheme.

TITLE II

ENISA (THE EUROPEAN UNION AGENCY FOR CYBERSECURITY)

CHAPTER I

Mandate and objectives

Article 3

Mandate

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

ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.

2. ENISA shall carry out the tasks assigned to it by Union legal acts that set out measures for approximating Member State laws, regulations and administrative provisions which are related to cybersecurity.

3. When carrying out its tasks, ENISA shall act independently while avoiding the duplication of Member State activities and taking into consideration existing Member State expertise.

4. ENISA shall develop its own resources, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.

Article 4

Objectives

1. ENISA 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, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.

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

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

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

5. ENISA 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, in particular in the event of cross-border incidents.

6. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

7. ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.

CHAPTER II

Tasks

Article 5

Development and implementation of Union policy and law

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

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

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

(3) assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet;

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

(5) supporting:

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

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

(c) Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy, including by providing advice to the European Data Protection Board upon request;

(6) supporting the regular review of Union policy activities by preparing an annual report on the state of the implementation of the respective legal framework regarding:

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

(b) summaries of notifications of breach of security or loss of integrity received from trust service providers provided by the supervisory bodies to ENISA, pursuant to Article 19(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([23]);

(c) notifications of security incidents transmitted by the providers of public electronic communications networks or of publicly available electronic communications services, provided by the competent authorities to ENISA, pursuant to Article 40 of Directive (EU) 2018/1972.

([23]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

Article 6

Capacity-building

1. ENISA shall assist:

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

(b) Member States and Union institutions, bodies, offices and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis;

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

(d) Member States in developing national CSIRTs, where requested pursuant to Article 9(5) of Directive (EU) 2016/1148;

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

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

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

(h) Member States by regularly organising the cybersecurity exercises at Union level referred to in Article 7(5) on at least a biennial basis and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them;

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

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

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

Article 7

Operational cooperation at Union level

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

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

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

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

(c) the establishment of practical arrangements for the execution of specific tasks, after consulting the Commission.

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

4. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by:

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

(b) assisting, at the 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 publicly available information or information provided voluntarily by Member States for that purpose; and

(d) at the request of one or more Member States, providing support in relation to *ex-post* technical inquiries regarding incidents having a significant or substantial impact within the meaning of Directive (EU) 2016/1148.

In performing those tasks, ENISA and CERT-EU shall engage in structured cooperation to benefit from synergies and to avoid the duplication of activities.

5. ENISA shall regularly organise cybersecurity exercises at Union level, and shall support Member States and Union institutions, bodies, offices and agencies in organising cybersecurity exercises following their requests. Such cybersecurity exercises at Union level may include technical, operational or strategic elements. On a biennial basis, ENISA shall organise a large-scale comprehensive exercise.

Where appropriate, ENISA shall also contribute to and help organise sectoral cybersecurity exercises together with relevant organisations that also participate in cybersecurity exercises at Union level.

6. ENISA, in close cooperation with the Member States, shall prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats based on publicly available information, its own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2016/1148, both on a voluntary basis, EC3 and CERT-EU.

7. ENISA shall contribute to developing 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 contributing to the establishment of 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) upon request, facilitating the technical handling of such incidents or crises, including, in particular, by supporting the voluntary sharing of technical solutions between Member States;

(d) supporting Union institutions, bodies, offices and agencies and, at their request, Member States, in the public communication relating to such incidents or crises;

(e) testing the cooperation plans for responding to such incidents or crises at Union level and, at their request, supporting Member States in testing such plans at national level.

Article 8

Market, cybersecurity certification, and standardisation

1. ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by:

(a) monitoring developments, on an ongoing basis, in related areas of standardisation and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to point (c) of Article 54(1) where standards are not available;

(b) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services and ICT processes in accordance with Article 49;

(c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8);

(d) participating in peer reviews pursuant to Article 59(4);

(e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5).

2. ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group pursuant to Article 22(4).

3. ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services and ICT processes, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.

4. ENISA shall contribute to 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.

5. ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services and ICT processes.

6. ENISA shall 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.

7. ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union.

Article 9

Knowledge and information

ENISA shall:

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

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

(c) in cooperation with experts from Member States authorities and relevant stakeholders, provide 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 to Directive (EU) 2016/1148 and those used by the providers of the digital services listed in Annex III to that Directive;

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

(e) collect and analyse publicly available information regarding significant incidents and compile reports with a view to providing guidance to citizens, organisations and businesses across the Union.

Article 10

Awareness-raising and education

ENISA shall:

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

(b) in cooperation with the Member States, Union institutions, bodies, offices and agencies and industry, organise 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 awareness and education.

Article 11

Research and innovation

In relation to research and innovation, ENISA shall:

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

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

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

Article 12

International cooperation

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

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

(c) at the request of the Commission, providing it with expertise;

(d) providing advice and support to the Commission on matters concerning agreements for the mutual recognition of cybersecurity certificates with third countries, in collaboration with the ECCG established under Article 62.

CHAPTER III

Organisation of ENISA

Article 13

Structure of ENISA

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

(a) a Management Board;

(b) an Executive Board;

(c) an Executive Director;

(d) an ENISA Advisory Group;

(e) a National Liaison Officers Network.

Section 1

Management Board

Article 14

Composition of the Management Board

1. The Management Board shall be composed of one member appointed by each Member State, and two members appointed by the Commission. All members shall have the right to vote.

2. Each member of the Management Board shall have an alternate. That alternate shall represent the member in the member's absence.

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

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

Article 15

Functions of the Management Board

1. The Management Board shall:

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

(b) adopt ENISA's draft single programming document referred to in Article 24, before its submission to the Commission for an opinion;

(c) adopt ENISA's single programming document, taking into account the Commission opinion;

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

(e) adopt the annual budget of ENISA and exercise other functions in respect of ENISA's budget in accordance with Chapter IV;

(f) assess and adopt the consolidated annual report on ENISA's activities, including the accounts and a description of how ENISA has met its performance indicators, submit both the annual report and the assessment thereof by 1 July of the following year, to the European Parliament, to the Council, to the Commission and to the Court of Auditors, and make the annual report public;

(g) adopt the financial rules applicable to ENISA in accordance with Article 32;

(h) 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;

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

(j) 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;

(k) adopt its rules of procedure, including rules for provisional decisions on the delegation of specific tasks, pursuant to Article 19(7);

(l) with respect to the staff of ENISA, exercise the powers conferred by the Staff Regulations of Officials (the 'Staff Regulations of Officials') and the Conditions of Employment of Other Servants of the European Union (the 'Conditions of Employment of Other Servants'), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([24]) on the appointing authority and on the Authority Empowered to Conclude a Contract of Employment ('appointing authority powers') in accordance with paragraph 2 of this Article;

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

(n) appoint the Executive Director and where relevant extend his or her term of office or remove him or her from office in accordance with Article 36;

(o) appoint an accounting officer, who may be the Commission's accounting officer, who shall be wholly independent in the performance of his or her duties;

(p) take all decisions concerning the establishment of ENISA's internal structures and, where necessary, the modification of those internal structures, taking into consideration ENISA's activity needs and having regard to sound budgetary management;

(q) authorise the establishment of working arrangements with regard to Article 7;

(r) authorise the establishment or conclusion of working arrangements in accordance with Article 42.

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

([24]) OJ L 56, 4.3.1968, p. 1.

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

Article 16

Chairperson of the Management Board

The Management Board shall elect a Chairperson and a Deputy Chairperson from among its members, by a majority of two thirds of the members. Their terms of office shall be 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 Chair shall replace the Chairperson *ex officio* if the Chairperson is unable to attend to his or her duties.

Article 17

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 its Chairperson, at the request of the Commission, or at the request of at least one third of its members.

3. The Executive Director shall take part in the meetings of the Management Board but shall not have the right to vote.

4. Members of the ENISA Advisory Group may take part in the meetings of the Management Board at the invitation of the Chairperson, but shall not have the right to vote.

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

6. ENISA shall provide the secretariat of the Management Board.

Article 18

Voting rules of the Management Board

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

2. A majority of two-thirds of the members of the Management Board shall be required for the adoption of the single programming document and of the annual budget and for 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 member's right to vote.

4. The Chairperson of the Management Board shall take part in the voting.

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

6. The Management Board's rules of procedure 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 19

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) together with the Management Board, ensure 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 set out in Article 20, assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters pursuant to Article 20.

3. The Executive Board shall be composed of five members. The members of the Executive Board shall be appointed from among the members of the Management Board. One of the members shall be the Chairperson of the Management Board, who may also chair the Executive Board, and another shall be one of the representatives of the Commission. The appointments of the members of the Executive Board shall aim to ensure gender balance on the Executive Board. The Executive Director shall take part in the meetings of the Executive Board but shall not have the right to vote.

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. Any such provisional decisions shall be notified to the Management Board without undue delay. The Management Board shall then decide whether to approve or reject the provisional decision no later than three months after the decision was taken. The Executive Board shall not take decisions on behalf of the Management Board that require the approval of a majority of two-thirds of the members of the Management Board.

Section 3

Executive Director

Article 20

Duties of the Executive Director

1. ENISA 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 ENISA;

(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 ENISA's activities, including the implementation of ENISA's annual work programme, and presenting it to the Management Board for assessment and adoption;

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

(g) preparing an action plan that follows up on the conclusions of internal or external audit reports, as well as on investigations by OLAF and reporting on progress biannually to the Commission and regularly to the Management Board;

(h) preparing the draft financial rules applicable to ENISA as referred to in Article 32;

(i) preparing ENISA'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 ENISA 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;

(m) exchanging views and information regularly with Union institutions, bodies, offices and agencies regarding their activities relating to cybersecurity to ensure coherence in the development and the implementation of Union policy;

(n) carrying out other tasks assigned to the Executive Director by this Regulation.

4. Where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities. The Executive Director shall inform the Management Board in advance thereof. 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 ENISA's internal rules of operation.

5. Where necessary, for the purpose of carrying out ENISA'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 States concerned, including the Member State in which the seat of ENISA is located, and shall 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 aggregate number of staff in all local offices shall be kept to a minimum and shall not exceed 40 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The number of the staff in each local office shall not exceed 10 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.

The decision establishing a local office 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 ENISA.

Section 4

ENISA Advisory Group, Stakeholder Cybersecurity Certification Group and National Liaison Officers Network

Article 21

ENISA Advisory Group

1. The Management Board, acting on a proposal from the Executive Director, shall establish in a transparent manner the ENISA Advisory 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 field of cybersecurity, and representatives of competent authorities notified in accordance with Directive (EU) 2018/1972, of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities. The Management Board shall aim to ensure an appropriate gender and geographical balance as well as a balance between the different stakeholder groups.

2. Procedures for the ENISA Advisory Group, in particular regarding its composition, the proposal by the Executive Director referred to in paragraph 1, the number and appointment of its members and the operation of the ENISA Advisory Group, shall be specified in ENISA's internal rules of operation and shall be made public.

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

4. The term of office of the members of the ENISA Advisory Group shall be two-and-a-half years. Members of the Management Board shall 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 to be 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 ENISA in respect of the performance of ENISA's tasks, except of the application of the provisions of Title III of this Regulation. It shall in particular advise the Executive Director on the drawing up of a proposal for ENISA's annual work programme, and on ensuring communication with the relevant stakeholders on issues related to the annual work programme.

6. The ENISA Advisory Group shall inform the Management Board of its activities on a regular basis.

Article 22

Stakeholder Cybersecurity Certification Group

1. The Stakeholder Cybersecurity Certification Group shall be established.

2. The Stakeholder Cybersecurity Certification Group shall be composed of members selected from among recognised experts representing the relevant stakeholders. The Commission, following a transparent and open call, shall select, on the basis of a proposal from ENISA, members of the Stakeholder Cybersecurity Certification Group ensuring a balance between the different stakeholder groups as well as an appropriate gender and geographical balance.

3. The Stakeholder Cybersecurity Certification Group shall:

(a) advise the Commission on strategic issues regarding the European cybersecurity certification framework;

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

(c) assist the Commission in the preparation of the Union rolling work programme referred to in Article 47;

(d) issue an opinion on the Union rolling work programme pursuant to Article 47(4); and

(e) in urgent cases, provide advice to the Commission and the ECCG on the need for additional certification schemes not included in the Union rolling work programme, as outlined in Articles 47 and 48.

4. The Stakeholder Certification Group shall be co-chaired by the representatives of the Commission and of ENISA, and its secretariat shall be provided by ENISA.

Article 23

National Liaison Officers Network

1. The Management Board, acting on a proposal from the Executive Director, shall set up a National Liaison Officers Network composed of representatives of all Member States (National Liaison Officers). Each Member State shall appoint one representative to the National Liaison Officers Network. The meetings of the National Liaison Officers Network may be held in different expert formations.

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

3. National Liaison Officers shall act as a point of contact at national level to facilitate cooperation between ENISA and national experts in the context of the implementation of ENISA's annual work programme.

4. While National Liaison Officers shall cooperate closely with the Management Board representatives of their respective Member States, the National Liaisons Officers Network itself shall not duplicate the work of the Management Board or of other Union forums.

5. The functions and procedures of the National Liaisons Officers Network shall be specified in ENISA's internal rules of operation and shall be made public.

Section 5

Operation

Article 24

Single programming document

1. ENISA shall operate in accordance with a single programming document containing its annual and multiannual programming, which shall include all of its planned activities.

2. Each year, the Executive Director shall draw up a draft single programming document containing its annual and multiannual programming with the corresponding financial and human resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) No 1271/2013 ([25]) and taking into account the 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 shall transmit it to the European Parliament, to the Council and to the Commission by 31 January of the following year, as well as any subsequently updated versions of that document.

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

([25]) Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).

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 multiannual 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 assigned to ENISA. Any substantial amendments to the annual work programme shall be adopted by the same procedure as for 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 multiannual work programme shall set out the overall strategic programming including objectives, expected results and performance indicators. It shall also set out the resource programming including multi-annual budget and staff.

8. The resource programming shall be updated annually. The strategic programming shall be updated where appropriate and in particular where necessary to address the outcome of the evaluation referred to in Article 67.

Article 25

Declaration of interests

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 to be prejudicial to their independence. The declarations shall be accurate and complete, shall be made annually in writing, and shall be 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 to be prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting on such items.

3. ENISA 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 26

Transparency

1. ENISA shall carry out its activities with a high level of transparency and in accordance with Article 28.

2. ENISA shall ensure that the public and any interested parties are provided with 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 25.

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

4. ENISA 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 27

Confidentiality

1. Without prejudice to Article 28, ENISA shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment 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 ENISA, including officials seconded by Member States on a temporary basis, shall comply with the confidentiality requirements of Article 339 TFEU, even after their duties have ceased.

3. ENISA 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 ENISA's tasks, the Management Board shall decide to allow ENISA to handle classified information. In that case ENISA, in agreement with the Commission services, shall adopt security rules applying the security principles set out in Commission Decisions (EU, Euratom) 2015/443 ([26]) and 2015/444 ([27]). Those security rules shall include provisions for the exchange, processing and storage of classified information.

Article 28

Access to documents

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

2. The Management Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 by 28 December 2019.

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

CHAPTER IV

Establishment and structure of ENISA's budget

Article 29

Establishment of ENISA's budget

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

2. Each year the Management Board, on the basis of the draft statement of estimates, shall produce a statement of estimates of ENISA's revenue and expenditure for the following financial year.

3. The Management Board, by 31 January each year, shall send the statement of estimates, which shall be part of the draft single programming document, to the Commission and the third countries with which the Union has concluded agreements as referred to in Article 42(2).

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

5. The European Parliament and the Council shall authorise the appropriations for the contribution from the Union to ENISA.

6. The European Parliament and the Council shall adopt ENISA's establishment plan.

([26]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
([27]) Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

7. The Management Board shall adopt ENISA's budget together with the single programming document. ENISA's budget shall become final following the definitive adoption of the general budget of the Union. Where necessary, the Management Board shall adjust ENISA's budget and single programming document in accordance with the general budget of the Union.

Article 30

Structure of ENISA's budget

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

(a) a contribution from the general budget of the Union;

(b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 32;

(c) Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in Article 32 and with the provisions of the relevant instruments supporting the policies of the Union;

(d) contributions from third countries participating in the work of ENISA as referred to in Article 42;

(e) any voluntary contributions from Member States in money or in kind.

Member States that provide voluntary contributions under point (e) of the first subparagraph shall not claim any specific right or service as a result thereof.

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

Article 31

Implementation of ENISA's budget

1. The Executive Director shall be responsible for the implementation of ENISA's budget.

2. The Commission's internal auditor shall exercise the same powers over ENISA as over Commission departments.

3. ENISA's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).

4. Upon the receipt of the Court of Auditors' observations on ENISA's provisional accounts pursuant to Article 246 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council ([28]), ENISA's accounting officer shall draw up ENISA's final accounts under his or her responsibility and shall submit them to the Management Board for an opinion.

5. The Management Board shall deliver an opinion on ENISA's final accounts.

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

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

([28]) Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).

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

9. By 15 November of year N + 1, the Executive Director shall publish ENISA's final accounts in the *Official Journal of the European Union*.

10. By 30 September of year N + 1, the Executive Director shall send the Court of Auditors a reply to its observations 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, any information required for the smooth application of the discharge procedure for the financial year concerned in accordance with Article 261(3) of Regulation (EU, Euratom) 2018/1046.

12. On a recommendation from the Council, the European Parliament 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 32

Financial rules

The financial rules applicable to ENISA shall be adopted by the Management Board after consulting the Commission. They shall not depart from Delegated Regulation (EU) No 1271/2013 unless such a departure is specifically required for the operation of ENISA and the Commission has given its prior consent.

Article 33

Combating fraud

1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([29]), ENISA shall by 28 December 2019, accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF) ([30]). ENISA shall adopt appropriate provisions applicable to all employees of ENISA, 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 of on-the-spot inspections, over all grant beneficiaries, contractors and subcontractors who have received Union funds from ENISA.

3. OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96 ([31]), 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 ENISA.

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

([29]) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

([30]) OJ L 136, 31.5.1999, p. 15.

([31]) 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 European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2).

CHAPTER V

Staff

Article 34

General provisions

The Staff Regulations of Officials and the Conditions of Employment of Other Servants, as well as the rules adopted by agreement between the Union institutions for giving effect to the Staff Regulations of Officials and the Conditions of Employment of Other Servants shall apply to the staff of ENISA.

Article 35

Privileges and immunity

Protocol No 7 on the privileges and immunities of the European Union, annexed to the TEU and to the TFEU, shall apply to ENISA and its staff.

Article 36

Executive Director

1. The Executive Director shall be engaged as a temporary agent of ENISA under point (a) of Article 2 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 employment contract with the Executive Director, ENISA 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 of the performance of the Executive Director and ENISA'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 in accordance with Article 18(2).

7. The Management Board, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, may extend the term of office of the Executive Director once by 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, if invited, shall 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 shall 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 37

Seconded national experts and other staff

1. ENISA may make use of seconded national experts or other staff not employed by ENISA. The Staff Regulations of Officials 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 of national experts to ENISA.

CHAPTER VI

General provisions concerning ENISA

Article 38

Legal status of ENISA

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

2. In each Member State ENISA 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 be a party to legal proceedings.

3. ENISA shall be represented by the Executive Director.

Article 39

Liability of ENISA

1. The contractual liability of ENISA 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 ENISA.

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

4. The Court of Justice of the European Union shall have jurisdiction in any dispute over compensation for damage as referred to in paragraph 3.

5. The personal liability of ENISA's staff towards ENISA shall be governed by the relevant conditions applying to ENISA's staff.

Article 40

Language arrangements

1. Council Regulation No 1 ([32]) shall apply to ENISA. The Member States and the other bodies appointed by the Member States may address ENISA and receive a reply in the official language of the institutions of the Union that they choose.

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

Article 41

Protection of personal data

1. The processing of personal data by ENISA shall be subject to Regulation (EU) 2018/1725.

2. The Management Board shall adopt implementing rules as 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) 2018/1725 by ENISA.

([32]) Council Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385/58).

Article 42

Cooperation with third countries and international organisations

1. To the extent necessary in order to achieve the objectives set out in this Regulation, ENISA may cooperate with the competent authorities of third countries or with international organisations or both. To that end, ENISA may establish working arrangements with the authorities of third countries and international organisations, subject to the prior approval of the Commission. Those working arrangements shall not create legal obligations incumbent on the Union and its Member States.

2. ENISA shall be open to the participation of third countries that have concluded agreements with the Union to that effect. Under the relevant provisions of such agreements, working arrangements shall be established specifying in particular the nature, extent and manner in which those third countries are to participate in ENISA's work, and shall include provisions relating to participation in the initiatives undertaken by ENISA, to financial contributions and to staff. As regards staff matters, those working arrangements shall comply with the Staff Regulations of Officials and Conditions of Employment of Other Servants in any event.

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

Article 43

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

After consulting the Commission, ENISA shall adopt security rules applying the security principles contained in the Commission's security rules for protecting sensitive non-classified information and EUCI, as set out in Decisions (EU, Euratom) 2015/443 and 2015/444. ENISA's security rules shall include provisions for the exchange, processing and storage of such information.

Article 44

Headquarters Agreement and operating conditions

1. The necessary arrangements concerning the accommodation to be provided for ENISA 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, ENISA's staff and members of their families shall be laid down in a headquarters agreement between ENISA and the host Member State, concluded after obtaining the approval of the Management Board.

2. ENISA's host Member State shall provide the best possible conditions for ensuring the proper functioning of ENISA, taking into account 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 of staff members.

Article 45

Administrative control

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

TITLE III

CYBERSECURITY CERTIFICATION FRAMEWORK

Article 46

European cybersecurity certification framework

1. The European cybersecurity certification framework shall be 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 Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes.

2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting 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, services and processes throughout their life cycle.

Article 47

The Union rolling work programme for European cybersecurity certification

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

2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.

3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:

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

(b) relevant Union or Member State law or policy;

(c) market demand;

(d) developments in the cyber threat landscape;

(e) request for the preparation of a specific candidate scheme by the ECCG.

4. The Commission shall take due account of the opinions issued by the ECCG and the Stakeholder Certification Group on the draft Union rolling work programme.

5. The first Union rolling work programme shall be published by 28 June 2020. The Union rolling work programme shall be updated at least once every three years and more often if necessary.

Article 48

Request for a European cybersecurity certification scheme

1. The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme.

2. In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. The Union rolling work programme shall be updated accordingly.

Article 49

Preparation, adoption and review of a European cybersecurity certification scheme

1. Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54.

2. Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board.

3. When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.

4. For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise.

5. ENISA shall closely cooperate with the ECCG. The ECCG 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.

6. ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme prepared in accordance with paragraphs 3, 4 and 5 to the Commission. The opinion of the ECCG shall not bind ENISA, nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission.

7. The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes which meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

8. At least every five years, ENISA shall evaluate each adopted European cybersecurity certification scheme, taking into account the feedback received from interested parties. If necessary, the Commission or the ECCG may request ENISA to start the process of developing a revised candidate scheme in accordance with Article 48 and this Article.

Article 50

Website on European cybersecurity certification schemes

1. ENISA shall maintain a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information provided in accordance with Article 55.

2. Where applicable, the website referred to in paragraph 1 shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

Article 51

Security objectives of European cybersecurity certification schemes

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

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

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

(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

(d) to identify and document known dependencies and vulnerabilities;

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

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

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

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

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

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

Article 52

Assurance levels of European cybersecurity certification schemes

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

2. European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity certification scheme under which the European cybersecurity certificate or EU statement of conformity is issued.

3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service or ICT process is to undergo.

4. The certificate or the EU statement of conformity shall refer 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.

5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level 'basic' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

6. A European cybersecurity certificate that refers to assurance level 'substantial' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

7. A European cybersecurity certificate that refers to assurance level 'high' shall provide assurance that the ICT products, ICT services and ICT processes for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.

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

Article 53

Conformity self-assessment

1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services and ICT processes that present a low risk corresponding to assurance level 'basic'.

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

3. The manufacturer or provider of ICT products, ICT services or ICT processes shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products or ICT services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for 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 an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.

5. EU statements of conformity shall be recognised in all Member States.

Article 54

Elements of European cybersecurity certification schemes

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

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

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

(c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme;

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

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

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

(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved;

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

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

(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;

(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;

(l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;

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

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

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

(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;

(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services or ICT processes;

(r) maximum period of validity of European cybersecurity certificates issued under the scheme;

(s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;

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

(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59;

(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.

2. The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law.

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

4. In the absence of harmonised Union law, 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 55

Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes

1. The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information:

(a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT 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 of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

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

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

Article 56

Cybersecurity certification

1. ICT products, ICT services and ICT processes that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme.

2. The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.

3. The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services and ICT processes covered by an existing certification scheme which are to be covered by a mandatory certification scheme.

As a priority, the Commission shall focus on the sectors listed in Annex II to Directive (EU) 2016/1148, which shall be assessed at the latest two years after the adoption of the first European cybersecurity certification scheme.

When preparing the assessment the Commission shall:

(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services or ICT processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services or ICT processes;

(b) take into account the existence and implementation of relevant Member State and third country law;

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

(d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services or ICT processes, including SMEs;

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

4. The conformity assessment bodies referred to in Article 60 shall issue European cybersecurity certificates pursuant to this Article referring to assurance level 'basic' or 'substantial' on the basis of criteria included in the European cybersecurity certification scheme adopted by the Commission pursuant to Article 49.

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

(a) a national cybersecurity certification authority as referred to in Article 58(1); or

(b) a public body that is accredited as a conformity assessment body pursuant to Article 60(1).

6. Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level 'high', the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body:

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

(b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.

7. The natural or legal person who submits ICT products, ICT services or ICT processes for certification shall make available to the national cybersecurity certification authority referred to in Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.

8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service or ICT process that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned.

9. A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met.

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

Article 57

National cybersecurity certification schemes and certificates

1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services and ICT processes that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services and ICT processes that are 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, ICT services and ICT processes already covered by a European cybersecurity certification scheme that is in force.

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

4. With a view to avoiding the fragmentation of the internal market, Member States shall inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes.

Article 58

National cybersecurity certification authorities

1. Each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, shall designate one or more national cybersecurity certification 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 designated national cybersecurity certification authorities. Where a Member State designates more than one authority, it shall also inform the Commission about the tasks assigned to each of those authorities.

3. Without prejudice to point (a) of Article 56(5) and Article 56(6), each national cybersecurity certification authority shall be independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making.

4. Member States shall ensure that the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in this Article and that those activities are carried out independently from each other.

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

6. For the effective implementation of this Regulation, it is appropriate that national cybersecurity certification authorities participate in the ECCG in an active, effective, efficient and secure manner.

7. National cybersecurity certification authorities shall:

(a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;

(b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services or ICT processes that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;

(c) without prejudice to Article 60(3), actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;

(d) monitor and supervise the activities of the public bodies referred to in Article 56(5);

(e) where applicable, authorise conformity assessment bodies in accordance with Article 60(3) and restrict, suspend or withdraw existing authorisation where conformity assessment bodies infringe the requirements of this Regulation;

(f) handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6) or in relation to EU statements of conformity issued under Article 53, and shall investigate the subject matter of such complaints to the extent appropriate, and shall inform the complainant of the progress and the outcome of the investigation within a reasonable period;

(g) provide an annual summary report on the activities conducted under points (b), (c) and (d) of this paragraph or under paragraph 8 to ENISA and the ECCG;

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

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

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

(a) to request conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires for the performance of its tasks;

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

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

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

(e) to withdraw, in accordance with national law, European cybersecurity certificates issued by the national cybersecurity certification authorities or European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6), where such certificates do not comply with this Regulation or with a European cybersecurity certification scheme;

(f) to impose penalties in accordance with national law, as provided for in Article 65, and to require the immediate cessation of infringements of the obligations set out in this Regulation.

9. National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services and ICT processes.

Article 59

Peer review

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

2. Peer review shall be carried out 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 assess:

(a) where applicable, whether the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in Article 58 and whether those activities are carried out independently from each other;

(b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services and ICT processes with European cybersecurity certificates pursuant to point (a) of Article 58(7);

(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services or ICT processes pursuant to point (b) of Article 58(7);

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

(e) where applicable, whether the staff of authorities or bodies that issue certificates for assurance level 'high' pursuant to Article 56(6) have the appropriate expertise.

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

5. The Commission may adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it. In adopting those implementing acts, the Commission shall take due account of the views of the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).

6. The outcomes of peer reviews shall be examined by the ECCG, which shall draw up summaries that may be made publicly available and which shall, where necessary, issue guidelines or recommendations on actions or measures to be taken by the entities concerned.

Article 60

Conformity assessment bodies

1. The conformity assessment bodies shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.

2. Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to point (a) of Article 56(5) and Article 56(6), the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1 of this Article.

3. Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification authority to carry out tasks under such schemes.

4. The accreditation referred to in paragraph 1 shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed on the same conditions, provided that the conformity assessment body still meets the requirements set out in this Article. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.

Article 61

Notification

1. For each European cybersecurity certification scheme, the national cybersecurity certification authorities shall notify the Commission of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 60(3) to issue European cybersecurity certificates at specified assurance levels as referred to in Article 52. The national cybersecurity certification authorities shall notify the Commission of any subsequent changes thereto without undue delay.

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

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish the amendments to the list of notified conformity assessment bodies in the *Official Journal of the European Union* within two months of 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 authority from the list referred to in paragraph 2. The Commission shall publish the corresponding amendments to that list in the *Official Journal of the European Union* within one month of the date of receipt of the national cybersecurity certification authority's request.

5. The Commission may adopt implementing acts to establish the circumstances, formats and procedures for 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 66(2).

Article 62

European Cybersecurity Certification Group

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

2. The ECCG shall be composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG shall not represent more than two Member States.

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

4. The ECCG shall have the following tasks:

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

(b) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme pursuant to Article 49;

(c) to adopt an opinion on candidate schemes prepared by ENISA pursuant to Article 49;

(d) to request ENISA to prepare candidate schemes pursuant to Article 48(2);

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

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

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

(h) to support the implementation of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to point (u) of Article 54(1);

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

5. With the assistance of ENISA, the Commission shall chair the ECCG, and the Commission shall provide the ECCG with a secretariat in accordance with point (e) of Article 8(1).

Article 63

Right to lodge a complaint

1. Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body when acting in accordance with Article 56(6), with the relevant national cybersecurity certification authority.

2. The authority or body with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken, and shall inform the complainant of the right to an effective judicial remedy referred to in Article 64.

Article 64

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 taken by the authority or body referred to in Article 63(1) including, where applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons;

(b) a failure to act on a complaint lodged with the authority or body referred to in Article 63(1).

2. Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.

Article 65

Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of 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 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 66

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, point (b) of Article 5(4) of Regulation (EU) No 182/2011 shall apply.

Article 67

Evaluation and review

1. By 28 June 2024, and every five years thereafter, the Commission shall evaluate the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification. The evaluation shall take into account any feedback provided to ENISA in response to its activities. Where the Commission considers that the continued operation of ENISA is no longer justified in light of the objectives, mandate and tasks assigned to it, the Commission may propose that this Regulation be amended with regard to the provisions related to ENISA.

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

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

4. By 28 June 2024, and every five years thereafter, the Commission shall transmit a report on the evaluation together with its conclusions to the European Parliament, to the Council and to the Management Board. The findings of that report shall be made public.

Article 68

Repeal and succession

1. Regulation (EU) No 526/2013 is repealed with effect from 27 June 2019.

2. References to Regulation (EU) No 526/2013 and to the ENISA as established by that Regulation shall be construed as references to this Regulation and to ENISA as established by this Regulation.

3. ENISA as established by this Regulation shall succeed ENISA as established by Regulation (EU) No 526/2013 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities. All decisions of the Management Board and the Executive Board adopted in accordance with Regulation (EU) No 526/2013 shall remain valid, provided that they comply with this Regulation.

4. ENISA shall be established for an indefinite period as of 27 June 2019.

5. The Executive Director appointed pursuant to Article 24(4) of Regulation (EU) No 526/2013 shall remain in office and exercise the duties of the Executive Director as referred to in Article 20 of this Regulation for the remaining part of the Executive Director's term of office. The other conditions of his or her contract shall remain unchanged.

6. The members of the Management Board and their alternates appointed pursuant to Article 6 of Regulation (EU) No 526/2013 shall remain in office and exercise the functions of the Management Board as referred to in Article 15 of this Regulation for the remaining part of their term of office.

Article 69

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*.

2. Articles 58, 60, 61, 63, 64 and 65 shall apply from 28 June 2021.

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

Done at Strasbourg, 17 April 2019.

For the European Parliament	*For the Council*
The President	*The President*
A. TAJANI	G. CIAMBA

ANNEX

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 shall have legal personality.

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

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

4. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service or ICT process which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes.

5. The conformity assessment bodies, their top-level management and the persons 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 the ICT products, ICT services or ICT processes which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services.

6. If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented.

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

8. Conformity assessment bodies and their staff shall carry out 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 which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities.

9. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff 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.

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

    (a) staff 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 to be carried out, to ensure 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 body notified pursuant to Article 61 and its 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 technology of the ICT product, ICT service or ICT process in question and the mass or serial nature of the production process.

11. 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.

12. The persons responsible for carrying out conformity assessment activities shall have the following:

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

(b) satisfactory knowledge of the requirements of the conformity 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 conformity assessments have been carried out.

13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed.

14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.

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

16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff 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 conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.

17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification.

18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.

19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services or ICT processes.

20. 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) No 765/2008 for the accreditation of laboratories performing testing.