Council of the European Union

Brussels, 22 January 2026
(OR. en)

5611/26

Interinstitutional File:
2026/0011 (COD)

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

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	21 January 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2026) 11 final
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)

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

Encl.: COM(2026) 11 final

EUROPEAN
COMMISSION

Strasbourg, 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

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

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Since the adoption of the Cybersecurity Act (CSA) in 2019, the cybersecurity threat landscape has significantly evolved[1] in an increasingly complex geopolitical reality. Cyberattacks have surged and became more sophisticated, targeting critical infrastructure, businesses, and the general public, with the ransomware activity at its core[2]. Emerging technologies like the artificial intelligence (AI) and quantum computing are reshaping the tools of defence and the tactics of adversaries. In his 2024 **report 'The future of European competitiveness'**, Mario Draghi highlighted the need to increase security and reduce dependencies as one main areas of action needed in the European Union[3]. Both the European Preparedness Union Strategy[4] and the European Internal Security Strategy (ProtectEU)[5] have placed cybersecurity at the heart of the Union's resilience agenda. These strategies recognise that persistent cybersecurity threats are not just technical challenges, but strategic risks to our democracy, economy and way of life. Similarly, the Communication on Strengthening EU economic security[6] identifies preventing access to sensitive information and data that could undermine the Union's economic security and preventing and mitigating disruptions to Union's critical infrastructure affecting the Union economy as priority objectives, in which effective cybersecurity measures play a crucial role.

Against this background, **there are four main problems** that this proposed revision of the CSA aims to tackle: (i) the misalignment between the Union's cybersecurity policy framework and stakeholders' needs in an increasingly hostile threat landscape; (ii) the stalled implementation of the European cybersecurity certification framework (ECCF); (iii) the complexity and diversity of the cybersecurity-related policies impacting the Union's cyber posture; and (iv) increasing ICT supply chains security risks.

Based on the main problems identified, the **two general objectives** of the intervention are to increase cybersecurity capabilities and resilience and prevent fragmentation across the single market by:

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

---

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

2 ENISA, *ENISA Threat Landscape 2025*.

3 European Commission, The future of European Competitiveness, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

4 JOIN/2025/130 final.

5 COM/2025/148 final.

6 JOIN(2025) 977 final.

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

To help achieve the general objectives listed above, this intervention pursues the following **specific objectives (SPOs)**:

- to address the misalignment between the Union cybersecurity policy framework and stakeholders' needs:
  - SPO1: create the capacity to effectively implement Union cybersecurity policies and continuous operational cooperation enabling more structured cooperation between Member States;
  - SPO2: develop and implement means and mechanisms to effectively support and address the needs of Member States, industry and other stakeholders;
- to address the limited uptake and effectiveness of the ECCF:
  - SPO3: create the prerequisites for faster delivery of cybersecurity certification schemes driven by market needs by broadening the scope of the ECCF, ensuring effective maintenance and agile procedures and increasing transparency;
- to address the fragmented compliance landscape and complexity of horizontal and sectoral frameworks:
  - SPO4: create mechanisms and conditions to facilitate compliance with cybersecurity requirements, thereby making their implementation more coherent and effective.
- to address cybersecurity risks in the supply chain:
  - SPO5: De-risk critical ICT supply chains from entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers) and reduce critical dependencies by developing a coherent and effective framework at EU level to address ICT supply chain security risks.

The revision of the CSA falls within the remit of the **regulatory fitness and performance programme (REFIT)**. It strongly contributes to improving clarity, removing inefficiencies and aligning procedures across legal frameworks. The revision of the CSA contributes to the proper functioning of the internal market while ensuring the security and strategic autonomy of the Union.

More concretely, it proposes a full reform of the mandate of the European Union Agency for Cybersecurity (ENISA) providing effective support for policy implementation and added value in terms of supporting operational cooperation among Member States.

Given the increasing cybersecurity risks and challenges the Union is facing, the proposal aims to increase ENISA's financial and human resources to reflect its enhanced role, tasks, and its critical position in defending the digital ecosystem of the Union, allowing ENISA to effectively carry out the tasks conferred on it by this proposal.

The revision will also help eliminate fragmented practices, improving coordination while lowering compliance and operational costs in the long term. By repealing the current CSA and introducing a reformed ECCF, the proposal delivers a more effective and efficient tool that both promotes trust among businesses, the general public and public authorities and eases compliance with relevant Union legislation. It increases efficiency by revising the governance model and supporting more predictable, coherent and agile certification procedures to enable faster scheme development and implementation.

Greater synergies with relevant existing Union legal frameworks will promote certification as a compliance tool for businesses and reduce the administrative burden on conformity assessment bodies active under multiple pieces of cybersecurity legislation. Furthermore, by extending the scope of the ECCF and enabling the development of a scheme on the cyber posture of entities, the proposal reduces compliance costs for entities subject to relevant Union cybersecurity legislation, starting with entities in scope of the NIS 2 Directive. This approach will significantly simplify regulatory obligations for entities subject to multiple compliance requirements and ensure a more effective use of resources across national authorities. In addition to this revision, a proposal for a directive introducing targeted amendments to the NIS 2 Directive aims at simplifying compliance with and ensuring streamlined and coherent implementation of specific aspects of the cybersecurity framework, including with regard to scope, definitions, ransomware reporting and supervision of entities providing cross-border services.

The new regulation also creates a harmonised framework to tackle non-technical risks affecting ICT supply chains, reducing the current fragmentation of approaches across Member States. Together, these aspects represent a substantial simplification and modernisation of the Union's cybersecurity legal framework, fully aligned with the REFIT principles of clarity, efficiency and digital readiness.

- **Consistency with existing policy provisions in the policy area**

The Union has expanded its legal and policy tools with the adoption of a number of legal instruments and policy measures: (i) the NIS2 Directive serves to strengthen cybersecurity for critical infrastructure; (ii) physical security measures are defined in its 'sister directive', the Critical Entities Resilience (CER) Directive; (iii) the Cyber Resilience Act (CRA) enhances the cybersecurity of products; (iv) the Cyber Solidarity Act (CSoA) builds EU-wide response capabilities; (v) the EU Cyber Blueprint[7] supports EU-level crisis management cooperation in which the Commission and High Representative have key roles in preparing for and responding to large-scale cybersecurity incidents; (vi) the 5G Cybersecurity Toolbox (5G Toolbox) supports cybersecurity in 5G networks; (vii) the European action plan on the cybersecurity of hospitals and healthcare providers[8] helps improve their cybersecurity; and (viii) the Cybersecurity Skills Academy[9] addresses the growing challenge of the cybersecurity talent gap.

The above-mentioned cybersecurity legal framework was complemented by sector-specific legislation, i.e. the Digital Operational Resilience Act (DORA Regulation) for the financial

[7] COM/2025/66 final.
[8] COM(2025) 10 final.
[9] COM(2023) 207 final.

sector, network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS) for the electricity sub-sector, or information security rules (Part-IS[10]) for the air transport sub-sector.

The CSA revision is aligned with and strengthens the NIS2 provisions regarding ENISA's role in supporting the NIS2 implementation, including as regards operational cooperation support; it is also aligned with the CRA, including as regards the overview and management of vulnerabilities across the internal market and increases added value of shared situational awareness. Regarding the ECCF, the CSA revision is aligned with the CRA on product security objectives and vulnerability handling, and with the New Legislative Framework (NLF) on accreditation. Furthermore, there is a strong synergy stemming from the development of cyber posture certification for the NIS2 Directive as well as potentially for facilitating compliance with other relevant Union legal acts such as the General Data Protection Regulation (GDPR), without prejudice to their specific certification requirements. Additionally, the horizontal framework that addresses ICT supply chains cybersecurity risks supports the overall objective of the NIS2 Directive to create a high common level of cybersecurity across the Union and relies on the NIS2 Directive risk-based approach.

Furthermore, the CSA revision, in combination with the proposal for a Directive introducing targeted amendments to the NIS2 Directive with the aim of simplification, provides the necessary tools to make this comprehensive framework more effective and efficient in delivering the expected results, provide for a stronger European dimension and fill in the remaining regulatory gaps.

- **Consistency with other Union policies**

The CSA revision would complement the CER Directive which includes supply chain considerations as part of the resilience measures of critical entities. Moreover, it would complement upcoming initiatives, such as: (i) the Cloud and AI Development Act (CAIDA) which aims, among others, to tackle the lack of a competitive Union-based offer of cloud computing services at sufficient scale to serve highly critical use cases or sectors; (ii) the proposal for the Digital Networks Act (DNA); (iii) the upcoming revision of Regulation (EU) 2023/1781[11], (iv) the public procurement framework[12] which is currently under evaluation[13] and the Proposal for Regulation on simplification of the digital legislation (Digital Omnibus)[14] which provides the obligation on ENISA to develop a single entry-point for incident reporting through which entities can simultaneously fulfil their incident reporting obligations under multiple legal acts. Furthermore, it would reinforce the position of the Union authorities and operators, when engaging with southern Mediterranean partners, notably through fostering interconnection through secure and trusted digital infrastructures across the Mediterranean, which is a fundamental goal of the Pact for the Mediterranean.

---

10 Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645.

11 Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act), *OJ L 229, 18.9.2023, pp. 1–53*

12 In particular Directives 2014/23/EU, 2014/24/EU and 2014/25/EU.

13 European Commission, Commission launches call for evidence and public consultation on the evaluation of the Public Procurement Directives, https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_en.

14 COM/2025/837 final

The CSA revision is also in line with the Union's strategic documents, in particular when it comes to the ICT supply chain security framework. In the ProtectEU Strategy, the Commission further stated that a harmonised approach to the security of the Information and Communication Technology (ICT) supply chain can address the current fragmentation of the internal market caused by different approaches at national level, avoid critical dependencies and de-risk ICT supply chains from high-risk suppliers, in this way securing critical infrastructure. The Economic Security Strategy also highlighted the need to make the EU's economy and supply chain more resilient in order to promote its own competitiveness[15]. The need to address disruptions of supply chains and cyberattacks was also highlighted in the Preparedness Union Strategy and the White Paper for European Defence[16]. It is also aligned with the Future of European Competitiveness report of Mario Draghi, as highlighted above. What is more, the CSA revision in the area of ICT supply chain security with the recently adopted Joint Communication to the European Parliament and the Council on strengthening EU economic security[17].

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis for this proposal is Article 114 of the Treaty on the Functioning of the European Union (TFEU). Article 114 TFEU provides for the adoption of measures to ensure the establishment and functioning of the internal market. Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification, commonly known as the CSA[18], was originally adopted under this provision.

In the area of the cybersecurity of ICT supply chain security, the fragmentation of national frameworks addressing non-technical risk factors brings negative effects to the functioning of the internal market as the divergence in national approaches might ultimately lead to higher vulnerability of some Member States, with potential spill-over effects across the Union, impacting overall resilience and also trustworthiness.

Given the evolving nature of cybersecurity threats, and the increasing interdependence of Member States' digital systems, Article 114 TFEU remains the justified legal basis for the revision of the CSA. The proposed regulation reflects the most recent developments in the cybersecurity legislative landscape, especially considering ENISA's growing responsibilities and the expanding scope of certifications and risk management.

• Subsidiarity (for non-exclusive competence)

The subsidiarity principle requires the assessment of the necessity and the added value of Union action. Compliance with the subsidiarity principle in this area was already recognised when adopting the current CSA.

As already analysed in relation to the CSA, Union intervention is crucial as cybersecurity threats and related challenges extend beyond individual Member States. Fragmented national solutions have proven insufficient to achieve market-wide trust and coordination. A revised Union legal framework is required to remove barriers, ensure consistent implementation, and

---

15 JOIN/2023/20 final.
16 JOIN/2025/120 final.
17 JOIN/2025/977 final
18 Regulation - 2019/881 - EN - EUR-Lex

support Member States in an increasingly complex regulatory and threat environment. Cybersecurity is an issue of common interest for the Union.

The actions covered by the proposed regulation offer clear added value by supporting harmonisation, legal clarity and coordinated responses to cybersecurity challenges.

ENISA's current tasks have expanded through subsequent legislation without a comprehensive revision of its core responsibilities and resourcing. This has created inefficiencies and insufficient prioritisation of core tasks in support of Member States. Therefore, the proposal for intervention aims to refine and prioritise the current tasks in order to strengthen ENISA's mandate, enabling it to act as a single point of expertise for cybersecurity at Union level. On this point, there is no substantial difference in terms of subsidiarity compared to the CSA. In addition, diverse national certification schemes and differing regulatory approaches by Member States create a market fragmentation and additional compliance burdens, undermining competitiveness.

The new proposal also envisages new actions, in relation to supply chain policies and simplification efforts at Union level. It further strengthens supply chain security and the cybersecurity sector within the Union, and increases the preparedness and resilience of the Member States and industry.

Dependencies on entities established in a third country posing cybersecurity or controlled by such third country, by an entity established in such third country, or by a national of such third country (high-risk suppliers) affect entities across the Union, while significant supply chain cybersecurity incidents often spread across national borders. In addition, given the cross-border nature of ICT supply chains, fragmentation of compliance requirements within the internal market would undermine legal certainty for entities. Furthermore, the proposals for Multiannual Financial Framework (MFF) mandate the exclusion of high-risk suppliers to protect the integrity of the EU budget and security interests. The supply chain framework included in this regulation provides for the mechanism to identify countries posing cybersecurity concerns, an activity that can be carried out effectively only at the EU level. In relation to ICT supply chain security, only intervention at the EU level will ensure the same minimum level of security across the Union and necessary harmonisation of approaches.

The purpose of the CSA is maintained and further enhanced in this revision. This cannot be sufficiently achieved by the Member States, but can be better achieved at Union level in accordance with Article 5 of the Treaty on European Union.

- **Proportionality**

The proposed measures do not go beyond what is necessary to achieve the policy objectives of the proposal. Furthermore, the scope of Union intervention does not impede any further national action on national security matters. Union action is therefore justified on grounds of subsidiarity and proportionality.

The proposal aims to reflect better, in legal terms, ENISA's mandate and the process for the development, adoption and maintenance of European cybersecurity certificates. While the proposal includes certain new tasks for ENISA, their aim is to support Member States in the areas where significant gaps have been identified. ENISA will not replace Member States' CSIRTs. As regards the ECCF, certification remains voluntary and can help entities demonstrate compliance with Union's cybersecurity requirements. This approach ensures that the proportionality principle is respected.

Regarding the solutions proposed in relation to the ICT supply chain security, the framework foresees gathering evidence of what constitutes key assets and what measures would be proportionate and necessary to ensure de-risking of the critical supply chains. Prior to defining these measures, an assessment of economic impacts will be performed, which would look at, among others, economic feasibility, available alternatives in the market, lifecycle of the specific products. This assessment will inform what risk-based measures are needed and most appropriate.

- **Choice of the instrument**

The present proposal reviews Regulation (EU) 2019/881 which sets out the current mandate and tasks for ENISA and the ECCF. Therefore, ENISA's revised mandate and amendments to the ECCF are best established under the same legal instrument, using the instrument of a regulation. The proposed legislation also entails an effective framework at EU level to address ICT supply chain security risks, for which a regulation would more effectively address the problems identified and meet the objectives formulated, since only intervention at the EU level will ensure the same level of security across the Union and necessary harmonisation of approaches. The transposition process in the case of a directive for such intervention could leave too much room for discretion at national level, potentially leading to lack of uniformity of certain essential cybersecurity requirements, legal uncertainty, further fragmentation or even discriminatory cross-border situations.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

The European Commission, according to Article 67 of Regulation (EU) 2019/881, assessed the relevance, impact, effectiveness, efficiency, coherence and the added value of ENISA and the ECCF, considering the evolving technological and regulatory landscape. This evaluation, completed in December 2024, covered the period from 2017 to 2023 and aimed to review ENISA's mandate and activities, and to assess the ECCF's role in fostering a secure cyber environment across the EU. The main findings can be summarised as follows.

- **Relevance:** ENISA’s relevance in the cybersecurity domain is underscored by its responsiveness to evolving stakeholder needs and adaptability to a changing landscape. Although stakeholder satisfaction is generally positive, there are opportunities to increase ENISA’s impact. This can be achieved by improving support and visibility for diverse sectors, particularly small to medium-sized enterprises (SMEs), which often struggle with cybersecurity requirements. Better resource organisation and clearer coordination with national authorities are essential. Reprioritising activities and optimising existing resources will better align ENISA with the dynamic needs of the European cybersecurity landscape.

  Regarding the ECCF, despite its promising premise, the framework is still considered to have more potential than practical impact, as only one certification scheme has recently become operational. The framework is designed to seamlessly integrate with other Union legal acts to streamline procedures and facilitate cross-border trade. Its significance is highlighted in high-assurance areas like cloud services and 5G infrastructures.

- **Effectiveness:** ENISA has successfully met its mandate by delivering nearly all planned outputs, showcasing flexibility and resilience during crises like the COVID-

19 pandemic and Russia's war of aggression against Ukraine. However, improved prioritisation, clear focus, and strategic resource allocation are needed to increase efficiency. A more agile approach to internal governance is essential to adapt to evolving cybersecurity demands and minimise delays.

The ECCF aimed to harmonise cybersecurity certification across the Union but encountered significant challenges, including procedural limitations and fragmentation, which led to delays and inefficiencies, such as the delay in adopting the European Common Criteria-based cybersecurity certification scheme (EUCC). External factors, like geopolitical tensions and the COVID-19 pandemic, further complicated the achievement of the ECCF's objectives, highlighting the need for adaptable measures and consistent resource allocation among stakeholders to achieve uniformity and effectiveness in cybersecurity certification. Despite these hurdles, there have been positive outcomes - particularly in raising awareness among Member States of the importance and intricacies of cybersecurity certification.

- **Efficiency:** ENISA operated efficiently under its matrix-based organisational framework, promoting cooperation and task prioritisation. However, ENISA faced challenges in meeting increasing demands and filling specialised positions, exacerbated by a global shortage of IT specialists, leading to delays and heavy workload. To address these issues, ENISA could optimise its internal workforce and reallocate resources effectively, as demonstrated by strategic adjustments like the 2022 shift in resources towards the Cybersecurity Support Action. Additionally, improving budget management and reducing administrative expenditure would further improve the Agency's operational efficiency.

  The efficiency of the ECCF has been criticised due to extended timelines for adopting cybersecurity certification schemes and the complexities involved, with the first scheme only adopted in early 2024 nearly five years after the adoption of the CSA. Political and technical challenges, such as debates about data sovereignty and difficulties in translating drafts into legal acts, contributed to delays. Political challenges and technical demands have impeded progress, as seen with the EU Cloud Certification Scheme (EUCS) and the EU5G Scheme. Despite these inefficiencies, the framework gave rise to several positive aspects. However, there remains a need for improvements in stakeholder engagement and internal governance to ensure optimal functioning and strategic input.

- **Coherence:** ENISA's coherence is supported by significant stakeholder engagement and alignment with recent legislative frameworks. However, to enhance coherence and resource allocation, it is essential to improve synergies with other Union bodies, such as the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), and national authorities. Moreover, internal communication and resource management within ENISA, along with transparent interaction with private stakeholders, must be refined. Clear delineation of ENISA's tasks, consistent with the CRA and the NIS2 Directive, will improve both efficiency and regulatory consistency.

  Regarding the ECCF, full consistency with other Union legislative instruments, including the NIS2 Directive and the CRA, is crucial for ensuring a unified cybersecurity approach. While the ECCF shows theoretical alignment with these legislative measures, real-world integration remains complex and requires diligent oversight. The implementation of the adopted EUCC scheme within the CRA framework will be a significant test in this regard.

- **EU added value:** ENISA has made substantial contributions to the Union's cybersecurity ecosystem by promoting cooperation and aligning practices. Its role in facilitating national efforts and providing insights into emerging threats has been vital. However, criticism from private-sector stakeholders about the need for more tailored support indicates a need for improved stakeholder engagement and industry collaboration. Strategically reassessing resource management would enable ENISA to better adapt to evolving cybersecurity challenges and serve diverse stakeholders more effectively. The ECCF aimed to introduce harmonised certification processes but faced implementation challenges due to prolonged timelines and fragmentation. The added value of the ECCF has been limited due to its shortcomings in reaching its objectives and its lack of efficiency. Despite those challenges, the ECCF did improve harmonisation among Member States and established better cooperation opportunities, particularly by creating stakeholder cooperation fora such as the European Cybersecurity Certification Group (ECCG).

- **Stakeholder consultations**

Between 2023 and 2025, several stakeholder consultations were carried out both in the context of the evaluation of the CSA and the revision of the CSA as follows below.

- **In 2023,** 65 interviews were conducted (52 of which focused more on ENISA and 13 mainly on the ECCF), a survey programme was carried out, which received 209 responses (of which 70 were on the ECCF), a public consultation was concluded, and two workshops were organised on SWOT (strengths, weaknesses, opportunities and threats) analysis and recommendations with 26 and 70 participants respectively. These activities specifically aimed to gather stakeholders' views to evaluate the impact, effectiveness and efficiency of ENISA. The final report of the *Study to Support the Evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework carried out for the Commission by PwC, Intellera Consulting and PPMI (2024)* was completed in December 2024.
- **In 2025,** the Commission launched a call for evidence. In particular, stakeholders were invited to submit written contributions, including position papers, technical reports, or comments on specific reform proposals. A total of 184 individual contributions were received from a broad range of stakeholder categories, including industry associations, cybersecurity firms, SMEs, academic institutions, and public interest organisations.
- **Between April and June 2025**, the Commission organised a public consultation as part of the revision of the CSA and received 193 replies. The consultation consisted of 38 questions, both closed and open-ended, covering ENISA's mandate, the ECCF, ICT supply chain security and simplification.
- **Targeted consultation (interviews):** A series of semi-structured interviews were conducted with selected stakeholders. These included ENISA's representatives as well as national public authorities that have developed or manage national reporting platforms. Interviews focused on ENISA's role and capacity, the operational functioning of the ECCF, practical challenges in aligning national and Union-level certification processes, reporting burdens, and implementation obstacles. These discussions provided qualitative insights that enriched the interpretation of the results of the public consultation and supported the refinement of policy options.

– **Consultation of Member State representatives within the framework of the Council working party[19] and in bilateral discussions,** where Member States could express their views on the review of the CSA.

– **Targeted consultation (ECCF groups – ECCG, Stakeholder Cybersecurity Certification Group (SCCG)):** The Commission in its capacity as the chair of both groups, presented the state of play on the CSA revision at the ECCG meetings on 12 March and 3 July 2025, and the SCCG meeting on 17 March 2025. In addition, supplementary expert opinions from ECCG members were collected through questionnaires.

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

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

- **Impact assessment**

The revision of the CSA, together with the proposal for a Directive introducing targeted amendments of the NIS2 Directive, were supported by an impact assessment, see the summary below. The Regulatory Scrutiny Board (RSB) issued a 'positive opinion with reservations' of on the resubmitted draft impact assessment report related to the revision of the CSA[20]. The impact assessment was adjusted to address the RSB's recommendations and comments.

The final policy proposal does not deviate from the options assessed in the impact assessment.

The Commission examined options in four areas of intervention, in view of the specific objectives to be achieved: (1) ENISA's mandate (also part of the current CSA); (2) the ECCF (also part of the current CSA); (3) targeted amendments to the NIS 2 Directive, with an aim to simplify, but also interlinked with ENISA's mandate and the ECCF; and (4) ICT supply chain security, which is also relevant both for NIS2 ecosystem and for ECCF. Each set of options represents an intervention area on its own, while simultaneously being interlinked with and relevant to each other.

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

[19] Horizontal Working Party on Cyber Issues

[20] Regulation (EU) 2019/881 (http://data.europa.eu/eli/reg/2019/881/oj)

Option A.1: *Clarifying ENISA's mandate and providing for prioritisation* – This option would provide a clear and stable framework for ENISA's tasks by incorporating the tasks set out by other pieces of legislation.

Option A.2: *Reforming ENISA's mandate* – This option would repeal and replace the CSA, overhauling the Agency's mandate.

Option A.3: *Reforming ENISA's mandate with a strong operational support focus* – This option would build upon option A.2. In addition, ENISA would develop capabilities to support NIS 2 Directive entities directly in responding to and recovering from cybersecurity incidents upon a Member State's request.

Options for the ECCF

Option B.1: *Clarifying the ECCF's scope, elements and objectives and introducing a maintenance mechanism* – This option would provide for a new maintenance mechanism for the schemes, after their adoption, to be implemented by ENISA.

Option B.2: *Reforming the ECCF by revising its procedures and extending the scope to facilitate simplification of regulatory compliance* – This option would repeal the CSA and replace it by a new regulation. In addition to option B.1, the procedures related to the request, development and adoption of schemes would be revised to improve accountability and efficiency.

Option B.3: *Reforming the ECCF as envisaged under option B.2 and introducing mandatory certification for cyber posture* – This option would build on option B.2, but aims to further increase the impact of the framework by introducing mandatory certification of essential entities considering specific risk scenarios, instead of relying solely on voluntary certification of entities.

Options for simplification

Option C.1: *Taking a soft law and non-legislative instruments approach, including the use of existing empowerments (adoption of implementing acts under Article 21(5) and Article 23(11) of the NIS 2 Directive)* – This option envisages the adoption of implementing acts using the existing empowerments under the NIS 2 Directive to ensure a higher degree of harmonisation of cybersecurity risk-management measures, incident reporting thresholds, as well as type of information, the formats and the procedure of notifications. It also envisages the adoption of a set of guidelines to enhance legal certainty and harmonised implementation.

Option C.2: *Targeted intervention – further simplification of compliance with the relevant Union cybersecurity legislative framework* – This option involves limited intervention through changes to the CSA and the NIS 2 Directive with an aim to simplify specific aspects of the cybersecurity framework, including scope adaptations, maximum harmonisation for implementing acts, compliance proof through certification, and adoption of the set of guidelines as envisaged under option C.1.

Option C.3: *Harmonising cybersecurity-related measures set out in Union legislation* – This option would build on option C.2 and would remove all cybersecurity risk-management measures included in sectoral legislation and empowerments in relation to such measures. Instead, the NIS 2 Directive ecosystem would be amended to provide for streamlined requirements for all types of entities, with an aim to promote harmonisation.

Options for ICT Supply Chain Security

Option D.1: Taking a s*oft law approach to address cybersecurity risks for ICT supply chains* - This option would not provide for regulatory intervention at EU level. Instead, the Commission would increase the number of coordinated risk assessments and voluntary toolboxes.

Option D.2: *Ad hoc regulatory intervention codifying the 5G Toolbox* - This option would codify the 5G Toolbox measures. It would introduce an obligation for Member States to ensure that components from high-risk suppliers are not used in key assets of the network.

Option D.3: *Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks* - This option would establish a horizontal, technology and sector-neutral regulatory framework to address non-technical cybersecurity risks in ICT supply chains.

After extensive analysis, the following combination of options emerged as the preferred policy package*:* option A.2 (reforming ENISA's mandate); option B.2 (reforming the ECCF by revising its procedures and extending the scope to facilitate simplification of regulatory compliance); and option C.2 (targeted intervention – further simplification of compliance with the relevant Union cybersecurity legislative framework) and Option D.3 - Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks.

This combination offers a well-balanced response to identified policy challenges, significantly enhancing effectiveness, efficiency and coherence across the Union.

The transition to the proposed preferred option for the regulatory framework will incur costs, both for ENISA to meet its new tasks (estimated at up to EUR 161.3 million over five years) and for public authorities across the Union for supervising (estimated at up to EUR 80 million over five years, considering relevant cost savings). Regarding businesses, over five years, phasing out specific high-risk equipment could lead to annual costs of EUR 3.4 to 4.3 billion for mobile network operators, while investments in trusted suppliers could grow up to 2 billion per year.

At the same time, streamlined and reduced compliance obligations are expected to generate cost savings of up to EUR 15.3 billion for businesses over five years. Furthermore, improving the Union's overall cyber posture and technological sovereignty and stimulating innovation and competitiveness would yield significant benefits for the general public, public authorities and businesses. This is expected to largely offset initial expenditures in the long term.

By reducing market fragmentation and harmonising regulatory requirements, the preferred options enhance competitive equality across the Union, providing businesses with clearer paths to compliance and innovation.

The preferred options would also contribute to simplification through clear guidance and integrated systems, decreasing administrative burdens. The options comply with the 'one-in, one-out' principle by ensuring that new obligations are counterbalanced by reductions elsewhere.

- **Regulatory fitness and simplification**

The CSA revision, through the selected policy options A.2, B.2, C.2 and D.3, strongly contributes to improving clarity, removing inefficiencies and aligning procedures across legal frameworks. More concretely, option A.2 proposes a full reform of ENISA's mandate, effectively supporting policy implementation and operational cooperation among Member States. This consolidation will also help eliminate fragmented practices, improving coordination while lowering compliance and operational costs in the long term. Option B.2,

which involves repealing the current CSA and introducing a reformed ECCF, increases efficiency by revising the governance model and supporting more predictable, coherent and agile certification procedures. This will enable faster scheme adoption and better alignment with cross-cutting legislation, reducing regulatory fragmentation and easing the burden on both public and private stakeholders. Option C.2 reduces compliance costs for entities subject to relevant Union cybersecurity legislation through scope changes and by enabling organisational cybersecurity certification schemes for entities in scope of the NIS 2 Directive and other legal acts. This approach will significantly simplify regulatory obligations for entities subject to multiple requirements and ensure a more effective use of resources across national authorities. Option D.3 creates a harmonised framework to tackle non-technical risks affecting ICT supply chains, reducing the current fragmentation of approaches across Member States. Together, these options represent a substantial simplification and modernisation of the Union's cybersecurity legal framework, fully aligned with the REFIT principles of clarity, efficiency and digital readiness.

The proposal is consistent with the 'Digital Check', as its emphasis on streamlined digital processes demonstrates the Union's commitment to a digital-first approach, ensuring faster, more reliable data exchange and decision-making. Option D.3 could also have a high impact on digitalisation as it would entail the replacement of components from entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers).

- **Fundamental rights**

The legislative proposal was assessed based on its potential to enhance or put at risk fundamental rights and promote equality and trust, with a particular focus on societal impacts and rights, including privacy, data protection and the ability of individuals to understand, exercise and enforce their rights.

Extending ENISA's mandate will contribute to more cyber resilience across the economy and society in general, leading to better protection of people's privacy and personal data. The proposal will also support education and training on cybersecurity as it clarifies ENISA's role in the development of skills for the cybersecurity workforce.

Furthermore, the ECCF will improve trust among the general public and businesses in the Union in certified ICT solutions that support everyday life. Putting in place additional schemes would increase this impact.

The proposal contributes to people's trust by incentivising entities in critical sectors to obtain cybersecurity certification, thereby publicly demonstrating their high level of cybersecurity. Moreover, by ensuring harmonised reporting on ransomware incidents and taking measures for transition to post-quantum cryptography, it would increase public trust in the protection of sensitive data in critical sectors.

The provisions regarding supply chain security will have some impact on the protection of fundamental rights by limiting the foreign interference. Activities such as espionage and surveillance heavily undermine citizens' fundamental rights. This horizontal framework would have the potential to improve the trust, security and privacy in various technologies and digital solutions.

4. BUDGETARY IMPLICATIONS

The estimated budget of the EU Cybersecurity Agency (ENISA), which will contribute to a significant boost for the EU's security, was estimated at EUR 341 million for 7 years or yearly average budget of EUR 49 million (projection for 2028 to 2034). This represents 81.5% increase to the budget of the Agency in 2025. The generated benefits of the proposed initiative, as analysed in the Impact Assessment will be significant with up to EUR 14.6 billion of cost savings for businesses. Furthermore, while the magnitude of the potential cost savings linked to the overall improvement of the preparedness of the Union against cybersecurity incidents is by nature difficult to quantify, it is estimated that costs savings linked to faster response and slowing down proliferation of cybersecurity incidents could range from ranging from EUR 3.7 to 4.4 bn over five years. In the context of upcoming policy initiatives, the Commission will look at the overall distributions of resources for and within European institutions, bodies, agencies and offices in the area of cybersecurity to leverage knowledge and expertise, and to identify and develop synergies.
The additional resources proposed to reinforce the Agency are translated into 118 FTEs and additional operational costs that will cover for current contribution agreements between the ENISA and the Commission such as the maintenance of the Single Reporting Platform; for the FTEs working on the operation and administration of the EU Cybersecurity Reserve, as well as for important Commission initiatives like the development of the Single Entry Point under the Digital Omnibus Proposal. Other operational costs are related to the coordinated vulnerability disclosure programme, gathering and analysis of cybersecurity threat intelligence, secure communications and building cybersecurity maturity for ENISA. The operational costs for the maintenance of the European Cybersecurity Certification schemes, the cybersecurity skills authorisations and the testing tools service are also added in this budged, however these costs also include self-funding mechanisms through fees.

Important aspect of the proposal is the introduction of fee mechanisms that among other policy objectives will also contribute to a sustainable financial circuit within the Agency. The revised CSA presents three types of fees that will contribute to the ENISA's budget, namely, fees from issuing authorisations for skills attestations, fees from testing tools service and fees from supporting the maintenance of the European Cybersecurity Certification schemes. The expected generated benefit for the EU budget is estimated at approximately, EUR 18.5 million over 7-year period from 2028 to 2034.

The budgetary request of the Commission translates into 50 additional FTE posts, which will be implementing the supply chain framework, as well as tasks related to drafting implementing acts for the fee mechanisms, maintenance of certification schemes, standardisation and support to operational cooperation among others. The cost for the Commission of implementing the supply chain framework is expected to be specifically impacted by the number of ownership and control assessments (OCA) the Commission will be performing. The results of this task, however, will contribute greatly to savings for the Member States when supervising the implementation of mitigating measures and obligations imposed on the NIS2 entities by the framework. Member States will be able to leverage the results of the OCA assessments directly, rather each one individually to spend resources on the same assessments needs.

See the financial fiche accompanying the cyber package for more detailed information.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The Commission will monitor the application of the proposed regulation and submit a report on its evaluation to the European Parliament and to the Council every five years. These reports will be public and detail the effective application and enforcement of the proposed regulation.

- **Explanatory documents (for directives)**

Not applicable as the proposal is a regulation.

- **Detailed explanation of the specific provisions of the proposal**

The proposal clarifies the role of ENISA and entrusts it with concrete tasks to support its stakeholders, at the forefront of which are the Member States, in particular as regards support in implementing Union policy and legislation, operational cooperation, capacity-building, cybersecurity certification and standardisation and the improvement of the cybersecurity workforce and its mobility across the Union. The proposal further aims at making the European Cybersecurity Certification Framework (ECCF) more effective and efficient to improve the level of cybersecurity within the Union and empower customers to make informed choices when procuring ICT products, services, processes and managed security services across the internal market. Moreover, in combination with the proposal for a Directive introducing targeted amendments to the NIS 2 Directive, this proposal aims to facilitate compliance with cybersecurity obligations and unlock resources to strengthen the operational cybersecurity preparedness of entities in the Union's critical sectors. Last, the proposal addresses the need to make the Union's economy and ICT supply chain more resilient to promote its own security and competitiveness. The details are provided below.

TITLE I: GENERAL PROVISIONS

Title I of the proposed regulation contains the general provisions: the subject matter (Article 1) and the definitions (Article 2), including references to relevant definitions from other Union instruments, such as Directive (EU) 2022/2555[21] (NIS 2 Directive), Regulation (EC) No 765/2008[22] and Regulation (EU) No 1025/2012[23].

TITLE II: ENISA (THE EUROPEAN UNION AGENCY FOR CYBERSECURITY)

Title II of the proposed regulation contains the key provisions related to ENISA.

Chapter I outlines the mission (Article 3) and objectives of ENISA (Article 4).

Chapter II outlines the tasks of the Agency in three sections.

Section 1 includes provisions concerning the tasks related to supporting the implementation of Union policy and law. It specifies which entities and organisations are to receive support and the manner in which this should be done (Article 5). Article 6 delineates the Agency's capacity-building responsibilities, including offering knowledge and expertise to Member States on preventing and addressing cyber threats, updating cybersecurity strategies and

[21] http://data.europa.eu/eli/dir/2022/2555/oj
[22] http://data.europa.eu/eli/reg/2008/765/oj
[23] http://data.europa.eu/eli/reg/2012/1025/oj

expanding the cybersecurity workforce. ENISA will also assist Member States in their awareness-raising activities (Article 7) and will perform analysis of the main market trends in cybersecurity and disseminate technical advice and analyses (Article 8). ENISA will also contribute to and promote international cooperation on cybersecurity matters as described in Article 9.

Section 2 sets out ENISA's tasks regarding operational cooperation in relation to Member States, Union entities and CERT-EU, the computer security incident response teams (CSIRTs) network, EU-CyCLONe and other stakeholders, including the issuance of guidelines and implementation of secure communications tools (Article 10). ENISA will also help improve situational awareness of cyber threats and incidents by (among others) developing one or more repositories of cyber threat intelligence, performing analysis and issuing early alerts (Article 11). The rules on such early alerts (content, timing, service) are set out in Article 12. To assist essential and important entities in preparing for, responding to and recovering from ransomware incidents, ENISA shall operate the EU Cybersecurity Reserve as explained in Article 13 and in cooperation with Europol and CSIRTs or other competent authorities as applicable. Article 14 includes provisions on ENISA's role in cybersecurity exercises at Union level, including the compilation of an annual rolling programme of Union-level cybersecurity exercises. In addition to these tasks, ENISA should provide tools and platforms, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 (Article 15). Lastly, the Agency must develop a common Union vulnerability management service capacity and provide vulnerability management services (Article 16).

Section 3 on cybersecurity certification and standardisation sets out the Agency's tasks in this regard. Article 17 describes ENISA's role in the development and implementation of the ECCF, including its leading role in preparing schemes and ensuring their maintenance and capacity-building, while Article 18 sets out how ENISA should engage in drafting technical specifications and contribute to standardisation activities at European and international level, including in the area of cryptographic algorithms.

Section 4 details the Agency's tasks regarding the implementation of the Cybersecurity Skills Academy. Article 19 includes provisions related to ENISA's role regarding the European cybersecurity skills framework (ECSF), while its tasks regarding the development and maintenance of European individual cybersecurity skills attestation schemes are set out in Article 20. Requirements to become an authorised attestation provider are stipulated in Article 21 and those related to the processing of applications in Article 22. ENISA must provide public information related to the ECSF and individual cybersecurity skills attestations (Article 23).

Chapter III concerns the organisation of ENISA. The administrative and management structure of the Agency also includes a Deputy Executive Director (Article 24). Provisions related to the Management Board, its composition, its chairperson, meetings, functions and voting rules are included in Section 1 (Article 25 to 29). The Executive Board must assist the Management Board as set out in Article 30 under Section 2. Section 3 includes rules on the appointment, dismissal and extension of the term of office of the Executive Director (Article 31) and rules on the Executive Director's tasks and responsibilities (Article 32). The Management Board may decide to create a Deputy Executive Director role to assist the Executive Director (Section 4, Articles 33 and 34). The Management Board must set up the ENISA Advisory Group, which must advise ENISA according to the rules in Article 35. Section 6 sets out rules on the creation and composition of the Board of Appeal (Article 36) and its members (Article 37). Article 38 specifies the circumstances under which members of

the Board of Appeal must abstain from appeal proceedings and outlines the grounds for objecting to any member of the Board. Appeals may be brought before the Board of Appeal against decisions taken by ENISA or if ENISA fails to act (Article 39). Article 40 includes provisions on the people entitled to appeal, the time limit and the form of the appeal. Articles 41 to 43 set out rules on interlocutory revision, the examination of decisions on appeals, and actions before the Court of Justice. Finally, Article 44 provides for the process related to the single programming document.

Chapter IV concerns the establishment and structure of the Agency's budget, as well as rules guiding its presentation and implementation (Articles 45 to 55). It also includes the provisions facilitating the combating of fraud, corruption and other unlawful activities (Article 51).

Chapter V relates to the staffing of the Agency. It includes general provisions on the staff regulations and the conditions of employment of other servants and rules guiding privileges and immunity (Articles 56 and 57). It introduces provisions requiring Member States to designate liaison officers as seconded national experts to ENISA and their role in the Agency (Article 58). It also includes provisions guiding the use of seconded national experts and other staff not employed by the Agency (Article 59).

Finally, Chapter VI contains the general provisions related to the Agency. It outlines its legal status (Article 60), establishes its seat (Article 61) and contains provisions on the Agency's headquarters agreement and operating conditions, and on administrative control by the Ombudsman (Articles 62 and 63). It includes provisions regulating the issues of liability, language arrangements, and protection of personal data (Article 64 to 66), as well as security rules on the protection of sensitive non-classified and classified information (Article 67). It provides rules for the cooperation with Union entities and national authorities (Article 68) and other stakeholders (Article 69). It describes the rules guiding the Agency's cooperation with third countries and international organisations (Article 70).

TITLE III: EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

Title III of the proposed regulation establishes the ECCF.

Chapter I introduces the objectives, scope and procedures of the framework. The objectives (Article 71) include to strengthen cybersecurity across the Union and facilitate a harmonised approach to the certification of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities. The framework should also leverage certification to simplify compliance with applicable Union legislation through presumption of conformity, thereby reducing the burden for businesses (Article 78). Chapter I then details procedural aspects, starting with consultations on strategic European cybersecurity certification priorities and public information related to scheme development by the Commission and the creation of a new European Cybersecurity Certification Assembly (Article 72). Following a detailed request by the Commission (Article 73), ENISA is expected to deliver a candidate scheme within 12 months. Article 74 provides for additional timelines related to the submission of the ECCG's opinion and the submission of the scheme in view of its adoption by the Commission. Article 75 introduces a clear maintenance mechanism for existing schemes, which might lead to the review of such schemes (Article 76). The review of a scheme might be further informed by a periodical evaluation of the scheme's effectiveness and impact on the Single Market. Article 77 provides a basis for ENISA to draw up technical specifications in support of the development and maintenance of European cybersecurity certification schemes. When adopting or reviewing a scheme, the Commission may include references to

such technical specifications (Article 74). The various procedures ensure transparency and quality of delivery by engaging expert and general stakeholders at various stages of the planning, development, adoption and maintenance of certification schemes. Article 79 provides for a dedicated ENISA website on European cybersecurity certification schemes, which ought to provide information on adopted schemes as well as European cybersecurity certificates and EU statements of conformity issued under those schemes.

Chapter II provides general rules for the content of European cybersecurity certification schemes.

Article 80 sets out a list of security objectives against which a scheme is to be designed by ENISA and ensures alignment with relevant cybersecurity legislation. Each European cybersecurity certification scheme may provide for elements specified in Article 81. These elements must be compatible with Union legislation and may be harmonised across schemes using model provisions. Both provisions provide the necessary flexibility to adapt to different types of schemes. Additional provisions specify the rules related to assurance levels (Article 82) and conformity self-assessment (Article 83). The chapter further sets out a list of supplementary information (Article 84) that the manufacturer or provider of ICT products, ICT services or ICT processes must make available.

Finally, Chapter III establishes the rules of governance for the ECCF, divided into three sections.

Section 1 relates to rules on the issuance of European cybersecurity certificates including those at the assurance level 'high' (Article 85). Furthermore, it lays down rules for harmonising European cybersecurity certification schemes with national cybersecurity certification schemes and cybersecurity certificates (Article 86) and provides for the possibility of international recognition of European cybersecurity certificates, based on the equivalence principle (Article 87). The section also outlines the role of and rules applicable to national cybersecurity certification authorities (Article 88) and lays down rules for a peer review mechanism between those authorities, ensuring equivalent standards across the Union (Article 89), and for cooperation between those authorities in the ECCG (Article 90).

Section 2 provides for: (i) harmonised rules on the accreditation and authorisation of conformity assessment bodies (Articles 91-92); (ii) notification rules, including an empowerment to ensure further alignment with relevant Union law and the NLF (Article 93); and (iii) a challenge procedure (Article 94) ensuring that the requirements for conformity assessment bodies are upheld.

Finally, Section 3 provides for rights and judicial remedies against certification-related decisions (Article 96) and requires Member States to lay down and enforce proportionate penalties for regulatory infringements.

TITLE IV

Chapter I, Article 98 sets out the scope of the trusted ICT supply chain framework. The framework will address non-technical risks in sectors of high criticality and other critical sectors as referred in Directive (EU) 2022/2555. The mechanism shall identify key ICT assets in critical ICT supply chains and set out appropriate and proportionate mitigation measures on type of entities referred to in Annex I and Annex II to Directive (EU) 2022/2555. The framework will be based on Union-level coordinated security risk assessments, requested by the Commission or at least three Member States. Article 99 details how these risk assessments

will be carried out and that they should also establish mitigating measures. These risk assessments should be finalised within six months from the request. Upon request from the Commission, the NIS Cooperation Group may agree to a shorter period. The framework foresees a possibility of an emergency procedure if an immediate intervention is justified to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that there is a significant cyber threat for the security of the Union in relation to critical ICT supply chains. In such case, the Commission shall consult Member States on the need to take one or several mitigation measures and shall conduct a risk assessment. Article 100 provides that where, as a result of the risk assessment referred to in Article 99, or based on other sources, such as a public statement on behalf of the Union or a Member State, it appears that a third country poses serious and structural non-technical risks to ICT supply chains, the Commission shall verify the threat posed by that country, taking into account of the elements listed in Article 100. Where the Commission concludes that a third country poses serious and structural non-technical risks to ICT supply chains, Article 100 provides for a procedure for the Commission to designate such a third country as a country posing cybersecurity concerns to ICT supply chains. Entities established in a third country posing cybersecurity concerns designated in accordance with this Article, or controlled by such third country, by an entity established in such third country, or by a national of such third country will not be allowed to carry out a number of activities specified in this Article. Article 101 provides for a general ICT supply chain mechanism where upon completion of the security risk assessment by the NIS Cooperation Group or by the Commission in accordance with Article 99, the Commission may take measures provided in Articles 102 and 103.

The Commission can identify, through implementing acts, key ICT assets used for the manufacturing of products, provision of services by the types of entity referred to Annex I and Annex II to Directive (EU) 2022/2555. Article 102 further details the elements to be taken account for the identification of key ICT assets. Article 103 establishes potential mitigation measures in the ICT supply chain. The Commission, through implementing acts, can decide that entities operating in sectors of high criticality and other critical sectors have to be subject to specific mitigating measures, further detailed in the Article.

The Commission, by way of implementing acts, shall establish lists of high-risk suppliers relevant for the prohibitions laid down in the implementing acts adopted in accordance with Article 103(1), Article 103(7) or the prohibition referred to in Article 110(1), after conducting an assessment of establishment and ownership and control. It should consult suppliers concerned and competent authorities (Article 104).

An entity established in or controlled by entities from a third country posing cybersecurity concerns designated in accordance with Article 100, may request to be allowed to provide ICT components in key ICT assets of entities of the type referred in Annexes I and II to Directive (EU) 2022/2555 and to participate in public procurement in relation to the provision of such ICT components. Article 105 specifies what the request should contain and what is the procedure for such an exemption. Article 106 specifies the rights of defence for an entity in question. The Commission shall maintain a publicly accessible register of the decisions regarding exemptions (Article 107). Articles 108 and 109 specifies confidentiality rules and fees related to the exemption procedure.

Chapter II provides for an application of the trusted ICT supply chain framework to mobile, fixed and satellite electronic communications networks, ensuring alignment with the proposed Digital Networks Act.

The key ICT assets for mobile, fixed and satellite electronic communications networks are set out in Annex II. The transition period of phasing out ICT components from high-risk suppliers for the key ICT assets of the mobile electronic communications network shall not exceed 36 months from the entry into force of this Regulation. Transition periods for fixed and satellite electronic communications networks shall be specified by the Commission by virtue of implementing acts. The Commission is empowered to adopt delegated act to amend designated key ICT assets and transition periods, including for the future mobile generations (Article 110). Article 111 stipulates that providers of mobile, fixed and satellite electronic communications networks cannot not use, install or integrate, in any form, ICT components from high-risk suppliers and cannot be granted general or individual authorisation.

Competent authorities, supervision and enforcement, jurisdiction, rights of defence (Chapter III)

Chapter III further lays down the rules on competent authorities, supervision and enforcement and jurisdiction.

Articles 112-114 specify the powers, means and responsibilities of Member States in ensuring the implementation and enforcement of the provisions in Title IV. Member States have to designate one or more competent authorities, to be notified to the Commission. Article 113 provides for the Commission to set up a network for cooperation of competent authorities of Member States and the Commission to facilitate compliance, while Article 114 specifies the supervisory and enforcement measures that competent authorities are entitled to take. Penalties in case of infringement of the provisions of Title IV are specified in Article 115. Article 116 details the possibility for Member States to mutually assist each other when entities are having cross-border activities or when their key ICT assets are located in several Member States. Article 117 provides for the rules on jurisdiction and territoriality.

TITLE VI: FINAL PROVISIONS

Title VI of the proposed regulation includes the final provisions, outlining rules for adopting implementing and delegated acts, the evaluation process of the proposed regulation, and the repeal and succession of Regulation (EU) 2019/881. It also specifies the date of entry into force of the proposed Regulation.

2026/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(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[24],

Having regard to the opinion of the Committee of the Regions[25],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Since the adoption of Regulation (EU) 2019/881 of the European Parliament and of the Council[26], the geopolitical, technological and policy landscapes have undergone significant transformations. Cybersecurity incidents, whether caused by system failures, human error, malicious acts or natural phenomena, have surged and cyberattacks have become more sophisticated, affecting essential entities, businesses, and the general public. The cybercrime ecosystem has proliferated, with ransomware activity at its core. Supply chain incidents, whether caused by criminals for financial gain or by State actors for disruption, espionage, disinformation or warfare have intensified. As part of a wider hybrid strategy, incidents resulting from malicious cyber activities and system failures ripple outward, disrupting essential services, undermining trust in institutions, and affecting the Union's societal and defence readiness. Such incidents have proved their potential to impact economic activity, financial stability and people's lives. At the same time, vulnerability of critical civilian infrastructure and systems pose a risk to defence capabilities where they rely on them.

(2) In parallel, emerging technologies such as artificial intelligence and quantum computing have a disruptive effect on cybersecurity and cyber defence. They are

---

24 OJ C , , p. .

25 OJ C , , p. .

26 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) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

reshaping the tools of defence and the tactics of adversaries, posing threats to cybersecurity and cyber defence while also offering avenues for technological advancements. Although they may contribute to cybersecurity through enhanced threat detection or automated incident response, they are also increasing the overall attack surface for organisations, are potential targets for manipulation, and can undermine the long-term viability of security measures such as encryption.

(3) To address those developments, the Union has enhanced its legal and policy tools. Directive (EU) 2022/2555 of the European Parliament and of the Council[27] strengthens cybersecurity for critical infrastructure, complemented by Directive (EU) 2022/2557 of the European Parliament and of the Council[28] for physical security. Regulation (EU) 2024/2847 of the European Parliament and of the Council[29] enhances the cybersecurity of products with digital elements. Regulation (EU) 2025/38 of the European Parliament and of the Council[30] builds Union-wide response capabilities, and the Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management[31] ('Recommendation on the Cyber Blueprint') supports Union-level crisis management cooperation. The 5G Cybersecurity Toolbox[32] constitutes a first step towards a coordinated approach at Union level to secure 5G networks. The Commission communication on the Cybersecurity Skills Academy[33] addresses the growing challenge of the cybersecurity talent gap. Additionally, the cybersecurity framework has been enhanced by sector-specific legislation, in particular Regulation (EU) 2022/2554 of the European Parliament and of the Council[34] for the financial sector, Commission Delegated Regulation (EU) 2024/1366[35] for the electricity

---

27 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

28 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

29 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

30 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) (OJ L, 2025/38, 15.01.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

31 OJ C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

32 Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures, NIS Cooperation Group, 1/2020, available at: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

33 Communication from the Commission to the European Parliament and the Council, Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy'), COM(2023)207 final, 18 April 2023.

34 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

35 Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (OJ L, 2024/1366, 24.05.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

subsector, Commission Delegated Regulation (EU) 2022/1645[36] and Commission Implementing Regulation (EU) 2023/203[37](PART-IS) as well as relevant aviation security rules set out in Commission Regulation (EU) 2019/1583[38] for the air transport sub-sector, and other policy documents such as the Commission communication on an EU action plan on the cybersecurity of hospitals and healthcare providers[39]. Union entities are also strengthened with Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council[40], which lays down measures that aim to achieve a high common level of cybersecurity within Union institutions, bodies, offices and agencies. This enhanced legal framework for cybersecurity has further specified ENISA's tasks.

(4) In this context, and as stated in the ProtectEU: European Internal Security Strategy[41], Preparedness Union Strategy[42], ensuring the preparedness, security and resilience of the Union's society and economy requires strong European coordination, trust and information sharing between stakeholders, robust frameworks to ensure the security of ICT products, services, processes and managed security services, as well as growing and strengthening the cybersecurity workforce. It further calls for bolstering ICT supply chains by ensuring European technological sovereignty over key assets, which would increase the Union's resilience and could benefit cyber defence efforts. In

---

36 Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 (OJ L 248, pp. 18–31, 26.9.2022, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

37 Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 (OJ L 31, 2.2.2023, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

38 Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures (OJ L 246, 26.9.2019, pp. 15–18, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

39 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European action plan on the cybersecurity of hospitals and healthcare providers, COM(2025) 10 final, 15 January 2025.

40 Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

41 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Protect EU: a European Internal Security Strategy, COM(2025)148 final, 1 April 2025.

42 Joint Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Preparedness Union Strategy, JOIN(2025) 130 final.

addition, the Communication on Strengthening EU economic security[43] identifies as priority objectives the needs to prevent access to sensitive information and data that could undermine the EU's economic security and to prevent and mitigate disruptions to EU critical infrastructure affecting the EU economy. It acknowledges the essential role effective cybersecurity measures play in this regard.

(5) Large-scale cybersecurity incidents affecting critical infrastructure, digital services or essential societal functions may have impacts on the population requiring coordinated civil protection and crisis management action at Union level. In line with the all-hazards approach of the European Preparedness Union Strategy and Decision No 1313/2013/EU on the Union Civil Protection Mechanism, arrangements for situational awareness, incident response and exercises under this Regulation should feed in Union crisis management, notably though the Emergency Response Coordination Centre (ERCC).

(6) This proposal is consistent with and complemented by the [Proposal for a Directive complementing [the revision of Regulation (EU) 2019/881] and amending Directive (EU) 2022/2555 as regards the simplification of the implementation of measures for a high common level of cybersecurity across the Union], as well as with the [Proposal for Regulation on simplification of the digital legislation (Digital Omnibus)[44] which provides the obligation on ENISA to develop a single entry-point for incident reporting through which entities can simultaneously fulfil their incident reporting obligations under multiple legal acts.

(7) Regulation (EC) No 460/2004 of the European Parliament and of the Council[45] established ENISA with the aim of contributing to 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. ENISA's mandate was extended three times before Regulation (EU) 2019/881 granted it a permanent mandate. In order to better address the needs created by the evolving threat and technological landscapes, in particular with regards to operational cooperation and the increased need for cybersecurity professionals, ENISA's mandate should be further reinforced. In the interest of legal certainty, Regulation (EU) 2019/881 should be replaced.

(8) In an evolving threat landscape where cybersecurity incidents become increasingly more significant, delivering trust for individuals, public authorities and businesses in their daily use of technologies is even more important than ever. An increase in trust can be facilitated by a reinforced Union-wide certification of the ECCF providing for common cybersecurity requirements and evaluation criteria across national markets and sectors. The new framework should lay down the main horizontal requirements for European cybersecurity certification schemes and allow for European cybersecurity certificates and EU statements of conformity to be recognised and used in all Member States. In doing so, it should establish a procedure and governance framework that allows for the timely and predictable development and maintenance of European cybersecurity certification schemes. The European cybersecurity

---

43 Joint Communication from the Commission to the European Parliament and the Council, Strengthening EU economic security, JOIN(2025) 977 final.

44 COM/2025/837 final

45 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, ELI: http://data.europa.eu/eli/reg/2004/460/oj).

certification schemes should be applied uniformly in all Member States to ensure a harmonised implementation of cybersecurity requirements, level the playing field and prevent 'certification shopping' based on different levels of stringency in different Member States. ENISA should have a key role in providing for the development of the schemes through technical specifications and ensuring that such schemes remain technically up to date. Furthermore, to meet the market needs effectively, the framework should provide for the possibility for certification of cybersecurity risk management measures addressed to entities and facilitate compliance with other applicable Union legislation in the field of cybersecurity. Alignment with existing Union law, such as Regulation (EU) 2024/2847 and Directive (EU) 2022/2555, is essential for European cybersecurity certification schemes to contribute to reducing compliance burden on businesses, increase their attractiveness and strengthen the cyber resilience of the Union.

(9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around four key areas of cybersecurity at Union level. First, ENISA should support Member States in the consistent implementation of Union policy and legislation regarding cybersecurity and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States.

(10) Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union and provides for the mandate of CERT-EU, establishing it as the Cybersecurity Service for Union institutions, bodies, offices and agencies to contribute to the security of the unclassified ICT environment of Union entities by advising them on cybersecurity, supporting them to prevent, detect, handle, mitigate, respond to and recover from incidents and acting as their cybersecurity information exchange and incident response coordination hub. Furthermore, CERT-EU is tasked with offering relevant cybersecurity services to Union entities. As part of its mission, ENISA should support also Union entities. In particular, it should do so by engaging through structured cooperation with CERT-EU on capacity building, operational cooperation and long-term strategic analyses of cyber threats. When relevant, ENISA may leverage the structured cooperation with CERT-EU for ENISA cybersecurity services or support that can be of added value to Union entities, in a coordinated manner to ensure synergies of efforts of CERT-EU.

(11) One of the core tasks of ENISA should be to support Member States in implementing Union policy and law regarding cybersecurity consistently, in particular as regards Directive (EU) 2022/2555, Regulation (EU) 2024/2847, and Regulation (EU) 2025/38. To help achieve consistent and effective implementation of the Union cybersecurity acquis, ENISA should issue technical guidance and reports, provide advice and best practices, and facilitate the exchange of best practices between competent authorities to this end. Furthermore, ENISA is assessing the state of cybersecurity in the Union

and adopts a report to that end in accordance with Article 18 of Directive (EU) 2022/2555. ENISA should also be able to respond to requests for advice and assistance by Member States and, where applicable, Union entities, on matters falling within ENISA's mandate.

(12) With a view to stimulating cooperation between the public and private sectors and within the private sector, in particular to support the protection of critical infrastructure, ENISA should support information sharing within and among sectors, in particular the sectors listed in Annexes I and II to Directive (EU) 2022/2555, and information regarding products with digital elements falling within the scope of Regulation (EU) 2024/2847. Such support may take the form of providing best practices and guidance on available tools and procedures, as well as providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral Information Sharing and Analysis Centres (ISACs).

(13) In view of supporting and facilitating the strategic cooperation and the exchange of information, ENISA should contribute to the work of the Cooperation Group established by Directive (EU) 2022/2555 ('NIS Cooperation Group'), in particular by providing expertise, advice and by facilitating the exchange of best practices, among others, in relation to cross-border dependencies, regarding risks and incidents. ENISA should also contribute to the work of the European Digital Identity Cooperation Group established by Regulation (EU) No 910/2014 of the European Parliament and of the Council[46], the European Cybersecurity Certification Group, and the administrative cooperation group (ADCO) established by Regulation (EU) 2024/2847.

(14) 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. Within its mandate, ENISA should support the security and resilience of the public core of the open internet and the stability of its functioning, including, but not limited to, the secure deployment and operation of key protocols (in particular Domain Name System, Border Gateway Protocol, and Internet Protocol version 6) and the operation of the domain name system (such as the operation of all top-level domains), by promoting best practices, guidance, and cooperation, in accordance with established global, multistakeholder Internet governance arrangements and the respective roles and responsibilities of relevant international technical and operational bodies.

(15) ENISA acts as a reference point for advice and expertise on cybersecurity. Therefore, at the Commission's request, ENISA should assist it by means of expertise, technical advice, information, analyses, including feasibility studies, opinions and preparatory work regarding any specific matter in the field of cybersecurity with a view to informing the Commission's policymaking and facilitating the Commission's monitoring of the implementation of Union legislation regarding cybersecurity.

(16) Similarly, taking into account its expertise, ENISA should assist Member States 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

[46] 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, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

information systems. In particular, ENISA should support the development and enhancement of computer security incident response teams ('CSIRTs') provided for in Directive (EU) 2022/2555, with a view to achieving a high common level of maturity of CSIRTs in the Union.

(17) ENISA has supported and should continue supporting Member States in developing and implementing guidelines for their national cybersecurity strategies contributing to the adoption and implementation of cybersecurity strategies by all Member States ENISA should promote the dissemination of such strategies through the National Cybersecurity Strategies (NCSS) Interactive Map and should further follow the progress of their implementation, including by providing support in the development of key performance indicators in this context.

(18) Regulation (EU, Euratom) 2023/2841 has tasked the Interinstitutional Cybersecurity Board with supporting Union entities in elevating their respective cybersecurity postures, and CERT-EU with contributing to the security of the unclassified ICT environment of all Union entities. ENISA, based on its experience in cybersecurity, should support the Interinstitutional Cybersecurity Board and CERT-EU in their tasks in accordance with Regulation (EU, Euratom) 2023/2841, including by contributing to cyber threat analysis, situational awareness, cybersecurity exercises, coordination on incident response and the exchange of know-how and best practices.

(19) Based on ENISA's expertise and to complement the capabilities of national and Union public authorities, ENISA should deliver training using the European Cybersecurity Skills Framework (ECSF) as a basis, in particular to support effective policy implementation, operational cooperation, and awareness-raising.

(20) To ensure synergies with the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres established pursuant to Regulation (EU) 2021/887 of the European Parliament and of the Council[47], ENISA should support them by sharing information about current and emerging risks and cyber threats, including risks and threats regarding information and communications technologies.

(21) The Preparedness Strategy highlights that digital literacy, which relies on acquiring basic digital skills, is essential to empower more resilient citizens in the face of potential crises. However, as highlighted in the Commission Communication on the Union of Skills[48], almost half the adult population does not have basic digital skills despite more than 90% of jobs requiring them. In order to ensure that the current and potential future workforce have the required skills in a rapidly evolving digital environment, and to contribute to the development of the European cybersecurity talent pipeline, ENISA should support cybersecurity awareness-raising activities that aim to attract talent and help informing about the education and skills needed in the area of cybersecurity, such as the European Cybersecurity Challenge. In this regard, ENISA should coordinate cybersecurity competitions, capture-the-flag events and similar practical exercises, as a means of developing cybersecurity skills and fostering

[47] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[48] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, The Union of Skills, COM(2025) 90 final, 5 March 2025.

capacity building across the Union. When carrying out awareness-raising activities, ENISA should ensure that these address the needs of national public authorities and Union entities, as well as the needs of businesses, in particular SMEs, and education and training institutions, by maintaining practical frameworks and trainings such as awareness-raising-in-a-box. ENISA should further develop practical and actionable guidance to support the implementation of Union cybersecurity policy and legislation. ENISA should also strive to provide relevant information on applicable certification schemes, for example by providing guidelines and recommendations.

(22) To support businesses operating in the cybersecurity sector, users of cybersecurity solutions, and to ensure effective the implementation of Title III of this Regulation, 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. Furthermore, to support the users of the EU Cybersecurity Reserve established pursuant to Regulation (EU) 2025/38, ENISA should prepare the mapping of the services needed by such users, and of availability of such services, pursuant to that Regulation.

(23) Cyber threats are a global issue. Closer international cooperation is necessary to improve cybersecurity, including to define common norms of behaviour and common approaches. To that end, ENISA should support Union's cooperation with third countries, with a focus on countries that are candidates for accession to the Union, and international organisations, such as NATO, by providing the necessary expertise and analysis to the Commission and relevant Union entities, where appropriate. ENISA's activities in the international area should always be in line with the priorities of the Union.

(24) To help achieve a high level of cybersecurity in the Union, ENISA should support operational cooperation among Member States, in cooperation with CERT-EU, among Union entities, and between stakeholders. To that end, ENISA's role should be strengthened. ENISA should become a member of the CSIRTs network, contributing to the network information exchange and analysis. ENISA should further 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. ENISA's active support for the work of the CSIRTs network and the European cyber crisis liaison organisation network (EU-CyCLONe) should enable those networks to continue strengthening their maturity level. ENISA's role in supporting such cooperation includes combating threats to the security and integrity of democratic institutions, elections and other processes, and the critical infrastructure on which they depend, in line with the European Democracy Shield: Empowering Strong and Resilient Democracies[49].

(25) To support capacity-building, operational cooperation, and long-term strategic analyses of cyber threats, ENISA should make use of the available technical and operational expertise of CERT-EU through structured cooperation, for example through dedicated arrangements.

(26) In order to strengthen cybersecurity across the Union and ensure a rapid and effective response to cyber threats, ENISA should support Member States at their request, including by providing advice on the improvement of their capabilities to prevent, detect, respond to and recover from incidents, by facilitating the technical handling of

[49] JOIN(2025) 791 final.

significant incidents within the meaning of Directive (EU) 2022/2555, in particular through supporting the voluntary sharing of technical solutions between Member States, or by ensuring that cyber threats and incidents are analysed. ENISA should also assist EU-CyCLONe in preparing reports to the Union's and Member States' political level.

(27) To reduce exposure to foreign interference, supply-chain manipulation, and strategic data exfiltration, ENISA should use within the CSIRTs network and EU-CyCLONe secure communications tools. Building on the Recommendation on the Cyber Blueprint, such tools should be provided by legal entities established or deemed to be established in the Union and controlled by Member States or by nationals of Member States.

(28) To contribute to Union-level preparedness and response in the case of large-scale cybersecurity incidents and crises, ENISA should carry out cybersecurity situational awareness activities.

(29) Access to real-time, verified, reliable cyber threat intelligence (CTI) is crucial for building shared situational awareness in the Union. ENISA, the Commission, CERT-EU and the European Cybercrime Centre (EC3) at Europol have already developed repositories of cyber threat intelligence that are tailored to their specific needs. ENISA and other relevant Union entities should cooperate, voluntarily, to develop repositories of real-time, verified, reliable CTI, and seek synergies to ensure economies of scale and reinforce sound financial management. This work should also include sectoral Union entities such as the EU agency for the Space Programme. They should share only derived analysis, trends, and tactics, techniques and procedures (TTPs), not raw sources, and should respect the independence of entities to manage their own CTI lifecycle in line with their mandates and need-to-know rules.

(30) In order to contribute to a timely and coordinated response, ENISA should be able to issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-CyCLONe, in particular in relation to entities listed in Annexes I and II to Directive (EU) 2022/2555. Information in such early alerts may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, as well as techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information and recommendations on mitigation measures.

(31) In order to maintain trust and not jeopardise information-sharing, it is important for ENISA to apply visible markings indicating the extent to which a document or information it has produced or received may be shared further. Similarly, ENISA should use documents or information it receives for the purposes of carrying out its activities, subject to any limitations by means of a visible marking on further distribution of that information.

(32) To help increase awareness of cyber threat indicators and recommendations on mitigation measures, ENISA should make an early alert service available to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such generic, voluntary early alerts should benefit in particular SMEs, and should be provided in a machine-readable format made publicly available. In any case, such voluntary service is separate from and not related to any public-private partnerships that ENISA may establish or has already established.

(33) To support Union shared cybersecurity 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) 2022/2555, both on a voluntary basis, Europol and CERT-EU. That report should be made available to the Council, the European External Action Service, EU-CyCLONe, the CSIRTs network, the Commission and Europol.

(34) In order to enhance the shared situational awareness of the cyber threat and incident landscape among stakeholders, ENISA should analyse trends in cyber threats and incidents. This should include a regular analysis addressing the sectors of high criticality and other critical sectors listed in Annexes I and II to Directive (EU) 2022/2555, including the healthcare, energy and transport sectors. Such analysis should include maturity levels of sectors and identify, among others, possible challenges specific to a given sector. Where relevant, and in order to identify supply chain effects, the analysis should evidence cyber threats and trends related to product categories covered by Regulation (EU) 2024/2847. ENISA should develop expertise in the field of cybersecurity of infrastructures and their critical supply chain dependencies, in particular to support the sectors listed in Annexes I and II to Directive (EU) 2022/2555 and the implementation of Regulation (EU) 2024/2847. To this end, ENISA should also cooperate, where appropriate, with other relevant Union entities.

(35) Further, to understand better the challenges in the area of cybersecurity, ENISA needs to analyse current and emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity. In order to ensure easier access of the public to information on cybersecurity risks and possible remedies, ENISA may provide relevant information on its website, in a user-friendly and well-structured manner.

(36) ENISA's strengthened role in fostering situational awareness, analysing threats and providing technical advice will contribute to enhance collective cybersecurity efforts concerning products with digital elements and support the implementation of Regulation (EU) 2024/2847. In accordance with Regulation (EU) 2024/2847, ENISA may propose joint activities to market surveillance authorities for checking compliance of products with digital elements and identify categories of products with digital elements for which sweeps may be organised. Information stemming from cyber threat analysis and early alerts should strengthen the support that ENISA provides to those authorities and contribute to an effective enforcement of Regulation (EU) 2024/2847 to prevent supply chain effects of cyber attacks across the internal market and enhance the overall Union's preparedness.

(37) Ransomware attacks are a prominent cybersecurity threat to the Union. To boost the Union's cybersecurity and combat ransomware, ENISA should develop capabilities for situational awareness and support for incident response and recovery. When assisting individual essential and important entities in responding to and recovering from a ransomware attack, ENISA should closely cooperate with Europol and with CSIRTs or competent authorities as applicable, thereby drawing from Europol's established experience in fighting ransomware crime. Such assistance should complement CSIRTs' activities supporting incident response. To achieve synergies in its work against ransomware, ENISA should establish a helpdesk and, for that

purpose, it could pool relevant capabilities and counter-ransomware services and make easily available information, guidance, and tools that can help essential and important entities respond to and recover from a ransomware incident.

(38) ENISA should provide technical expertise and support to the Commission in preparing an annual rolling programme of Union-level cybersecurity exercises in accordance with the Recommendation on the Cyber Blueprint to prepare for cyber crises, to test the level of cybersecurity of entities participating in such exercises, and to minimise duplication of effort. ENISA should, for example, advise on the appropriate types of exercise, such as tabletop, hybrid or full live, as well as objectives, scenarios and participation.

(39) Access to correct and timely information about vulnerabilities and a robust vulnerability management are imperative for ensuring a high level of cybersecurity in the internal market. For that reason, ENISA should maintain a European vulnerability database pursuant to Directive (EU) 2022/2555 and create a common Union vulnerability management service capacity, ensuring a resilient and sustainable service level and reducing the risk of disruptions. To that end, ENISA should explore possibilities to deepen structured cooperation with programmes, registries or databases similar to the European vulnerability database, in order to avoid a duplication of efforts and to seek complementarity on an international level, where appropriate. Furthermore, ENISA should support multi-party coordinated vulnerability disclosure at Union level and provide value added services, such as vulnerability advisories, severity scoring and product lists, as well as providing an enhanced European known exploited vulnerabilities catalogue to help entities in their vulnerability management.

(40) The role of ENISA in the development of the ECCF should be a key aspect of its mandate. ENISA should provide its technical expertise throughout the lifecycle of European cybersecurity certification schemes. In view of a future scheme, ENISA should identify existing standards or technical specifications that can underlie such as a scheme and, where relevant, draft technical specifications itself that can be referenced in a scheme. ENISA should be in charge of preparing candidate scheme following a Commission request. For schemes already in place, ENISA should be responsible for their maintenance. In doing so, ENISA should contribute to building and developing a certification ecosystem where the feedback of Member States and private stakeholders is sought and their certification capacities are reinforced. This should also include operating a dedicated certification website where relevant information related to adopted schemes, including certificates and statements of conformity, is freely and publicly accessible.

(41) To support the implementation of relevant Union legislation, ENISA should shape the state of the art in cybersecurity by delivering technical specifications to support the implementation of relevant Union legislation, including in view of their potential referencing in European cybersecurity certification schemes. ENISA should also monitor the creation and evolution of standards by relevant standardisation bodies with a view to following standardisation trends at European and global level, and whenever needed, shape such standards by participating to, including through drafting contributions, and leading in the activities of standardisation organisations. In doing so, ENISA should remain impartial. For instance, there might be situations, where ENISA should withdraw from relevant activities in standardisation bodies if ENISA is asked to assess European standards that were requested by the Commission in support of Union legislation. ENISA should not contribute to the drafting of the standards that it is in charge of assessing.

(42) To support the implementation of Union policies and preparation of potential standardisation activities, ENISA should contribute to the development and evaluation of cryptographic algorithms, in particular in the area of post-quantum cryptography. In that context, upon request by the Commission and subject to a contribution agreement as defined in Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council[50], ENISA may establish a process to solicit and evaluate algorithms for cryptographic algorithms by relevant stakeholders, in particular the cryptographic, academic and research communities, as well as manufacturers, CSIRTs, national cybersecurity certification authorities and competent authorities pursuant to Directive (EU) 2022/2555. Where ENISA contributes to establishing such processes, it should promote collaboration between the relevant stakeholders and implement the organisational aspects. The process should be formal, open, transparent and inclusive, including consultation of relevant stakeholders on draft minimum requirements and the evaluation process and evaluation criteria, notably for security and performance of evaluations.

(43) To support the implementation of conformity assessment activities under European cybersecurity certification schemes and other relevant Union legislation, ENISA may provide relevant technical testing tools to support Member States, businesses and conformity assessment bodies in evaluation activities. Such tools should aim to create synergies at Union level and an efficient operation of conformity assessment procedures to meet the needs of Member States and market needs. Such needs may arise for instance in the area of security by design to support businesses, including small and medium-sized enterprises, in their implementation efforts in the context of Regulation 2024/2847. In this context, ENISA should levy fees to cover relevant costs related to establishing, designing, developing, maintaining and updating needed software and hardware capabilities for such testing tools.

(44) To support Member States in their efforts to address the shortage of cybersecurity professionals and the growing need for a skilled, diverse, including with regards to gender balance, and agile workforce, and to enable labour mobility and preparedness across Member States, ENISA should build on the principles and work initiated under the Cybersecurity Skills Academy. In particular, ENISA should establish the European Cybersecurity Skills Framework ('ECSF') as a common framework on cybersecurity professional role profiles. ENISA should further support Member States in addressing gender disparities in cybersecurity roles. This approach is consistent with the vision outlined in the Commission Communication on the Union of Skills and would contribute to its objectives. A quality label for European individual cybersecurity skills attestations should further be explored.

(45) The ECSF should be a practical and flexible tool to be used on a voluntary basis that provides a common understanding and terminology of the relevant roles and associated tasks, skills and knowledge mostly required in cybersecurity roles, with a view to supporting the identification of critical skill sets, including transversal skills, required for the workforce, and enabling learning providers, including companies, higher education institutions or vocational education and training providers, to design programmes, and help policymakers to develop initiatives to address skills gaps. Having the potential to be used as a reference framework for skills recognition, it

[50] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (OJ L, 2024/2509, 26.09.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

should also be interoperable with the European classification of skills and occupations (ESCO) in order to support human resources departments to understand the requirements for resource planning, recruitment, and career development in support of cybersecurity needs. Whereas DigComp 3.0 describes knowledge, skills and attitudes that are needed to be digitally competent for daily life, participation in society, working and learning, and can be used by both adults and children, the ECSF offer a simple framework identifying cybersecurity roles and associated tasks, knowledge, skills needed to perform them. In this regard, it addresses a specialised audience in cybersecurity, ranging from actually or potential cybersecurity professionals, education institutions to employers. The ECSF should also support the development of European individual cybersecurity skills attestations by being the key instrument used to develop the schemes, allowing the emergence of new market players and supporting market competition within a common framework. The ECSF should be evaluated and updated on a regular basis to ensure that it adequately reflects the cybersecurity labour market's needs, technological and policy developments. ENISA should support the uptake of the ECSF by and within Member States and Union entities, and provide adequate support where such assistance is required.

(46) Cybersecurity skills and qualifications should be made comparable, transparent and trusted across the internal market. To this end, European individual cybersecurity skills attestations[51] should support employers, including SMEs and startups, to recruit actual or potential cybersecurity professionals in an effective manner within and across Member States, in line with the objectives set out in the Communication on the Union of Skills. To ensure consistent implementation across Member States, European individual cybersecurity skills attestations should be based on a common understanding, at Union level, of the skills needed to meet those objectives and should be delivered by providers authorised by ENISA against a common set of criteria. This approach should be consistent with and contribute to the objectives of the future Skills Portability Initiative.

(47) The development of European individual cybersecurity skills attestation schemes should aim to supplement Member States' actions by offering the possibility to public authorities and economic actors to make use of a European attestation mechanism, in line with the supporting competence of the Union in the area of education and vocational training, as referred to in Article 6, point (e) and Articles 165(1) and 166(1) TFEU. The schemes, together with the work of the Cybersecurity Skills Academy, can also represent the basis for the higher education programmes, such as sectoral European degrees and for the development of micro-credentials. Therefore, the European individual cybersecurity attestation schemes should not aim to harmonise law and regulations in Member States, but rather be considered as an enabler and an opportunity which Member States and economic actors may wish to take up and promote.

(48) ENISA should ensure that European individual cybersecurity skills attestation schemes remain close to market needs and build on experience from both public and private providers of individual certifications, including Member States, higher education institutions, vocational education and training institutions and businesses.

[51] European individual cybersecurity skills attestations should be understood as following a similar approach to what the market recognises as 'cybersecurity certifications'. However, in order to avoid confusion with regards to the European Cybersecurity Certification Framework, the expression 'attestation', already used in the communication on the Cybersecurity Skills Academy, is preferred.

ENISA should consult the Commission on prioritisation of the European individual cybersecurity skills attestation schemes, taking into due consideration policy implementation and market needs.

(49) To ensure alignment between the ECSF and the schemes, revision of an ECSF role profile should automatically trigger an evaluation of fitness of the associated European individual cybersecurity skills attestation scheme or schemes, which may lead to their review.

(50) Taking into consideration the diversity of cybersecurity role profiles and associated tasks, skills and knowledge, the assessment of individuals and assessment methods may have to be adapted in each European individual cybersecurity skills attestation scheme. Each scheme should ensure that the assessment of an individual's required skills in terms of learning outcomes, including, where relevant, the evaluation of the level of proficiency, is systematically evaluated against an ECSF role profile or subset thereof. Assessment methods may include elements such as testing theoretical knowledge, practical examination, prerequisites and peer assessment. Experience of individuals should be duly taken into consideration.

(51) In order to ensure a consistent implementation of European individual cybersecurity skills attestation schemes, in particular with regard to the assessment of individuals, ENISA should provide obligatory training to personnel in charge of carrying out the assessment of individuals. Such personnel should have experience in the field of cybersecurity which could be demonstrated by holding a European individual cybersecurity skills attestation for the role profile they are conducting the assessment for and at a proficiency level at least equivalent to that of the individuals they are assessing.

(52) The role of the authorised attestation providers is to attest the knowledge and competences of an individual to be able to perform one of the ECSF roles and to give assurance to the employers across the Union. As also employers operating Unions critical infrastructure would look at the assurance of the quality of skills and competences of individuals acquiring European individual cybersecurity skills attestation, the authorised providers attesting the level of skills and competences should be trustworthy from the cybersecurity point of view and should not be subject of the undue influence by a third country that may pose cybersecurity concerns. Therefore, entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation or controlled by such third country, by an entity established in such third country, or by a national of such third country (high-risk suppliers) in accordance with this Regulation should not be eligible to become authorised attestation providers of any European individual cybersecurity skills attestations pursuant to Title II, Section 4.

(53) To ensure that individuals that hold a European cybersecurity skills attestation can easily use and share it, and that such an attestation can be used across Member States, authorised attestation providers should ensure that electronic attestations of the European individual cybersecurity skills attestations are issued to the European Digital Identity Wallet (EUDI wallet) established by Regulation (EU) No 910/2014 at the request of the individual. Authorised attestation providers should be considered as trust service providers and subject to the supervisory and liability regime laid down in Regulation (EU) No 910/2014. The scheme for the attestation of attributes used

pursuant to Commission Implementing Regulation (EU) 2025/1569[52] should be registered in the catalogue of schemes for the attestation of attributes provided for in that Implementing Regulation.

(54) To contribute to the development of the cybersecurity workforce and the portability of skills across the Union, ENISA should make the European individual cybersecurity skills attestation schemes and the list of authorised attestation providers available to the public via a dedicated website.

(55) ENISA should be governed and operated taking into account the principles of the Common Approach on Union decentralised agencies adopted on 19 July 2012 by the European Parliament, the Council and the Commission[53]. The recommendations in the Common Approach should also be reflected, as appropriate, in ENISA's work programmes, evaluations of ENISA, and ENISA's reporting and administrative practice.

(56) In order for the Management Board to perform its functions effectively, particularly in guiding the overall direction of ENISA's activities and setting its strategic priorities, it is essential for the Board to consist of high-level representatives from Member States and the Commission. To that end, each Member State should appoint the head of a national competent authority of that Member State responsible for cybersecurity designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as a member of the Management Board.

(57) To ensure that alternates in the Management Board can fulfil their roles adequately, Member States should appoint alternates that have appropriate professional expertise and experience. The Commission and the Member States, as regards alternates, should make efforts to achieve a balanced representation between men and women on the Management Board and should limit their turnover in order to ensure continuity of the Management Board's work.

(58) To enable ENISA to fulfil its mission effectively, the Management Board, composed of the representatives of the Member States and of the Commission, should establish the general direction of ENISA's operations, including its strategic priorities, 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 and 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, decide on the extension and termination of the Executive Director's term of office, and decide whether to create a function of Deputy Executive Director and, if such a function is created, on their appointment, and the extension and termination of their term of office. Any person exercising an executive function within ENISA should therefore be appointed by the Management Board. The Management Board should also be responsible for appointing or dismissing members of the Board of

---

52 Implementing regulation - EU - 2025/1569

53 Common Approach, annexed to the Joint Statement of the European Parliament, the Council of the EU and the European Commission on decentralised agencies, adopted on 19 July 2012 and available at: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

Appeal, as well as establishing rules to prevent or manage conflicts of interest in this respect.

(59) To help ensure that ENISA establishes its strategic priorities and maintains them up to date, the Management Board should hold at least one meeting per year dedicated to the strategic priorities of ENISA. To ensure that meetings of the Management Board are effective and well-informed, the Management Board may invite to its meetings any person whose opinion could be pertinent and of interest to the topics discussed to provide insights, expertise or advice. Such a person would be an *ad hoc* observer without voting rights.

(60) The Management Board should adopt decisions by an absolute majority of its members with voting rights, unless otherwise provided for in this Regulation. Due to the importance of budgetary and human resources matters, in particular matters on the annual budget, annual activity report, the anti-fraud strategy, implementing rules giving effect to Staff Regulations, the appointment of the Executive Director, the Deputy Executive Director and the accounting officer, follow-up to findings of the European Anti-Fraud Office (OLAF) and of the European Public Prosecutor's Office (EPPO), and the adoption of the financial rules of ENISA, the Management Board should adopt such decisions only if the representative of the Commission casts a positive vote. For the purposes of taking a decision on adopting a final single programming document after taking into account Commission's opinion, a positive vote of the representative of the Commission should only be required on the elements of the decision not related to the annual and multiannual work programme of ENISA.

(61) 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. It should also assist and advise the Executive Director in implementing Management Board decisions.

(62) 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 Management Board should appoint the Executive Director from the list of candidates prepared by the Commission, following an open and transparent procedure that respects the principle of gender balance.

(63) The Executive Director should prepare a proposal for ENISA's single programming document, after prior consultation with the Commission, and should take all steps necessary to ensure the proper implementation of that single programming document. 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 socio-economic 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. Setting up of an *ad hoc* working group might also be necessary for maintenance activities in relation to specific adopted European

cybersecurity certification schemes. *Ad hoc* working groups should also be set up to develop and maintain European individual cybersecurity skills attestation schemes and assist the Agency in the governance, implementation and evolution of the ECSF. 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 entities and the private sector, including industry, users, and academic experts in network and information security, as well as academic experts in products with digital elements.

(64) The Management Board may decide to create a function of a Deputy Executive Director to assist the Executive Director, where the Management Board considers that such a function is necessary to ensure or maintain the smooth functioning of ENISA. When deciding on whether to create that function, the Management Board may take into account the opinion of the Executive Director.

(65) ENISA should have an Advisory Group 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. Representatives of national and Union law enforcement, data protection and market surveillance authorities should be eligible to be represented in the ENISA Advisory Group.

(66) Applicants to become authorised attestation providers or to renew their authorisation should have access to the necessary remedies where they are affected by decisions taken by ENISA. Therefore, an appropriate appeal mechanism should be set up so that related decisions of ENISA can be challenged before a Board of Appeal, the decisions of which can be subject to judicial review by the Court of Justice of the European Union in accordance with the Treaties. The requirement to exhaust the appeal procedure within ENISA before bringing an action before the Court of Justice of the European Union is only applicable to the persons that have standing before the Board of Appeals.

(67) In order to guarantee the full autonomy and independence of ENISA and to enable it to perform its tasks, ENISA should be granted a sufficient and autonomous budget primarily funded from a contribution from the Union, but also from contributions from third countries participating in ENISA's work, and from fees paid by authorised attestation providers and by conformity assessment bodies participating in schemes and issuing European cybersecurity certificates and EU statements of conformity. The host Member State, and any other Member State, should be allowed to make voluntary contributions to ENISA's budget. No contribution, whether financial or in kind, received by ENISA from Member States, third countries, or other entities or persons should compromise its independence and impartiality. The Union budgetary procedure should be applicable as far as the Union contribution and any other subsidies chargeable to the general budget of the Union are concerned. The Court of Auditors should audit ENISA's accounts to ensure transparency and accountability. In order to enable the Agency to participate in all relevant future projects, it should be given the possibility to receive grants.

(68) To ensure ENISA's capacity to respond to demand for the activities it carries out, in particular as regards decisions to authorise providers to deliver European individual cybersecurity skills attestations, and as regards the maintenance of the European cybersecurity certification schemes and of testing tools, ENISA should be given the power to levy fees. Fees associated with processing of applications to become an authorised attestation provider should be appropriately determined to sufficiently contribute to covering the estimated costs of developing and maintaining the European individual cybersecurity skills attestation schemes and evaluating whether requirements and obligations to become and remain an authorised attestation provider are and continue to be met. Fees associated to the costs of issuing and renewing authorisations to authorised attestation providers should include costs associated to evaluations performed by or under the supervision of ENISA. Fees associated with the participation in European cybersecurity certifications schemes and for the issuance of certificates under such schemes should be appropriately determined to sufficiently contribute to covering the estimated costs of maintaining such schemes. The payment of such fees should enable notified conformity assessment bodies and, where applicable, certificate holders under a scheme to take part in such activities as well as relevant capacity building and promotional activities to promote the exchange of best practices and foster the uptake of schemes and certified solutions.

(69) To ensure proportionality, transparency and legal certainty, fees should be set in a transparent and fair manner. All expenditure of ENISA attributed to staff involved in activities subject to fees, in particular the employer's pro-rata contribution to the pension scheme, and costs related to the Board of Appeal, should be reflected in that cost. Fees must not lead to the imposition of unnecessary financial or administrative burdens on applicants. Reasonable deadlines should be set for the payment of fees.

(70) It is necessary to put in place a set of indicators to measure the Agency's workload, effectiveness and efficiency in relation to activities financed through fees. Having regard to these indicators, the Agency should adapt its staff planning and management of resources related to fees to be able to adequately respond to such demand and to any fluctuations in revenue from fees.

(71) To identify and correctly manage the risk of actual or perceived conflict of interests, ENISA should have rules in place regarding the prevention and the management of conflicts of interest. ENISA should also apply the rules on access to documents set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council[54]. The processing of personal data by ENISA should be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council[55]. ENISA should comply with the provisions applicable to the Union entities, and with national legislation regarding the handling of information, in particular sensitive non-classified information and European Union classified information (EUCI).

---

54 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, ELI: http://data.europa.eu/eli/reg/2001/1049/oj).

55 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(72) When performing its tasks, ENISA may have access to sensitive information, such as information regarding cyber threats and incidents. Therefore, it is essential for ENISA to preserve the confidentiality of information it handles. In particular, in line with Article 339 of the Treaty on the Functioning of the European Union (TFEU), officials and other servants of ENISA should not disclose any information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components, even after their duties have ceased.

(73) 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, relevant Union entities, including CERT-EU, EC3 at Europol, the ECCC, the European Defence Agency (EDA), the European Union Agency for the Space Programme (EUSPA), 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 entity involved in cybersecurity. ENISA should also liaise with competent authorities under Directive (EU) 2022/2555, market surveillance authorities and 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.

(74) Europol has an important role in preventing and combating cybercrime, including cybercrime related to network and information security incidents. To create synergies between the respective tasks of each Agency, ENISA should cooperate with Europol, in particular by sharing information regarding trends in techniques, demands and impacts of ransomware attacks. Such cooperation may also consist in identifying the most common ransomware strains targeting entities listed in Annexes I and II to Directive (EU) 2022/2555 to support essential and important entities in incident response and recovery.

(75) To support operational cooperation and shared situational awareness of cyber threats and incidents, it is essential for ENISA to cooperate with stakeholders and in particular companies and organisations from the private sector, with which ENISA may establish public-private partnerships.

(76) To effectively meet the goals outlined in this Regulation, ENISA may collaborate in particular with academic institutions that have research initiatives in relevant fields, and develop appropriate channels for input from consumer organisations and other organisations.

(77) Given the borderless nature of cyber threats and incidents, the level of cybersecurity and preparedness of third countries may impact entities in the Union. Therefore, ENISA should be able to provide capacity-building activities, including training, capacity-building, twinning activities in third countries, and in particular tailored capacity-building activities for countries that are candidates for accession to the Union or other partner countries in accordance with the Union priorities. Such activities should be conducted following a specific request to provide adequate support, taking into account the priorities of the Union, and be implemented through special arrangements, including through contribution agreements as referred to in Regulation (EU, Euratom) 2024/2509. The European cybersecurity certification framework aims to protect against cyber threats such as maliciously exploited cybersecurity

vulnerabilities or cybersecurity incidents affecting the functionality (design and operation) of ICT products, ICT services, ICT processes, managed security services, or cyber posture of entities. By focusing on technical risks related to ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, the ECCF should complement the security of ICT supply chains framework, which aims to ensure a harmonised approach at Union level to address non-technical risks in sectors of high criticality and other critical sectors.

(78) It should be possible for Member States to have recourse to European cybersecurity certification in the context of public procurement in accordance with Directive 2014/24/EU of the European Parliament and of the Council[56].

(79) To facilitate simplification of compliance for entities, the ECCF should provide for the possibility to certify their cyber posture. Entities, notably those providing multiple types of services across several Member States, may face different cybersecurity and data security-related obligations under horizontal instruments, such as Regulation (EU) 2016/679 of the European Parliament and of the Council[57] and Directive (EU) 2022/2555 of the European Parliament and of the Council[58], as well as sector-specific instruments. In order to streamline the implementation of the overall cybersecurity regulatory framework and facilitate compliance therewith, it should be possible for Union legislation to provide for the possibility of entities to demonstrate their compliance with cybersecurity risk-management requirements through a European cybersecurity certification certificate. A relevant scheme could contribute to streamlining compliance requirements arising from different regulatory instruments, without prejudice to their specific certification requirements. Such simplification measures have the potential to reduce administrative burden, unlocking resources to strengthen the operational cybersecurity preparedness of entities in critical sectors of the Union.

(80) European certification of cybersecurity risk-management requirements developed within the ECCF should enable entities to demonstrate compliance with relevant Union legislation where a scheme covers the respective legal requirements laid down in such an act and where it provides so. On that basis, a Union legal act may also provide for a presumption of conformity with those requirements. Such schemes could contribute to improving the coherent implementation of cybersecurity requirements of Union legislation to level the playing field across Member States and ease the compliance burden.

(81) The European cybersecurity certification framework should provide for the possibility to certify ICT processes, defined as a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service. A protection profile is an example of an ICT process, as specified under Commission Implementing Regulation (EU)

---

[56] 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, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

[57] 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

[58] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

2024/482[59]. Another example of an ICT process is the set of activities undertaken by a manufacturer to securely design and develop an ICT product, including the physical, logical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the design and implementation of an ICT product in its development environment. The certification of such activities is often referred to as 'site certification' in the context of a certification process under Commission Implementing Regulation (EU) 2024/482.

(82) The definition of managed security services in this Regulation should be consistent with that of managed security service providers in Directive (EU) 2022/2555. Those services consist of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, and have gained increasing importance in the prevention and mitigation of incidents. Accordingly, the providers of those services are considered to be essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555. Managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. However, managed security service providers have themselves also been the target of cyberattacks and pose a particular risk because of their close integration in the operations of their customers. It is therefore necessary that essential and important entities within the meaning of Directive (EU) 2022/2555 exercise increased diligence in selecting managed security service providers.

(83) European cybersecurity certification schemes are relevant to a wide community of stakeholders, such as providers of ICT solutions, conformity assessment bodies and users. To promote wide stakeholder engagement, the European Cybersecurity Certification Assembly ("the Assembly") should be organised at least once a year with the aim to foster collaboration between the Commission, ENISA, Member States and relevant stakeholders. It will play a pivotal role in identifying and addressing new cybersecurity challenges and strategic priorities for certification, and ensuring that certification schemes facilitate the secure integration of digital technologies and are fit for users' needs. The Assembly should foster Union leadership in certification activities and uphold the certification framework's ability to deliver trust for businesses, public authorities, and the public.

(84) The Commission should maintain a dedicated website to ensure transparency by publishing up to date information on the implementation progress of the ECCF. The website should include information related to certification schemes under preparation, strategic priorities for upcoming certification schemes, requests to ENISA to prepare candidate certification schemes and information on adoption of certification schemes. The Commission website will complement ENISA's website on European cybersecurity certification schemes, which should offer comprehensive details on the technical preparation of candidate schemes and of the maintenance of schemes, focusing on issued European cybersecurity certificates and EU statements of conformity.

---

[59] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(85) In order to enhance the dialogue between the Union institutions and to contribute to a formal, open, transparent and inclusive consultation process, the Commission should take into account elements arising from the views expressed by the European Parliament and by the Council and the European Cybersecurity Certification Assembly when evaluating this Regulation.

(86) Feasibility studies conducted by ENISA should help to prepare for the planning and development of cybersecurity certification schemes. The studies should incorporate the perspectives of relevant stakeholders and align the future certification schemes with ongoing research, development, and technological assessment activities, recognising, in particular, the contributions of Union and Member State research initiatives. Such studies can help to identify available standards and technical specifications. They should be carried out upon request from the Commission, or in accordance with the Union strategic priorities to ensure that the evolving technological landscape and cybersecurity needs are adequately addressed and reflected when requesting and developing schemes.

(87) The design of the candidate scheme and its coverage of security objectives and elements should be commensurate to the subject matter and scope of the certification object. For example, a certification scheme of cloud services might therefore address security objectives which are relevant for ICT services and organisational security. As another example, a security objective related to not including known exploitable vulnerabilities will likely not be relevant to certification of ICT processes.

(88) In order to ensure that European cybersecurity certification schemes are implemented in a harmonised manner across Member States, it is necessary to provide for rules on the maintenance of the schemes. Maintenance activities are also necessary to ensure that the schemes and their supporting documentation remain up-to-date, especially in a cybersecurity field where the threat landscape and technologies constantly evolve. Certification schemes should therefore be designed and maintained in a way that avoids the risk that they are quickly outdated. Maintenance activities should typically involve drafting and updating supporting documentation, including technical specifications and guidelines, as well as identifying standards or technical specifications that are relevant to the scheme. The analysis of the functioning of the scheme, its potential shortcomings and necessary improvement, should also be part of the maintenance activities. In addition, maintenance activities should include information sharing between Member States with regard to on the implementation of the schemes and contributions to peer review and peer assessment mechanisms.

(89) Due to the technical nature of the maintenance activities, ENISA should manage such activities, in cooperation with the Commission and with the support of the European Cybersecurity Certification Group (ECCG) and its relevant sub-group on maintenance. The establishment of the ECCG sub-group on maintenance allows gathering technical contributions and insights from Member States with a view to harmonising approaches.

(90) Maintenance activities should entail interactions with relevant stakeholder groups to ensure that schemes remain market-relevant and up to date, including by sharing and receiving technical contributions. Such stakeholder groups can be standardisation organisations, conformity assessment bodies, vendors, users, public authorities, or trade associations. The specificities of each scheme, including their corresponding technical forums and industries, imply that it should be possible for technical contributions to be gathered in different ways from one scheme to the other. For some

schemes, ENISA should be able to rely on an ad hoc working group that gathers experts from the public administrations of the Member States, Union entities, and the private sector. Technical contributions could also come from ISACs or standardisation organisations. ENISA should analyse which format is most suitable for each scheme and include a maintenance strategy in each candidate scheme.

(91) European cybersecurity certification schemes should rely on standards or technical specifications, notably for the definition of security requirements and evaluation methodologies. ENISA should be given the possibility to draft technical specifications to support the preparation and maintenance of schemes, in particular where deliverables from standardisation organisations are missing or not suitable to fulfil the objectives of the scheme. As part of the drafting process, ENISA should be supported by the ECCG and, where applicable, the ad hoc working group set up for the relevant scheme. ENISA should also seek contributions from stakeholder groups. Additionally, ENISA should consider market acceptance, as well as European and international standards. Taking into account the quality of the technical specifications and the objectives of the scheme, it should be possible for the Commission to reference technical specifications drafted by ENISA in a European cybersecurity certification scheme.

(92) Technical specifications developed by ENISA and referenced in a scheme should be made available on the ENISA website on European cybersecurity certification schemes so that all interested parties can access them. However, in some specific cases, publication on the website could pose a risk to the cybersecurity of certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities and by extension to public safety. For example, technical specifications could contain precise information on new attack paths whose public availability would make it possible for malicious actors to use them. This type of information should be distributed in a restricted manner on a need-to-know basis to relevant stakeholders, such as national cybersecurity certification authorities, conformity assessment bodies and vendors being certified. Due to their restricted distribution, such technical specifications should not be referenced in European cybersecurity certification schemes and, therefore, should be of non-binding nature.

(93) The cyber posture certification schemes should be designed in a modular way, with a view to allowing demonstration of compliance and the presumption of conformity with relevant cybersecurity requirements set out in other Union legislation, where that legislation provides for that possibility. The presumption of conformity with the requirements of these legal acts will therefore only take effect as a possible avenue to demonstrate compliance if the respective legal acts enable such presumption of conformity. The details of such a scheme, namely purpose, objectives or elements will therefore likely differ from those of other schemes. In particular, schemes for the certification of cyber posture of entities should be developed to provide for assessment of continuous conformity of an entity with Union legislation. It is therefore not necessary that cyber posture certification schemes cover all elements of the European cybersecurity certification schemes, such as assurance levels, and this should be reflected in the rules for the schemes.

(94) A framework for cyber posture certification in the ECCF, allows for developing a scheme that enables entities providing services across several Member States to demonstrate compliance with the cybersecurity risk-management obligations laid down in Directive 2022/2555 of the European Parliament and of the Council. On that basis, with the ability to demonstrate compliance, entities can benefit from more

coherent and less burdensome supervisory approaches across the internal market. The development of such a certification scheme should be facilitated by the adoption of implementing acts under Directive (EU) 2022/2555. Through extension profiles, a cyber posture certification scheme may demonstrate compliance with requirements where a Member State adopted or maintained provisions ensuring a higher level of cybersecurity in line with Directive (EU) 2022/2555. On this basis, an entity providing services across several Member States can demonstrate compliance with all relevant extension profiles through a single European cybersecurity certificate.

(95) The security objectives and the security requirements set out in European cybersecurity certification schemes for what pertains to product security should be consistent with the essential cybersecurity requirements set out in Annex I to Regulation (EU) 2024/2847. This coherence is necessary to ensure that manufacturers whose products fall within the scope of Regulation (EU) 2024/2847 do not face contradictory requirements when certifying their products under a European cybersecurity certification scheme. Furthermore, consistency of requirements facilitates the presumption of conformity by Article 27 of Regulation (EU) 2024/2847 whereby manufacturers of products with digital elements that have been certified under a European cybersecurity certification scheme can benefit under certain conditions from presumption of conformity with the essential cybersecurity requirements set out in Annex I to that Regulation.

(96) Within the European cybersecurity certification scheme, it should be possible to specify an extension profile, by setting out additional or specific requirements for use cases, including additional capabilities such as enhanced product features, specialised service offerings or assets, optimised processes, and advanced security measures. Since extension profiles do not correspond to a specific assurance level, they should describe their purpose in detail, including the security threats addressed. Extension profiles are intended in particular to demonstrate compliance with specific standards and regulatory requirements, including, where applicable, requirements as regards additional cybersecurity risk-management measures laid down by a Member State following the minimum harmonisation principle in line with Directive (EU) 2022/2555.

(97) Without prejudice to the general peer review system to be put in place across all national cybersecurity certification authorities within the ECCF, it should be possible to include in the European cybersecurity certification schemes a peer-assessment mechanism for the bodies that issue European cybersecurity certificates for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities, in particular for those bodies that issue certificates with an assurance level ‘high’ under such schemes. Such bodies should also include certification bodies of the national cybersecurity certification authorities issuing certificates at assurance level ‘high’. 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.

(98) Crises such as wars, natural disasters, and pandemics might negatively impact certification activities. In crisis scenarios of this nature, it might not be feasible, for example, to ensure site security due to infrastructure destruction, cyberattacks, personnel unavailability, and the inaccessibility of the site. A European cybersecurity certification scheme should therefore specify temporary rules on continuity of certification activities during such scenarios.

(99) Translating technical candidate schemes into implementing acts requires complex technical and legal knowledge and can create significant administrative burden. Moreover, certain elements of European cybersecurity certification schemes, such as vulnerability management or the conditions under which such marks or labels may be used, are cross-sectoral and may benefit from harmonised reference provisions. To ensure the quality of adopted European cybersecurity certification schemes and reduce compliance burden for businesses, the Commission should be empowered to adopt model provisions covering certain elements of European cybersecurity certification schemes.

(100) In order to ensure the consistency of the European cybersecurity certification framework, it should be possible within a European cybersecurity certification scheme to specify assurance levels for European cybersecurity certificates and EU statements of conformity issued under that scheme. A European cybersecurity certificate should refer to one of the assurance levels: 'basic', 'substantial' or 'high', while the EU statement of conformity should only refer to the assurance level 'basic'. The assurance levels should provide the corresponding rigour and depth of the evaluation of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity and should 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.

(101) 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, ICT processes, managed security services or the context of the certification of entities. Accordingly, the assurance level should be commensurate with the level of risk associated with the intended use of the ICT product, ICT service, ICT process, managed security services, or the operational environment and nature of the entity the cyber posture of which is subject to certification.

(102) 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, ICT process, managed security service or cyber posture of an entity by the conformity assessment body. Where the certification includes ICT processes, the process used to design, develop and maintain an ICT product, ICT service, managed security service or cyber posture of an entity 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, ICT processes or managed security services, or the entity whose cyber posture of which is subject to certification, has carried out a self-assessment of the compliance of the ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with the certification scheme.

(103) 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, ICT process, managed security service or cyber posture of an entity with its technical documentation.

(104) 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 against elaborate cyberattacks performed by persons who have significant skills and resources. Conformity assessment activities should be performed in the European Economic Area for assurance level 'high' or where a scheme is designed to demonstrate compliance and provide for presumption of conformity with other Union legislation. This requirement is justified by the fact that assessment activities taking place outside the European Economic Area give rise to additional threats to cybersecurity, in particular the intellectual property of the evaluated ICT products, ICT services, ICT processes, managed security services or entities. For instance, the source code of an ICT product could be scrutinised when crossing the border of a third country, which constitutes a risk to intellectual property. Additionally, testing laboratories established in third countries do not operate in an environment that is concerned by the cybersecurity measures mandated by EU legislation, such as Directive (EU) 2022/2555 or Regulation (EU) 2024/2847. For instance, a testing laboratory may rely on a third-party cloud service provider which do not abide to the cybersecurity requirements of Directive (EU) 2022/2555. Nevertheless, a certification scheme should be allowed to provide for derogation mechanisms for instance related to site certification or in other instances where conformity assessment activities cannot be reasonably performed in the European Economic Area.

(105) In some cases, different approaches to meet security objectives of a given assurance level might be required to address specifics of an ICT product, ICT service, ICT process, managed security services or cyber posture of entities. To allow for a more granular approach, it should be possible in a European cybersecurity certification scheme to specify one or several evaluation levels corresponding to one of the assurance levels. This will enable development of schemes where multiple evaluation levels designed for a different purpose will correspond to the level of security associated with a specific assurance level.

(106) European cybersecurity certification schemes should be allowed to provide for a conformity assessment to be carried out under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entity the cyber posture of which is certified ('conformity self-assessment'). In such cases, it should be sufficient that the manufacturer, provider or entity the cyber posture of which is certified, carries out all of the checks itself to ensure that the ICT products, ICT services, ICT processes, managed security service or cyber posture of an entity conform with the European cybersecurity certification scheme. Conformity self-assessment should be considered to be appropriate for ICT products, ICT services, ICT processes, managed security service or cyber posture of entity that are of low complexity, that present a low risk to the public and that have a simple design or simple production mechanisms.

(107) Where a European cybersecurity certification scheme allows for both conformity self-assessments and certifications of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, in such a case, the certification scheme should provide for clear and understandable means for consumers or other users to differentiate between self-assessed and third-party certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.

(108) The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, or the entities the cyber posture of which is certified, 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, ICT process, managed security service or the cyber posture of an entity 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, ICT processes or managed security services, or the entity the cyber posture of which is certified, assumes responsibility for the compliance of the ICT product, ICT service, ICT process, managed security service or the cyber posture of the entity with the security 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.

(109) Manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, or entities the cyber posture of which is certified, should make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity 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 and in line with applicable Union legislation. The technical documentation should specify the requirements applicable under the scheme 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, ICT service, ICT process or managed security service, or cyber posture of the entity complies with the requirements applicable under the scheme.

(110) European cybersecurity certificates and EU statements of conformity should help users make informed choices. Therefore, relevant information should be published on a website maintained by ENISA. Furthermore, 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 user. All users should have access to information regarding the reference number of the certification scheme, the issuing authority or body, and, where applicable, the assurance level, or should be able to obtain a copy of the European cybersecurity certificate. That information should be regularly updated and made available on a dedicated website on European cybersecurity certification schemes. Furthermore, in order to ensure continuous accessibility, manufacturers and providers should be required to notify the relevant certification body if the location of the online or, where relevant, physical information changes.

(111) A conformity assessment is a procedure for evaluating whether specified requirements relating to an ICT product, ICT service, ICT process, managed security service or entity 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, ICT processes or managed security services that are being certified, nor the entity the cyber posture of which is being assessed. A European cybersecurity certificate should be issued following the successful evaluation of an ICT product, ICT service, ICT process, managed security service or cyber posture of the entity. A European cybersecurity certificate should be considered to be a confirmation that the evaluation has been properly carried out.

(112) The strict separation of the supervisory and certification activities is important to avoid distortions and interferences that may be caused in situations where the entity supervising the market is also competing in the same market. Consequently, activities

where the national cybersecurity certification authorities merely carry out their supervisory role, such as by providing prior approval to the issuance of a certificate, should not require further internal separation from other supervisory activities. This includes, for example, a situation where the national cybersecurity certification authority actively gathers information throughout the certification process carried out by private conformity assessment bodies and then gives its opinion on the issuance of the certificate by those bodies ('prior approval model').

(113) European cybersecurity certification schemes should specify the conditions under which ICT products, ICT services, ICT processes, managed security services or cyber posture of an entity may need to be recertified or under which the scope of a specific European cybersecurity certificate may need to be reduced. Furthermore, European cybersecurity certification schemes should take into account any possible adverse effects of any subsequently detected vulnerabilities or nonconformities concerning the certified ICT product, ICT service, ICT process, managed security service or cyber posture of an entity with regard to conformity with the security requirements of that certificate.

(114) Harmonisation plays a crucial role in ensuring robust cybersecurity and enhancing market access for businesses. In contrast, fragmentation and the lack of mutual recognition of certificates pose significant barriers to the seamless flow of data, thereby increasing operational costs for Union industry. To mitigate those challenges, it is essential to avoid fragmentation both in the scope of the security controls and in the conformity assessment methods throughout the Union.

(115) Member States should inform the Commission and the ECCG sufficiently in advance before adopting new national cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities in order to help the Commission and the ECCG evaluate the impact of the new national cybersecurity certification scheme on the proper functioning of the internal market, and in light of any strategic interest in requesting a European cybersecurity certification scheme.

(116) 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, where relevant, Member States should reflect the adoption of a European cybersecurity certification scheme in their national legislation.

(117) With a view to facilitating the growth of a reliable internal market, while also creating partnerships with third countries, the certification process established within the ECCF should be implemented in a manner that facilitates international recognition, mutual recognition and alignment with international standards.

(118) In order to further facilitate trade, and recognising that ICT supply chains are international, mutual recognition agreements concerning European cybersecurity certificates may be concluded by the Union in accordance with Article 218 TFEU. The Commission should be empowered to adopt implementing acts to unilaterally recognise the equivalence of third country certificates with European cybersecurity certificates. It should be possible to provide specific conditions for such recognition of third country certificates.

(119) In order to achieve equivalent implementation of the framework 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, ICT processes, managed security services and cyber posture of entities with European cybersecurity certificates, for monitoring the obligations of manufacturers or providers of ICT products, ICT services, ICT processes, managed security services and certified entities 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'. ENISA should participate in the peer reviews as observer and support the organisation of the peer review mechanism and peer reviews, including by developing relevant guidance documents and templates, in cooperation with the Commission and the ECCG. ENISA should also make publicly available on their website on European cybersecurity certification schemes the information on the schedule of peer reviews and the list of peer-reviewed national cybersecurity certification authorities that are to carry out the schedule. Commission Implementing Regulation (EU) 2025/2540[60], adopted under Regulation (EU) 2019/881 establishes the plan for peer reviews which is being utilised by the adopted European cybersecurity certification schemes. It is necessary to ensure the continuation of the peer reviews. Nevertheless, the Commission should be able, by means of implementing acts, where needed, to establish a new plan for peer reviews of at least five years, as well as to lay down criteria and methodologies for the operation of the peer review system.

(120) Once a European cybersecurity certification scheme is adopted, manufacturers or providers of ICT products, ICT services, ICT processes, managed security services or the entities the cyber posture of which is the subject of certification, should be able to submit applications for certification of their ICT products, ICT services, ICT processes, managed security services or cyber posture 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 the requirements set out in this Regulation, and, where applicable, with the requirements specified by the Commission in accordance with this Regulation. The system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008 of the European Parliament and of the Council[61].

(121) Conformity assessment bodies that have been accredited or notified under existing Union legislation, in particular Regulation (EU) 2024/2847 or Implementing Regulation (EU) 2024/482, might possess competencies that are relevant to newly adopted European cybersecurity certification schemes. To avoid unnecessary financial and administrative burden, it is appropriate to create synergies for the accreditation of conformity assessment bodies under this Regulation. For this reason, the accreditation requirements of the schemes should be established in such a way that there is as much alignment as possible with requirements relating to notified bodies set out in

---

60 Commission Implementing Regulation (EU) 2025/2540 of 9 December 2025 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of the plan for peer review (OJ L 2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

61 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, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Regulation (EU) 2024/2847 and accreditation requirements under Implementing Regulation (EU) 2024/482. In addition, conformity assessment bodies that undergo an accreditation process under this Regulation should be able to rely on previous results of evaluation of their competences under other Union legislation, whenever there is an overlap in the accreditation requirements.

(122) With a view to facilitating harmonised conformity assessment services across the Union, it should be possible to set out in a European cybersecurity certification scheme additional or specific requirements for conformity assessment bodies. In the context of certification, an authorisation should be understood as a decision by a national cybersecurity certification authority that a conformity assessment body meets the specific or additional requirements set out in a European cybersecurity certification scheme, to carry out a specific conformity assessment activity.

(123) Where a European cybersecurity certification scheme sets out additional or specific requirements in accordance with this Regulation, the conformity assessment bodies should be authorised by the national cybersecurity certification authorities to carry out tasks under such scheme. In order to avoid multiple authorisation, to enhance acceptance and recognition of authorisation decisions and to carry out effective monitoring of authorised conformity assessment bodies, conformity assessment bodies should request authorisation by the national cybersecurity certification authority of the Member State in which they are established. Nevertheless, it is necessary to ensure that a conformity assessment body is able to request authorisation in another Member State in the event that there is no national cybersecurity certification authority in its own Member State or where the national cybersecurity certification authority does not have the competence to provide the authorisation services requested. In such cases, appropriate cooperation and exchange of information between national cybersecurity certification authorities should be ensured. The Commission should be empowered to adopt implementing acts establishing the procedures for authorisation, including for cross-border cooperation with regard to authorisation.

(124) In order to safeguard the level of protection required for an ICT product, ICT service, ICT process, managed security service or cyber posture of an entity, it is essential that conformity assessment subcontractors and subsidiaries are required to meet the same requirements as the notified conformity assessment bodies in relation to the performance of conformity assessment tasks. Accordingly, a conformity assessment body should have the appropriate competence and be able to verify that the applicable requirements are met by its subcontractors.

(125) The extent to which the conformity assessment body intends to rely on subcontractors established outside the Union, or have access to personnel or facilities outside the Member State of notification should be appropriately assessed by the notifying authority. The public authority of a Member State should have the possibility to decide that it cannot take the overall responsibility as a national cybersecurity certification authority for such an arrangement, and to withdraw or limit the scope of the notification.

(126) In order to evaluate the cybersecurity requirements for ICT products, ICT services, ICT processes, managed security services or the cyber posture of entities, accredited conformity assessment bodies should be notified by the national cybersecurity certification authorities to the Commission and the other Member States. Notification of accredited and, where applicable, authorised conformity assessment bodies indicates that those bodies can be trusted in performing evaluation and certification

activities in accordance with this Regulation and the European cybersecurity certification scheme, contributing to the overall reputation of European cybersecurity certification. It is therefore essential to ensure that conformity assessment bodies that have been notified meet their requirements and fulfil their obligations over time, and that the list of notified conformity assessment bodies is kept up to date.

(127) Commission Implementing Regulation (EU) 2024/3143[62] adopted under Regulation (EU) 2019/881 establishes the circumstances, formats and procedures for notifications of conformity assessment bodies which are being utilised by the adopted European cybersecurity certification schemes. It is therefore necessary to ensure the continuation of the notification activities. Nevertheless, the Commission should be empowered to adopt implementing acts to adjust those circumstances, procedures and formats for the notification of conformity assessment bodies. In this context, the Commission should draw on the experience gained in the context of existing schemes, and seek alignment with other relevant Union legislation and frameworks, in particular Regulation (EU) 2024/2847 and the new legislative framework, in view of reducing compliance burden for conformity assessment bodies active under different legal instruments.

(128) Information and communication technology (ICT) supply chains are composed of a linked set of resources and processes between economic operators. ICT supply chains play a crucial role in sustaining societal stability and driving economic activity across the Union. They also play a critical role in enabling the digital infrastructure in the Union and underpin the functioning of Union society and economy. ICT supply chains enable the manufacture, production, distribution, and maintenance of ICT services, ICT systems and ICT products that underpin various critical and highly critical sectors, including healthcare, finance, transportation, telecommunication, energy and customs. The security of the ICT supply chains of those critical sectors may also have impact on the security of defence and military infrastructure, where this infrastructure relies on civilian critical sectors and their ICT supply chains. However, according to the report on the status of the cybersecurity threats issued by ENISA (ENISA Threat Landscape 2025)[63], attacks against supply chains are amongst the five prime threats to cybersecurity showing that attackers actively leveraging indirect pathways through third-party providers and dependencies. Disruption of ICT supply chains can impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society. Cybersecurity preparedness and effectiveness are therefore more essential than ever to the proper functioning of the internal market.

(129) Beyond technical risks which are addressed by Directive (EU) 2022/55 of the European Parliament and of the Council[64], Regulation (EU) 2024/2847 of the

---

62 Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 establishing the circumstances, formats and procedures for notifications pursuant to Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (OJ L 3143, 19.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

63 ENISA Threat Landscape 2025, October 2025.

64 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333 du 27.12.2022, p. 80-152, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj).

European Parliament and of the Council[65] and the European cybersecurity certification Framework established by Regulation (EU) 2019/881, ICT supply chains are increasingly exposed to risks of a non-technical nature. Such non-technical risks may be linked, but not limited, to the jurisdiction to which a supplier of certain components is subject, in particular where a third country or threat actors controlled from that country engage in economic espionage, carry out malicious cyber activities or campaigns against the Union or its Member States, or engages in irresponsible State behaviour in cyberspace. Non-technical risks can also be linked to concealed vulnerabilities or backdoors or potential systemic supply disruptions, in particular in the case of technological lock-in or supplier dependency. For instance, kill switches could be used to negatively impact the availability of communication networks and electricity grids.

(130) The Joint Communication on Strengthening EU economic security[66] underlined the risk of third countries gaining access to sensitive information and data in the Union or its Member States, either as a result of industrial espionage, their supply of hardware or software used in certain products or due to their ownership and control of certain businesses possessing sensitive information and data. It also underlined the risk of the Union's critical infrastructure - including critical transport, space systems, energy and communications infrastructure, in particular those that are identified as strategic to military mobility - being disrupted by foreign actors, which could lead to cascade effects on the Union economy. Disruptions could occur through physical, cyber or hybrid attacks, including the sabotage of entire facilities or their parts or subcomponents. They could also be linked to ICT supply chains, which underly critical components or services to critical infrastructures.

(131) In response to challenges to ICT supply chain security posed by non-technical risks, some Member States have taken regulatory measures, including designation of high-risk suppliers, whilst other Member States are likely to do so. This could lead to further divergence in national approaches, and ultimately to higher vulnerability of some Member States, with potential spill-over effects across the Union. Therefore, it is necessary to harmonise certain aspects related to the non-technical cybersecurity risks to the ICT supply chain. Such intervention at Union level is also justified in view of the need to ensure a high level of cybersecurity across the Union. The provisions on the ICT supply chain security aim to remove such wide divergences among Member States, in particular by setting out rules for risk assessment mechanisms of ICT supply chain security risks at Union level and minimum standards of protection from ICT supply chain risks.

(132) To reduce critical dependencies and vulnerabilities, it is necessary to establish a trusted ICT supply chain framework which should address non-technical risks related to high-risk suppliers and dependencies in sectors of high criticality and other critical sectors. Therefore, it is necessary to provide an objective, risk-based, future-proof and technology-neutral framework at Union level, to identify key ICT assets and provide for a set of proportionate mitigating measures to address the risks.

---

65 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).

66 Joint Communication to the European Parliament and the Council, Strengthening EU economic security, 3 December 2025, JOIN(2025) 977 final.

(133) Cybersecurity risks, including risks related to dependency on high-risk suppliers may be observed in several critical ICT supply chains in the Union, including detection equipment, connected and automated vehicles, electricity supply systems and electricity storage, water supply systems, drones and counter-drones systems, cloud computing services, medical devices, surveillance equipment, space services and semiconductors. For example, vulnerabilities in security detection equipment could grant access to ICT systems allowing malicious actors to manipulate scanners in such a way that prohibited items could be brought through the security checkpoint without being detected, with possibly catastrophic consequences.

(134) This Regulation should not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity for what concerns ICT supply chain security, provided that such provisions are consistent with Member States' obligations laid down in Union law. Such provisions may for instance include imposing stricter mitigation measures as regards the key ICT assets.

(135) In order to identify potential cybersecurity risks affecting specific ICT supply chains, the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 ('NIS Cooperation Group') may assess specific ICT supply chains by means of Union-level coordinated security risk assessments. The Union-level coordinated security risk assessments should look, among others, at the main threat actors, the main threats and vulnerabilities affecting the key ICT assets. The Union-level coordinated security risk assessments should develop a list of risk scenarios and a list of measures to mitigate the risks. Union-level coordinated security risk assessments should be completed within six months. In case of specific urgency, it should be possible to shorten the deadlines.

(136) In cases where the Commission has sufficient reason to believe that there is a significant cyber threat for the security of the Union related to critical ICT supply chains and an action might be necessary to preserve the proper functioning of the internal market, it should without delay consult Member States on the need for mitigating measures and carry out a security risk assessment, taking into account the consultation of the Member States.

(137) Where, as a result of a security risk assessment conducted by the NIS Cooperation Group or the Commission, it appears that a specific third country poses serious and structural non-technical cybersecurity risks to ICT supply chains, the Commission should verify the threat posed by that country. The Commission may initiate such verification also on the basis of other sources such as a public statement on behalf of the Union or a Member States in response to, instances of irresponsible state behaviour in cyberspace that has led to a cybersecurity incident. In order to assess the level of threat, the Commission should take into account elements such as the existence of laws or practices in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited. Another relevant element is the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct security concerns, including about existing practices, the substantiated information about incidents of threat actors operating out of the territory of that country carrying out malicious cyber activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors. The Commission should also take into account information

stemming from Union-level coordinated security risk assessments or reports issued by Member States or international organisations such as NATO.

(138) For the purpose of this Regulation, the notion of control should be understood as the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities The control of entities from a third country posing cybersecurity concerns should also be established in situations where such entity is having executive management structures in that country.

(139) The Union should not fund projects involving high-risk suppliers, which would jeopardise the Union's security and undermine the Union's interests and credibility. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in any Union funding programmes and instruments implemented in direct and indirect management in accordance with the Article 136 of the Regulation (EU/Eurotom) 2024/2509 and Union sector specific rules as well as in any Union funding activities implemented in shared management, including under the next Multiannual Financial Framework in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets. Union implementing partners, such as European Investment Bank Group and national promotional banks and institutions should refrain from supporting projects that contradict the above, including in operations at own risk.

(140) Public procurement can be a strong tool for public authorities to contribute to a more innovative, sustainable and competitive economy and for spending public money in a strategic manner. Public procurement related to ICT supply chains should not be used to benefit suppliers that threaten the security of the Union's critical infrastructure. High-risk suppliers identified under this Regulation should therefore not be entitled to participate in public procurement concerning the provision of ICT components or components that include ICT components to be used in identified key ICT assets.

(141) Cybersecurity certification plays a role in strengthening overall security and countering cyber threats, serving as benchmark of trust. This trust could be eroded if cybersecurity skills attestations were delivered by high-risk suppliers that should therefore not be entitled to apply to become authorised providers of any Union individual cybersecurity skills attestations. In a similar vein, it is also appropriate to exclude high-risk suppliers from obtaining cybersecurity certification under the ECCF, and becoming accredited conformity assessment bodies to deliver such certificates.

(142) Cybersecurity standards play a critical role in the security and trustworthiness of digital infrastructures. It is necessary to take appropriate measures to ensure standardisation in the field of cybersecurity. The involvement of entities established in or controlled from countries which have been identified as posing cybersecurity concerns to the ICT supply chain in line with this Regulation may lead to influencing cybersecurity standards in a way that undermines their security and trustworthiness.

(143) Based on the results of the security risk assessments, the Commission may identify, by means of implementing acts, which ICT assets should be regarded as key ICT assets due to their criticality and subject to specific mitigating measures. The mere existence of the possibility of connectivity of the asset should be sufficient to consider their cybersecurity risk.

(144) Where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, the mitigating measures may be applied to entities in relation to their ICT supply chain and in particular to key ICT assets identified. The proposed

mitigating measures should be based on the assessment of potential risks and dependencies, including the potential economic and societal impact of such measures on the entities concerned operating in highly critical or other critical sectors and in particular SMEs. The economic impact should look at the costs of the implementation of the mitigation measures, including the duration of the lifecycle of the relevant components in the key ICT assets in case where the measures include the replacement of suppliers. The availability of alternative suppliers on the market should also be assessed in order to ensure continued provision of the services.

(145) As mitigating measures could potentially have a restrictive effect on international trade in goods and services, they should be proportionate and targeted to pursue the legitimate objective to ensure the cybersecurity of ICT supply chains in relation to entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555, in line with the Union's international obligations.

(146) Use, installation or any other kind of integration of components provided by high-risk suppliers in the operation of key ICT assets may be related to risks of subsequent transfers of data to a third country. In particular, risks may be posed by an insufficient level of protection offered to the data in the third country, such as for the protection of fundamental rights, intellectual property or trade secrets, or unlawful access and exploitation of that data for possible future supply chain disruptions and espionage purposes. To mitigate such risks, restrictions in relation to transfer of specific types of data to third countries may be applied.

(147) Important vulnerabilities stem from a lack of diversity in equipment used by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. A reliance on a single supplier creates a dependency on specific equipment or solutions. A lack of diversity of suppliers increases the overall vulnerability of critical infrastructure, in particular if entities source their ICT components used in sensitive ICT assets from a supplier presenting a high degree of risk. Dependency also significantly affects national and Union-wide resilience and creates single points of failure. To mitigate such risks, requirements to have more than one supplier for specific key ICT assets may be applied.

(148) Union entities may also be using key assets as defined by this Regulation. Therefore, the rules laid down in this Regulation concerning ICT supply chain security should also be applicable to them. To ensure that the specificity of Union entities is taken into account, it is important to consider non-technical risks stemming from ICT supply chains in regard to Union entities when conducting Union-level coordinated security risk assessments.

(149) In exceptional circumstances justifying an immediate intervention to preserve the proper functioning of the internal market and where there is a clear evidence giving the Commission sufficient reason to consider that the use of ICT components or components that include ICT components from a specific supplier represents a significant cybersecurity threat for the economic or societal activities of at least three Member States, the Commission may propose, in close consultation with Member States, to prohibit the use, installation or integration of such components from this supplier by type of entities referred to in Annexes I and II to Directive (EU) 2022/2555.

(150) In order to ensure proportionality of measures applied, entities established in a third country posing cybersecurity concerns designated in accordance with this Regulation, or controlled by such third country, by an entity established in such third country, or

by a national of such third country can apply to be exempted from the prohibition to provide to entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555 ICT components or components that include ICT components for their use, installation or integration in key ICT assets of that entity and participate in public procurement procedures organised in accordance with legislation transposing Directives 2014/24/EU[67] and 2014/25/EU of the European Parliament and of the Council[68] procedures in relation to the provision of ICT components or components that include ICT components to be used in identified key ICT assets. For that purpose, the entity should demonstrate with clear evidence that it applies effective measures addressing the non-technical risks and ensuring the absence of any possible undue interference by a third country posing cybersecurity concerns.

(151) Electronic communications networks form the backbone for a wide range of services that are essential for the functioning of the internal market and the maintenance and operation of vital societal and economic functions – such as energy, transport, banking, health, defence, as well as industrial control systems. Therefore, those highly critical networks are attractive targets for all types of cyberattacks and hybrid threats, for disruptions, espionage, intelligence gathering, as well as for fraud and financial crime. The risk assessment of the NIS Cooperation Group on the cybersecurity and resiliency of Europe's communications infrastructures and networks identified a number of risks and threats of strategic importance from a Union perspective, such as wiper/ransomware, attacks, supply chain attacks, network intrusions, and Distributed denial-of-service (DDoS) attacks.

(152) In view of the interconnection and interdependence between the different national electronic communications networks, it is necessary that all Member States take appropriate measures to ensure the security of their networks. For the same reasons, there is a need to have in place an effective legal framework at Union level addressing also non-technical risks and ensuring the security of interconnected electronic communications networks in a comprehensive way.

(153) In particular, the cybersecurity of 5G networks is a matter of strategic importance for the Union as those networks form the backbone for a wide range of services of essential importance for the functioning of the internal market and are also key in setting up our defence readiness, including in relation to military mobility. 5G networks are capable of providing reliable ultra-fast connectivity, for example for data and information sharing, detection of drones and real-time battlefield coordination.

(154) 5G deployment consists primarily in non-standalone networks, where only the radio access network is upgraded to 5G technology, while the rest of the network still relies on an existing 4G core network. 5G non-standalone networks builds primarily on infrastructure already in place, meaning that the security of future 5G networks is, to a certain extent, determined by network equipment already in place and the configuration of such equipment. Therefore, mitigating measures should also cover 4G networks on which the 5G deployment relies.

---

67 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, pp. 65–242, ELI: https://eur-lex.europa.eu/eli/dir/2014/24/oj/eng).

68 Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94 du 28.3.2014, p. 243-374, ELI: https://eur-lex.europa.eu/eli/dir/2014/25/oj?locale=fr).

(155) In order to address important security challenges in 5G networks, Member States within the NIS Cooperation Group, together with the Commission and ENISA, carried out a Union-level coordinated security risk assessment of 5G networks, examining both technical and non-technical risks. This assessment identified several risks, including potential interference from third countries or third country actors via the supply chain, and categorised assets according to their criticality. This assessment should be taken as a basis for defining the key ICT assets for 5G communications networks.

(156) To mitigate the risks identified in the Union-level coordinated security risk assessment of 5G networks, the NIS Cooperation Group adopted the EU Toolbox on 5G cybersecurity, setting out strategic and technical measures. Even though a majority of the Member States have legal frameworks that allow for restrictions or exclusions of high-risk suppliers as recommended in the 5G Toolbox, the implementation of those frameworks has not been uniform. This results in an important number of 5G sites across the Union being supplied by high-risk suppliers as referred to in the Commission's communication on the implementation of the 5G Toolbox[69]. This situation creates vulnerabilities, including strategic dependency and potential exposure to third-country interference, which could also affect future 6G infrastructure built on existing 5G networks. The fragmented implementation of the 5G Toolbox recommended measures, particularly regarding the scope of restrictions on high-risk suppliers, has led to divergences between Member States, which results in an unlevelled playing field that divides the internal market and weakens overall network security. The European Court of Auditors has highlighted these disparities, warning that the absence of a coordinated approach undermines the functioning of the internal market. Persistent dependency on high-risk suppliers poses serious risks to the security of critical infrastructure in the Union and could erode trust in the internal market, as inconsistent security levels may discourage consumers and businesses from relying on 5G-based products and services across the Union. It is therefore essential to have Union-level measures to ensure a harmonised approach to the security of 5G networks.

(157) For the purpose of setting up a phasing out period for the key ICT assets of fixed and satellite electronic communications networks, the Commission should carry out an assessment taking due account of the degree of the security risks related to each specific ICT key assets of the fixed and satellite networks, the lifetime of relevant components and the economic impact that the removal of those components would have on the operators concerned. Based on the results of that assessment, the Commission may consider setting up different phasing out periods for the particular key ICT assets and their integral elements.

(158) For the purposes of effective supervision and enforcement of obligations concerning the providers of mobile, fixed and satellite electronic communication networks, the relevant competent authorities under this Regulation should ensure close cooperation with the competent authorities under the [DNA proposal]. Upon request from a competent authority designated under this Regulation, national regulatory authorities or other competent authorities for radio spectrum, where appropriate, should withdraw the rights referred to in Article 9 and Article 20 [DNA Proposal] if the provider of public electronic communications networks is not complying with the obligations under this Regulation, including if the provider does not phase out ICT components or

[69] Communication from the Commission on the implementation of the 5G cybersecurity Toolbox, 15 June 2023, C(2023) 4049 final.

components that include ICT components from high-risk suppliers in the operation of key ICT assets within the period specified in accordance with this Regulation.

(159) In view of the differences in national governance structures, Member States should designate or establish one or more competent authorities responsible for the supervisory and enforcement measures under this Regulation.

(160) The competent authorities should provide support to entities of the type referred to in Annexes I and II o Directive (EU) 2022/2555 for the compliance with their obligations under this Regulation. For that purpose, the Commission should assess whether suppliers that may be affected by specific prohibitions are established in third country posing cybersecurity concerns or controlled by such third country or by an entity established in such third country or by a national of such third country. Competent authorities should cooperate closely with the Commission and other competent authorities within the Network established under this Regulation. Based on the assessment by the Commission, the competent authorities should share relevant information concerning high-risk suppliers with relevant entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Entities are not expected to verify whether a supplier is under foreign control but may rely fully on information received from competent authorities. The competent authorities should ensure that no unnecessary administrative burden is imposed on those entities.

(161) In order to ensure effective compliance, this Regulation should provide for supervisory and enforcement measures through which the competent authorities can supervise entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Where the competent authorities execute their supervisory and enforcement tasks in relation to those entities, they should not go beyond what is necessary and be proportionate to the identified risks.

(162) In order to make enforcement effective and consistent across the Union, it is necessary to provide enforcement powers that competent authorities can exercise for breach of the obligations laid down in this Regulation. When exercising those enforcement powers, the competent authorities should have due regard to a number of factors, including the nature, gravity and duration of the infringement, the material or non-material damage caused, whether the infringement was intentional or negligent, actions taken to prevent or mitigate the material or non-material damage, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The enforcement measures, including penalties, should be proportionate and their imposition should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of defence.

(163) It is important to also provide for the power to impose periodic penalty payments, in order to compel an entity of the type referred to in Annexes I or II to Directive (EU) 2022/2555 to cease an infringement of this Regulation in accordance with a prior decision of the competent authority.

(164) In order to ensure effective enforcement of the obligations laid down in this Regulation, each competent authority should have the power to impose or request the imposition of penalties.

(165) For the purpose of imposing penalties on an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555 that is an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU. Where a fine is imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the penalties. It should be for the Member States to determine whether and to what extent public authorities should be subject to penalties. Imposing a penalty should not affect the application of other powers of the competent authorities.

(166) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission in respect of the adoption of implementing acts laying down detailed rules relating to fees levied by ENISA, implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, implementing acts laying down common principles and reference provisions intended to provide for elements across European cybersecurity certification schemes, implementing acts specifying procedures for prior approval or general delegation models, implementing acts on recognising a third country or international organisation cybersecurity certificates as equivalent to European cybersecurity certificates, implementing acts establishing a plan for peer review, implementing acts to establish the procedures, including on cross-border cooperation, for authorisation of the conformity assessment bodies, implementing acts to establish the circumstances, formats and procedures for notifications of conformity assessment bodies, implementing acts designating a third country as a country posing cybersecurity concerns to ICT supply chains, implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to Annexes I and II to Directive (EU) 2022/2555, implementing acts establishing that entities operating in sectors of high criticality and other critical sectors are subject to specific mitigating measures and specifying the time periods for the phasing out of ICT components or components that include ICT components provided by high-risk suppliers, implementing acts further specifying conditions regarding the exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns, as well as the adoption of implementing acts laying down detailed rules relating to fees levied by the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council, and the examination procedure should be used. In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should also be conferred on the Commission in respect of establishing a list of high-risk suppliers relevant for certain measures provided for in this Regulation.

(167) It is necessary that European cybersecurity certification schemes reflect the latest technological developments, new related threats, and the adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation. For these reasons, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in order to add or modify the security objectives that European cybersecurity certification schemes pursue. Similarly, in the interests of a trusted ICT supply chain framework, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend Annex II to this Regulation in order to adapt it to

technological developments. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts should systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(168) ENISA's operations should be subject to regular and independent evaluation. That evaluation should have regard to ENISA's objectives, and the relevance of its tasks, in particular its tasks relating to the operational cooperation at Union level. 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.

(169) Commission Implementing Regulation (EU) 2024/482 lays down rules as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC). The EUCC is the first and only European cybersecurity certification scheme adopted under Regulation (EU) 2019/881. It concerns the certification of ICT products, including products belonging to the technical domains 'smart cards and similar devices' and 'hardware devices with security boxes', and protection profiles (as ICT processes). It is therefore necessary to ensure the continuation of certification activities as well as of the Agency's activities.

(170) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725[70] and delivered a joint opinion [date].

(171) Regulation (EU) 2019/881 should be repealed.

(172) 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,

HAVE ADOPTED THIS REGULATION:

TITLE I
GENERAL PROVISIONS

Article 1
Subject matter and scope

1. This Regulation lays down:

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

[70] 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(b) a framework for establishing European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, managed security services or the cybersecurity posture of entities 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; and

(c) a trusted ICT supply chain framework.

2. The framework referred to in paragraph 1, point (b) applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.

3. The framework referred to in the first subparagraph point (c) shall apply to public or private entities of a type referred to in Annex I or II to Directive (EU) 2022/2555 which provide their services or carry out their activities within the Union.

4. This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

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) 'Union entities' means Union entities as defined in Article 3, point (1), of Regulation (EU, Euratom) 2023/2841;

(3) 'authorised attestation provider' means an entity, public or private, for which ENISA has adopted a decision authorising that entity to award European individual cybersecurity skills attestations as laid down in a European individual cybersecurity skills attestation scheme;

(4) 'European individual cybersecurity skills attestation' means a record, in digital or physical form, attesting that an individual knows, understands and is able to perform the tasks associated to a role profile or a subset of a role profile of the European Cybersecurity Skills Framework ('ECSF'), following an assessment as laid down in a European individual cybersecurity skills attestation scheme;

(5) 'European individual cybersecurity skills attestation scheme' means a comprehensive set of rules, requirements, standards and procedures established by ENISA and associated to a role profile of the ECSF or a subset thereof, and that apply to and are applied by authorised attestation providers;

(6) 'network and information system' means a network and information system as defined in Article 6, point (1), of Directive (EU) 2022/2555;

(7) 'national cybersecurity strategy' means a national cybersecurity strategy as defined in Article 6, point (4), of Directive (EU) 2022/2555;

(8) ‘incident’ means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

(9) ‘large-scale cybersecurity incident’ means a large-scale cybersecurity incident as defined in Article 6, point (7), of Directive (EU) 2022/2555;

(10) ‘incident handling’ means incident handling as defined in Article 6, point (8), of Directive (EU) 2022/2555;

(11) ‘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;

(12) ‘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, ICT processes, managed security services or cyber posture of entities;

(13) ‘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, ICT processes, managed security services or cyber posture of entities falling under the scope of the specific scheme;

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

(15) ‘EU statement of conformity’ means a document issued by a manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification, stating that the fulfilment of the requirements corresponding to assurance level “basic”, laid down in the European cybersecurity certification scheme, has been demonstrated through conformity self-assessment;

(16) ‘ICT product’ means an element or a group of elements of a network or information system;

(17) ‘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;

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

(19) ‘managed security service’ means a service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing, security audits and consulting, including expert advice related to technical support;

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

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

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

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

(24) ‘standard’ means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[71];

(25) ‘technical specification’ means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;

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

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

(28) ‘conformity self-assessment’ means an action carried out by a manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification, which evaluates whether those ICT products, ICT services, ICT processes, managed security services or cyber posture of entities meet the requirements of a specific European cybersecurity certification scheme;

(29) ‘cyber posture of entities’ means entities’ level of cybersecurity with respect to the specific security requirements;

(30) ‘prior approval model’ means a model whereby a conformity assessment body may issue a European cybersecurity certificate based on the assessment by a national cybersecurity certification authority in the context of a specific certification process under a relevant scheme;

(31) ‘general delegation model’ means a model whereby a conformity assessment body may issue a European cybersecurity certificate based on a delegation of certification activities by a national cybersecurity certification authority;

(32) ‘computer security incident response team’ or ‘CSIRT’ means a CSIRT designated or established pursuant to Article 10 of Directive (EU) 2022/2555.

(33) ‘ICT components’ means ICT products, ICT services or ICT processes that may be used in the operation of ICT assets;

---

[71] 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, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(34) ‘ICT assets’ means software or hardware assets in the network and information systems used by an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555;

(35) ‘key ICT assets’ means ICT assets identified in accordance with Article 102;

(36) ‘electronic communications network’ means electronic communications network as defined in Article 2, point (1), of Regulation (EU) XX/XXXX [DNA proposal];

(37) ‘control’ means the ability to exercise a decisive influence on a legal entity directly, or indirectly through one or more intermediate legal entities;

(38) ‘establishment’ means the effective exercise of activity through stable arrangements in the country where the entity has its central administration or its principal place of business;

(39) ‘high-risk supplier’ means either of the following:

(a) an entity established in a third country posing cybersecurity concerns designated in accordance with Article 100, or controlled by such third country, by an entity established in such third country, or by a national of such third country;

(b) an entity designated in accordance with Article 103(7) and entities controlled by that entity;

(40) ‘ICT supply chain’ means a sum of ICT services, ICT products and ICT processes that encompass activities and actors involved at all stages upstream of a product being made available or a service being delivered on the market;

(41) ‘third country’ means third country as defined in Article 3 (4) of Regulation (EU) 2023/2675 of the European Parliament and the Council[72];

(42) ‘non-technical risk’ means the likelihood of the supplier being subject to influence by a third country with the potential to cause loss or disruption of the service provided or to compromise the product manufactured by an entity or to lead to exfiltration of data, including for the purposes of espionage or revenue generation;

(43) ‘significant non-technical cybersecurity risk’ means a non-technical cybersecurity risk which can be assumed to have a high likelihood to cause an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;

(44) ‘core network functions of mobile electronic communications networks’ means the central architectural element of the mobile electronic communications networks connecting major network nodes to the Internet and managing essential system functions that includes user equipment authentication, lawful interception (LI) functions, security gateways (SeGW) at the network edge, signalling security functions, roaming and session management, user and control plane data transport, access policy management, registration and authorisation of network services, storage of end-user and network data, critical network services including domain name system (DNS), interconnection with third-party mobile networks, exposure of

[72] Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries (OJ L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).

core network functions to external applications, and the selection and management of network slices;

(45) ‘network function virtualisation (NFV) and management and network orchestration (MANO) of mobile electronic communications networks’ means the software and architectural framework ensuring the lifecycle management, orchestration, and automation of virtualised network functions (VNFs), cloud-native network functions (CNFs) and the selection and management of network slices within mobile electronic communications networks;

(46) ‘radio access network (RAN) of mobile electronic communications networks’ means the network connecting the mobile user equipment to the core network, including base stations (eNodeB for 4G, gNodeB for 5G), remote radio heads (RRH) and baseband units (BBU), active antenna systems (AAS), and where applicable, disaggregated RAN components such as centralised units (CU) and distributed units (DU), and the RAN intelligent controller (RIC);

(47) ‘core network functions of fixed electronic communications networks’ means the backbone intelligence of the network, connecting the major nodes and handling a range of essential functions, including user authentication and authorisation (AAA), lawful interception (LI) functions, domain name system (DNS) and IP addressing services (DHCP), access policy management, storage of end-user and network data, IP switching and routing, and international internet gateways (IIG);

(48) ‘network management system of fixed electronic communications networks’ means all centralised platforms and software components necessary for the operation, administration, maintenance and provisioning (OAM&P) of the network and the monitoring of network-related information;

(49) ‘transport and transmission functions of fixed electronic communications networks’ means all components necessary for the backhaul and aggregation of traffic across the network, including optical transport equipment, microwave links and submarine cable systems that include the underwater equipment as well as the submarine line terminal equipment (SLTE) and the physical landing station facilities;

(50) ‘access network of fixed electronic communications networks’ means the network connecting the end-user premises to the aggregation or core network, including the optical line termination (OLT) and the optical network termination (ONT) for fibre networks; coaxial cable modem termination system (CMTS) and cable modems for coaxial cable networks, and fixed wireless access components where used as a fixed line substitute.

TITLE II
THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

Chapter I
Mission and Objectives

Article 3
Mission of ENISA

1. The mission of ENISA is to support Member States and Union entities in achieving a high level of cybersecurity, cyber resilience and trust within the Union.
2. ENISA shall act as a reference point for advice and expertise on cybersecurity for Member States, as well as for other stakeholders in the Union.
3. ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.
4. ENISA shall carry out the tasks assigned to it by Union legal acts.
5. ENISA shall develop its own capabilities, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.

Article 4
Objectives of ENISA

1. ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice, contributions, 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 Member States and, where appropriate, Union entities in implementing horizontal and sectoral Union policies and legislation related to cybersecurity, including market surveillance activities.
3. ENISA shall provide its expertise and assist the Commission in developing Union policies and legislation related to cybersecurity.
4. ENISA shall support capacity-building and preparedness across the Union by assisting Member States, Union entities, through the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) referred to in Chapter IV of Regulation (EU, Euratom) 2023/2841, and public and private stakeholders to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities.
5. ENISA shall contribute to the implementation of the Cybersecurity Skills Academy and the growth of the cybersecurity workforce in the Union by supporting efforts to develop skills portability across the Union, including through the maintenance and uptake of the ECSF and the development, maintenance and uptake of European individual cybersecurity skills attestation schemes in accordance with Chapter II, Section 4 of this Title, and by ensuring the provision of training in accordance with Article 6(8).
6. ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union entities in accordance with Regulation (EU, Euratom) 2023/2841, and relevant private and public stakeholders on matters related to cybersecurity.
7. 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.
8. ENISA shall support operational cooperation at Union level, including by contributing to shared situational awareness of the cyber threat and incident

landscape among Member States and, in cooperation with CERT-EU, among Union entities.

9. ENISA shall closely cooperate with Europol, CSIRTs and other relevant national authorities in order to improve cybersecurity preparedness and response to ransomware incidents.

10. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market.

11. ENISA shall contribute to the harmonisation of the digital single market by engaging in standardisation work relevant for Union policies related to cybersecurity and by developing technical specifications.

12. ENISA shall promote a high level of cybersecurity awareness among organisations and businesses.

Chapter II
Tasks

Section 1
Support for implementation of Union policy and law

Article 5
Support for implementation of Union policy and law

1. ENISA shall contribute to the implementation of Union policy and law by:

   (a) assisting Member States in implementing Union policy and law regarding cybersecurity consistently, including by issuing technical guidance and reports, by providing advice and sharing best practices, and by facilitating the exchange of best practices between competent authorities in this regard;

   (b) supporting information sharing within and between sectors, in particular regarding the sectors listed in Annexes I and II to Directive (EU) 2022/2555 and products with digital elements falling within the scope of Regulation (EU) 2024/2847, by providing best practices and guidance on available tools and procedures;

   (c) at the request of the Commission, assisting Member States by providing support, such as technical guidance, including on cybersecurity risk management measures, tools for cybersecurity maturity assessment, and incident response playbooks, tailored to the sectors listed in Annexes I and II to Directive (EU) 2022/2555 or support for the implementation of secure-by-design principles for products with digital elements in line with Regulation (EU) 2024/2847, with a view to facilitating the improvement of the cybersecurity maturity levels and compliance with Union law regarding cybersecurity;

   (d) contributing to the work of the Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 ('NIS Cooperation Group'), the European Digital Identity Cooperation Group established pursuant to Article

46e(1) of Regulation (EU) No 910/2014, the European Cybersecurity Certification Group ('ECCG') as referred to in Article 90 of this Regulation, and the administrative cooperation group (ADCO) established pursuant to Article 52(15) of Regulation (EU) 2024/2847;

(e) assisting Member States and relevant Union entities in developing and promoting cybersecurity policies related to sustaining the general availability and integrity of the public core of the open internet;

(f) in accordance with Regulation (EU) 2024/2847, providing technical advice and support to Member States and the Commission on matters related to the implementation of that Regulation;

(g) assisting Member States in carrying out mutual assistance and in facilitating such cooperation processes for essential and important entities pursuant to [Article 37a of Directive (EU) 2022/2555];

(h) at the request of the European Data Protection Board, providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy.

2. ENISA shall contribute to coordinated Union level cybersecurity risk assessments, including those carried out pursuant to Article 22 of Directive (EU) 2022/2555.

3. ENISA shall issue guidelines regarding the interoperability of network and information systems used for information-sharing, including with regard to Cross-Border Cyber Hubs as referred to in Article 6(3) of Regulation (EU) 2025/38.

4. ENISA shall be a member of the NIS Cooperation Group pursuant to Article 14(3) of Directive (EU) 2022/2555.

5. At the Commission's request, ENISA shall provide expertise, technical advice, information or analysis or carry out preparatory work on specific cybersecurity matters with a view to informing the Commission's policymaking and monitoring of the implementation of Union legislation.

Article 6
Capacity-building

ENISA shall assist:

(1) 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;

(2) Member States, at their request, in establishing and implementing vulnerability disclosure policies on a voluntary basis;

(3) in accordance with Regulation (EU, Euratom) 2023/2841, CERT-EU and the Interinstitutional Cybersecurity Board in their efforts to support Union entities in strengthening their cybersecurity, improve the prevention, detection and analysis of cyber threats and incidents as well as to improve their capabilities to respond to such cyber threats and incidents;

(4) Member States in developing national CSIRTs, where requested pursuant to Article 10(10) of Directive (EU) 2022/2555;

(5) Member States in developing or updating a national cybersecurity strategy and key performance indicators for the assessment of that strategy, where requested pursuant to Article 7(4) of Directive (EU) 2022/2555, promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices;

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

(7) national 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;

(8) Member States, Union entities and public and private stakeholders in their efforts to assess, grow and enhance the cybersecurity workforce, including by developing, maintaining and promoting the uptake of relevant tools, such as the ECSF and European individual cybersecurity skills attestation schemes in accordance with Section 4 of this Chapter;

(9) relevant public bodies as well as private stakeholders by conducting targeted trainings, where appropriate in cooperation with stakeholders;

(10) the NIS Cooperation Group in the exchange of best practices and information, in particular in relation to the implementation of Directive (EU) 2022/2555 pursuant to Article 14(4), point (c), of that Directive;

(11) the market surveillance authorities designated pursuant to Regulation (EU) 2024/2847 in their activities that aim to ensure the effective implementation of that Regulation, including support for guidance and technical advice to economic operators, support for compliance checks, evaluation of risks, joint activities and sweeps as laid down in Regulation (EU) 2024/2847;

(12) the ECCG members in the exchange of best practices and upon request from individual Member States assist national cybersecurity certification authorities in relation to the implementation of the European cybersecurity certification schemes at national level;

(13) public authorities and private stakeholders in relation to conformity assessment and evaluation activities, including conformity assessment bodies and small and medium-sized enterprises, to support a robust, competitive, inclusive and harmonised conformity assessment ecosystem supporting the implementation Regulation (EU) 2024/2847 and the European cybersecurity certification framework;

(14) the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres established pursuant to Regulation (EU) 2021/887 by sharing information about current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies;

(15) Member States by providing technical support, including for the establishment and operation of regulatory sandboxes in the area of cybersecurity in accordance with relevant Union legislation.

Article 7
Awareness-raising and talent pool

ENISA shall assist Member States in their efforts to raise awareness of Union policies and legislation regarding cybersecurity and promote their visibility by developing actionable tools and guidance. ENISA shall support initiatives aimed at increasing the European cybersecurity talent pool, in particular by coordinating competitions.

Article 8
Market knowledge and analyses

1. ENISA shall carry out and disseminate analyses of the main market trends in the cybersecurity market on both the demand and supply sides, in particular related to the areas where European cybersecurity certification schemes exist or are planned, sectors listed in Annexes I and II to Directive (EU) 2022/2555, and product categories covered by Regulation (EU) 2024/2847, including Annexes III and IV to that Regulation.
2. ENISA shall carry out and disseminate analyses of technological cybersecurity trends in particular in relation to activities and entities falling within the scope of Directive (EU) 2022/2555 and products with digital elements falling within the scope of Regulation (EU) 2024/2847.
3. ENISA shall build knowledge and disseminate technical advice and analyses on state-of-the-art cybersecurity tools, frameworks standards and best practices.

Article 9
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 with third countries and international organisations;

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

(d) providing expert advice and support to the Commission on matters relating to the international recognition of European cybersecurity certificates in accordance with Article 87;

(e) providing expert advice and support to the Commission on matters concerning international standardisation and engaging with relevant international standardisation organisations, where relevant, in collaboration with the ECCG established under Article 90.

Section 2

Operational Cooperation

Article 10
Operational cooperation at Union level

1. ENISA shall support operational cooperation among Member States, Union entities through CERT-EU, and between other stakeholders.

2. ENISA shall be a member of the network of national CSIRTs established pursuant to Article 15(1) of Directive (EU) 2022/2555 and shall provide the secretariat of the CSIRTs network pursuant to Article 15(2) of Directive (EU) 2022/2555.

3. ENISA shall provide the secretariat of the European cyber crisis liaison organisation network (EU-CyCLONe) pursuant to Article 16(2), second subparagraph, of Directive (EU) 2022/2555.

4. ENISA shall support technical and operational cooperation among Member States, in particular through the CSIRTs network and EU-CyCLONe. Such support shall include:

   (a) advising on improvement of capabilities to prevent, detect, respond to and recover from incidents;

   (b) at the request of one or more Member States, providing advice and assessments in relation to a specific potential or ongoing incident or cyber threat, including through the provision of expertise and facilitating the technical handling of such incidents, and through supporting the voluntary sharing of relevant information and technical solutions between Member States;

   (c) analysing vulnerabilities, threats and incidents;

   (d) at the request of one or more Member States, providing support in relation to *ex post* technical inquiries regarding significant incidents within the meaning of Article 23(3) of Directive (EU) 2022/2555;

   (e) contributing to supporting the coordinated management of large-scale cybersecurity incidents and crises at operational level, in particular by assisting EU-CyCLONe in preparing reports to political level and by facilitating timely information sharing between the CSIRTs network and EU-CyCLONe;

5. At the request of a Member State or a Union entity in cooperation with CERT-EU, ENISA shall support consistent public communication relating to an incident or cyber threat.

6. ENISA shall support cooperation among Member States and through CERT-EU among Union entities with regard to the deployment of secure communications tools. ENISA shall use within the CSIRTs network and EU-CyCLONe secure communications tools which are provided by legal entities established or deemed to be established in the Union and controlled by Member States or by nationals of Member States.

Article 11
Shared cybersecurity situational awareness

1. For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape among Member States and among Union entities, ENISA shall:

   (a) develop in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, CERT-EU, Europol and other relevant Union entities,

repositories of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures;

(b) in accordance with Article 12, issue early alerts of a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in particular in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555;

(c) provide timely ad hoc analyses on emerging trends in incidents upon request of the CSIRTs network, EU-CyCLONe, or the Commission;

(d) provide, at the request of Member States or the Commission, analysis or other information regarding an actual or perceived cybersecurity risk or threat;

(e) provide analysis and technical advice regarding cybersecurity risks in products with digital elements, including to support market surveillance and by drawing up a biennial technical report on emerging trends in accordance with Article 17(3) of Regulation (EU) 2024/2847;

(f) prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats, and make the report available to the Council, EU-CyCLONe, the CSIRTs network, the Commission, the European External Action Service and Europol;

(g) monitor trends in techniques, demands and impact of ransomware attacks and provide information about such trends to the Commission, the CSIRTs network and EU-CyCLONe and Europol.

2. For the purposes of an enhanced shared situational awareness of the cyber threat and incident landscape among stakeholders, ENISA shall:

(a) perform analyses of cyber threats, incidents, trends, emerging technologies and their impacts, including a regular analysis addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847;

(b) issue, in cooperation with the Commission, and, where appropriate, the CSIRTs network, 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 Annexes I and II to Directive (EU) 2022/2555;

(c) carry out long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents.

3. ENISA may make the analyses, advice, guidance, best practices and reports referred to in paragraph 2 public, in agreement with the contributing entities referred to in paragraph 2.

4. In carrying out the activities listed in paragraph 1, points (a) to (d) and (f), and paragraph 2, ENISA shall use its own analyses and, as appropriate, the information received in carrying out its tasks, including:

(a) information provided in publicly available sources, including publicly known vulnerabilities in ICT products or ICT services available in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555;

(b) information shared by Member States, Union entities, CERT-EU, private sector or non-governmental partners and third country and international organisations, subject to any limitations by means of a visible marking on further distribution of that information.

5. ENISA shall cooperate closely with the Member States in the preparation of the EU Cybersecurity Technical Situation Report referred to in paragraph 1, point (e). The Report shall be based on publicly available information, ENISA's own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2022/2555, both on a voluntary basis, EC3 and CERT-EU. In agreement with the contributing entities, ENISA may make an aggregated version of the Report publicly available.

Article 12
Early alerts

1. Early alerts referred to in Article 11(1), first subparagraph, point (b), of this Regulation shall contain relevant information concerning a potential or ongoing significant or large-scale incident, or a cyber threat of a potential cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555. Such information may include publicly known vulnerabilities and whether they affect products with digital elements covered by Regulation (EU) 2024/2847, techniques and procedures, indicators of compromise, adversarial tactics, threat actor-specific information and recommendations on mitigation measures.

2. Early alerts referred to in Article 11(1), first subparagraph, point (b), shall be issued as soon as possible to the CSIRT or CSIRTs concerned, and, where appropriate, to the CSIRTs network and EU-CyCLONe.

3. ENISA shall offer an early alert service to entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555.

4. The service referred to in paragraph 3 shall be provided upon a request of the entity and in a machine-readable format made publicly available. That service shall include sharing of information on cyber threat indicators and recommendations on mitigation measures.

5. ENISA shall establish a procedure to disseminate the early alerts to entities referred to in paragraph 3.

Article 13
Support in incident response and review

1. ENISA shall operate and administer the EU Cybersecurity Reserve, in full or in part, in accordance with Regulation (EU) 2025/38.

2. At the request of the Commission or EU-CyCLONe, ENISA, with the support of the CSIRTs network and with the approval of the Member State concerned, shall review and assess significant cybersecurity incidents or large-scale cybersecurity incidents in accordance with Article 21 of Regulation (EU) 2025/38.

3. ENISA shall assist, in cooperation with Europol and CSIRTs or other competent authorities as applicable, individual essential and important entities listed in Annexes I and II to Directive (EU) 2022/2555 in preparing, responding to and recovering from a ransomware incident. For that purpose, ENISA shall establish a helpdesk and in

particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation.

Article 14
Cybersecurity exercises at Union level

1. ENISA shall support the Commission in compiling an annual rolling programme of Union-level cybersecurity exercises
2. ENISA shall maintain a repository of lessons learned from the exercises referred to in paragraph 1 and recommend to Member States and, where relevant, to Union entities how to implement the lessons learned effectively and efficiently.
3. At the request of EU-CyCLONe, the Commission, ENISA shall organise, or contribute to the organisation of, cybersecurity exercises at Union level, including testing preparedness to respond to large-scale cybersecurity incidents and crises at Union level.
4. At the request of Member States, ENISA shall support them in organising national cybersecurity exercises.
5. At the request of CERT-EU, ENISA shall contribute to the organisation of cybersecurity exercises organised by CERT-EU pursuant to Article 13(7) of Regulation (EU, Euratom) 2023/2841.

Article 15
Provision of tools and platforms

1. ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.
2. Where appropriate for the purposes of paragraph 1, ENISA shall cooperate and exchange information with the CSIRTs network and, where applicable, market surveillance authorities.

Article 16
Vulnerability management services

ENISA shall develop a common Union vulnerability management service capacity and provide vulnerability management services to stakeholders by:

(a) maintaining the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555;

(b) providing vulnerability management services to stakeholders, building on the European vulnerability database and making use of relevant information available to ENISA;

(c) where appropriate, entering into structured cooperation with organisations providing programmes, registries or databases similar to the European vulnerability database;

(d) actively supporting the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 with regard to the management of the coordinated disclosure of vulnerabilities which may have a significant impact on entities in more than one Member State;

(e) developing and maintaining methodologies and governance mechanisms for vulnerability identification and coordinated disclosure, in cooperation with national competent authorities, CSIRTs, industry and the research community.

Section 3

Cybersecurity Certification and Standardisation

Article 17
Cybersecurity certification

1. ENISA shall contribute to and promote the development and implementation of Union policy on cybersecurity certification as established in Title III of this Regulation. ENISA shall be in charge of:

   (a) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes, managed security services and the cyber posture of entities in accordance with Article 74 and, where applicable, developing technical specifications in accordance with Article 77;

   (b) maintaining adopted European cybersecurity certification schemes in accordance with Article 75, including in view of a possible review of the adopted European cybersecurity certification schemes in accordance with Article 76;

   (c) promoting the uptake of adopted schemes and maintaining a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity in accordance with Article 79;

   (d) organising capacity-building related to certification processes, evaluation activities, peer review and peer assessment, including by providing support to Member States at their request in accordance with Article 6, point (12).

2. ENISA shall support the Commission in the following activities:

   (a) the governance of the ECCG pursuant to Article 90;

   (b) organising a European Cybersecurity Certification Assembly in accordance with Article 72(1);

   (c) relating to the international recognition of European cybersecurity certificates in accordance with Article 87;

   (d) organising peer reviews pursuant to Article 89;

   (e) preparing model provisions to be referenced in the European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities in accordance with Article 81(5).

Article 18
Standardisation, technical specifications and guidance

1. ENISA shall draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. When drafting those technical specifications, ENISA shall consider existing European and international standards as well as other relevant technical specifications. ENISA shall ensure the consistency of its technical specifications and guidance.

2. ENISA shall monitor and, where relevant, participate and lead in standardisation development activities at Union level and, in accordance with Article 9, at international level, in view of supporting Union policies related to cybersecurity.

3. ENISA shall support the development and evaluation of cryptographic algorithms. Where a cryptographic algorithm is evaluated positively by ENISA, ENISA shall cooperate, in accordance with Regulation (EU) No 1025/2012, with the European standardisation bodies to support its standardisation.

4. ENISA shall provide technical advice to the Commission and, where relevant, the Member States, on appropriate standards or technical specifications in support of Union policies related to cybersecurity, including for Union harmonisation legislation in the field of cybersecurity, in particular Regulation (EU) 2024/2847, technical areas for the purpose of Article 25 of Directive (EU) 2022/2555, and European cybersecurity certification schemes pursuant to Article 81(1), point (d).

5. ENISA shall assist the Commission in the assessment of draft harmonised standards to support the implementation of Union harmonisation legislation in the field of cybersecurity.

6. ENISA shall promote the uptake of European and international standards for cybersecurity.

7. ENISA shall carry out the tasks referred to in paragraphs 1 to 6 with integrity, impartiality and confidentiality, including by withdrawing or pausing its participation from specific technical bodies when such a participation conflicts with other tasks or objectives.

Section 4
Implementation of the Cybersecurity Skills Academy

Article 19
European Cybersecurity Skills Framework

1. ENISA shall develop and make publicly available a European Cybersecurity Skills framework (‘ECSF’). Before making the ECSF publicly available or updating it pursuant to paragraph 4, ENISA shall consult the Commission.

2. The ECSF shall define profiles of cybersecurity professionals and association of specific tasks, skills and knowledge to a given role profile. The use of the ECSF shall be voluntary for public and private entities.

3. ENISA may consult stakeholders in the development and uptake of the ECSF.

4. ENISA shall assess the need to update the ECSF on a regular basis and, where relevant, update it.

Article 20
Development, adoption and maintenance of European individual cybersecurity skills attestation schemes

1. ENISA shall develop, adopt and maintain European individual cybersecurity skills attestation schemes. The use of European individual cybersecurity skills attestation schemes shall be voluntary for national public bodies and private entities, unless otherwise specified by national law.

2. Prior to initiating a new European individual cybersecurity skills attestation scheme, ENISA shall consult the Commission. ENISA shall only adopt such a scheme following a positive opinion from the Commission. When preparing a European individual cybersecurity skills attestation scheme, ENISA may consult relevant stakeholders.

3. A European individual cybersecurity skills attestation scheme shall include the following:

   (a) subject matter and scope of the attestation scheme based on ECSF role profiles or subsets thereof;

   (b) requirements applicable to individuals trained to perform assessments ('assessors') in accordance with Article 21, the necessary skills, knowledge and experience as well as training methods;

   (c) market uptake analysis specific to each attestation scheme;

   (d) the learning outcomes, assessment methods, and conditions that authorised attestation providers shall use to evaluate an individual's demonstration of the required skills in accordance with Article 21;

   (e) where relevant, one or more proficiency levels;

   (f) rules concerning the retention of records by authorised attestation providers;

   (g) the content and the format of the European individual cybersecurity skills attestations, taking into due consideration Article 21(5), point (e);

   (h) maximum period of validity of a European individual cybersecurity skills attestation issued under the attestation scheme.

4. A European individual cybersecurity skills attestation scheme may include the indicative cost of a European individual cybersecurity skills attestation.

5. ENISA shall ensure close cooperation with Member States throughout preparation of the European individual cybersecurity skills attestation schemes.

6. The modification of a European individual cybersecurity skills attestation scheme shall not affect the authorisation granted pursuant to Article 22(3)(a), which shall remain valid for the period it is granted for.

Article 21
Authorised attestation providers

1. Authorised attestation providers shall assess whether individuals meet the requirements of a European individual cybersecurity skills attestation scheme and, where those requirements are met, issue European individual cybersecurity skills attestations. Attestation providers may hold several authorisations, each granted for one European individual cybersecurity skills attestation scheme.

2. ENISA shall provide guidance to and conduct obligatory training of assessors regarding the requirements and assessment methods included in the European individual cybersecurity skills attestation scheme as referred to in Article 20(3), point (b).

3. Entities wishing to become authorised attestation providers or renew their authorisation ('applicants') shall submit an application to ENISA. They shall meet the following requirements:

   (a) they shall have legal personality;

   (b) they shall be capable of carrying out the tasks laid down in this Regulation in relation to European individual cybersecurity skills attestations, regardless of whether the assessment is carried out by the authorised attestation provider itself or on its behalf and under its responsibility;

   (c) they shall have the means necessary to perform the technical and administrative tasks connected with the European individual cybersecurity skills attestation scheme in an appropriate manner and have access to all necessary equipment and facilities.

   For the purposes of the first subparagraph, point (b), 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.

4. Applicants shall not be high-risk suppliers.

5. Authorised attestation providers shall meet the following obligations:

   (a) for the implementation of each European individual cybersecurity skills attestation scheme:

      (i) have at their disposal the necessary assessors and personnel to carry out their activities as established in that scheme in a timely manner;

      (ii) ensure that assessors observe professional secrecy, are impartial and perform their work independently and with the highest degree of professional integrity;

      (iii) have written procedures for carrying out their activities under the scheme that they are authorised for.

   (b) not assess or issue European individual cybersecurity skills attestations to their own assessors;

   (c) ensure, where relevant by putting in place appropriate safeguards, that their assessors can perform their work independently, in particular where such individuals belong to their own structure or are employees or learners of such a structure;

   (d) not engage in any activity that may conflict with the independence of judgement or integrity of their assessors;

   (e) ensure that, at the request of the individual, electronic attestations of European individual cybersecurity skills attestations are issued as electronic attestations of attributes in a format that can be stored in the European Digital Identity Wallets set out in Regulation (EU) No 910/2014.

6. Authorised attestation providers shall immediately inform ENISA if any of the requirements listed in paragraphs 3 and 4 or the obligations listed in paragraph 5, are no longer met or if any doubt that those requirements or obligations are not met, arises, including regarding the independence of assessors.

7. Authorised attestation providers may request a fee from individuals for assessing and issuing the European individual cybersecurity skills attestations, taking into account the indicative cost of a European individual cybersecurity skills attestation pursuant to Article 20(4) and made public on a dedicated website in accordance with Article 23, point (d).

8. Applicants and authorised attestation providers shall allow ENISA to conduct evaluations as part of the application process or maintenance of the authorisation and share all relevant information to ensure the requirements laid down in paragraphs 3 and 4, or the obligations laid down in paragraph 5, are met or continue to be met in accordance with Article 22(2).

Article 22

Examination of applications to become an authorised attestation provider and maintenance of authorisations

1. Applicants shall pay a fee to ENISA for the examination of their application. Authorised attestation providers shall pay a fee to ENISA for the maintenance of their authorisation.

2. ENISA shall evaluate whether the requirements laid down in Article 21(3) and (4) and the obligations laid down in Article 21(5) are met or continue to be met by applicants and authorised attestation providers.

3. After examining an application against the requirements laid down in Article 21(3) and (4), ENISA may issue one of the following decisions:

   (a) granting the applicant the status of authorised attestation provider or renewing it;

   (b) rejecting the application to become an authorised attestation provider or not renewing it;

   (c) closing the processing of the application due to the applicant's inaction following a request for additional information by ENISA.

   ENISA may amend, suspend or revoke such decisions based on its evaluation pursuant to Article 22(2) or in the case referred to in Article 21(6).

4. ENISA shall issue the decision referred to in paragraph 3 within three months from the date of submission of an application in accordance with Article 21(3). Where ENISA requested the applicant for the additional information, ENISA shall issue the decision referred to in paragraph 3 within one month of receiving additional information.

5. The decision referred to in paragraph 3, point (a) shall have a maximum duration of three years and indicate the fee related to the yearly maintenance of the authorisation.

6. ENISA shall ensure that its activities relating to the development and adoption of European individual cybersecurity skills attestation schemes as laid down in Article 20 are strictly separated and carried out independently from the activities on the

examination of applications and on evaluations set out in paragraphs 2 and 3 of this Article.

Article 23
Public information

ENISA shall maintain and regularly update a dedicated website providing public information on:

(a) the ECSF, including the framework and its timeline for update;

(b) the European individual cybersecurity skills attestation schemes, their progress and timelines for their development;

(c) the fees associated with each European individual cybersecurity skills attestation scheme adopted pursuant to Article 47 of this Regulation;

(d) the indicative cost of a European individual cybersecurity skills attestation in accordance with Article 20(4);

(e) the list of authorised attestation providers.

Chapter III
Organisation of ENISA

Article 24
Administrative and management structure of ENISA

The administrative and management structure of ENISA shall comprise:

(a) a Management Board which shall exercise the functions set out in Article 28;

(b) an Executive Board which shall exercise the functions set out in Article 30;

(c) an Executive Director who shall exercise the responsibilities set out in Article 32;

(d) a Deputy Executive Director who shall exercise the responsibilities set out in Article 34;

(e) an ENISA Advisory Group;

(f) a Board of Appeals which shall exercise the functions set out in Articles 39 to 42.

Section 1
Management Board

Article 25
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. The alternates shall represent the members in their absence.

3. Each Member State shall appoint the head of a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as the member of

the Management Board. Where this proves not to be feasible, Member States shall appoint a high-level representative of a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as the member of the Management Board.

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

5. The term of office of the members appointed by Member States shall be equal to the term of their function referred to in paragraph 3.

6. The term of office of the alternates and of the members appointed by the Commission shall be four years. That term shall be renewable.

Article 26
Chairperson of the Management Board

1. The Management Board shall elect a Chairperson and a Deputy Chairperson from among its members with voting rights. The Chairperson and the Deputy Chairperson shall be elected by a majority of two thirds of the members of the Management Board with voting rights.

2. The Deputy Chairperson shall automatically replace the Chairperson if the Chairperson is prevented from attending to their duties.

3. The term of office of the Chairperson and of the Deputy Chairperson shall be four years and may be renewed once. If, however, their membership of the Management Board ends at any time during their term of office, that term of office shall automatically expire on that date.

Article 27
Meetings of the Management Board

1. The Chairperson shall convene meetings of the Management Board.

2. The Executive Director shall take part in the meetings of the Management Board, without the right to vote.

3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, at the request of the Commission, or at the request of at least one third of its members.

4. A representative from the European Cybersecurity Industrial, Technology and Research Competence Centre established by Regulation (EU) 2021/887 shall be a permanent observer, without voting rights, at the meetings of the Management Board.

5. The Management Board may invite any person whose opinion may be of interest to attend a meeting, or part of a meeting, as an *ad hoc* observer, without voting rights and subject to the rules of procedure of the Management Board.

6. 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.

Article 28
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 44, before its submission to the Commission for an opinion;

(c) taking into account the opinion of the Commission, adopt ENISA's single programming document in accordance with Article 29(2), point (a);

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

(e) adopt the annual budget of ENISA in accordance with Article 29(2), point (b), 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 European Court of Auditors; make the annual report public;

(g) adopt the financial rules applicable to ENISA in accordance with Article 50;

(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) ensure adequate follow-up to findings and recommendations stemming from internal or external audit reports and evaluations and from investigations of the European Anti-Fraud Office (OLAF) and of the European Public Prosecutor's Office (EPPO);

(j) adopt its rules of procedure, including rules for provisional decisions on the delegation of specific tasks, pursuant to Article 30(7);

(k) exercise, in accordance with paragraph 2 of this Article, with respect to the staff of ENISA, the powers conferred by the Staff Regulations of Officials of the European Union (the 'Staff Regulations') and by the Conditions of Employment of Other Servants of the European Union (the 'Conditions of Employment'), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68[73], respectively, on the appointing authority and on the authority

[73] OJ L 56, 4.3.1968, p. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

empowered to conclude a contract of employment ('appointing authority powers');

(l) adopt implementing rules giving effect to the Staff Regulations and the Conditions of Employment in accordance with Article 110(2) of the Staff Regulations;

(m) appoint the Executive Director and, if it decides to create the function of a Deputy Executive Director, the Deputy Executive Director, and where relevant extend their term of office or remove them from office in accordance with Article 31;

(n) appoint an accounting officer, subject to the Staff Regulations and the Conditions of Employment, who shall be independent in the performance of their duties;

(o) 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;

(p) authorise the conclusion of working arrangements with regard to Article 68;

(q) authorise the conclusion of working arrangements in accordance with Article 70;

(r) appoint and remove the members of the Board of Appeal in accordance with Article 29(2), point (d);

(s) adopt rules for the prevention and management of conflicts of interest in respect of the members of the Board of Appeal.

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

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 29
Voting rules of the Management Board

1. The Management Board shall adopt its decisions by an absolute majority of its members with voting rights, except if otherwise provided in this Regulation.

2. A majority of two thirds of the members of the Management Board with voting rights shall be required for:

(a) the adoption of the single programming document referred to in Article 28(1)(c);

(b) the adoption of the annual budget referred to in Article 28(1)(e);

(c) the appointment, extension of the term of office or removal of the Executive Director and of the Deputy Executive Director, as referred to in Articles 31 and 33;

(d) the appointment and removal of the members of the Board of Appeal, as referred to in Article 36.

3. Decisions on budgetary or human resources matters, in particular matters referred to in Article 28(1), points (c), (e), (f), (g), (h), (i), (k), (l), (m), (n), shall only be adopted if the representatives of the Commission cast a positive vote. For the purposes of adopting the decisions referred to in Article 28(1), point (c) regarding ENISA's single programming document, a positive vote of the representative of the Commission shall only be required on the elements of the decision not related to the annual and multiannual work programme of ENISA.

4. Each member with voting rights shall have one vote. In the absence of a member with the right to vote, their alternate shall be entitled to exercise the member's right to vote.

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

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

7. 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 30
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 findings and recommendations stemming from internal or external audit reports and evaluations, as well as from investigations of OLAF and the EPPO;

(c) without prejudice to the responsibilities of the Executive Director set out in Article 32, assist and advise the Executive Director in implementing the decisions of the Management Board, with a view to reinforcing supervision of administrative and budgetary management.

3. The Executive Board shall be composed of the Chairperson of the Management Board, one representative of the Commission to the Management Board, and three other members appointed by the Management Board from among its members with the right to vote. The Chairperson of the Management Board shall also be the Chairperson of the Executive Board. 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 without 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. The term of office of members of the Executive Board shall end when their membership of the Management Board ends.

5. The Executive Board shall hold at least one ordinary meeting every three months. In addition, it shall meet on the initiative of its Chairperson or at the request of its members.

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

7. When necessary due to 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 that 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 with voting rights.

Section 3
Executive Director

Article 31
Appointment, dismissal and extension of the term of office

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

2. 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.

3. The Executive Director shall be engaged as a temporary agent of ENISA under Article 2(a) of the Conditions of Employment.

4. For the purpose of concluding the contract with the Executive Director, ENISA shall be represented by the Chairperson of the Management Board.

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

6. 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 for no more than five years.

7. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post at the end of the overall period.

8. The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office in accordance with paragraph 6. 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. The Executive Director may be removed from office only upon a decision of the Management Board acting on a proposal from the Commission.

Article 32
Tasks and responsibilities of the Executive Director

1. The Executive Director shall manage ENISA and shall be accountable to the Management Board.

2. The Executive Director shall be independent in the performance of their tasks and shall neither seek nor take instructions from any government nor from any other body.

3. The Executive Director shall report to the European Parliament on the performance of their tasks when invited to do so. The Council may invite the Executive Director to report on the performance of their tasks.

4. The Executive Director shall be the legal representative of ENISA.

5. The Executive Director shall be responsible for the implementation of the tasks assigned to ENISA by this Regulation. In particular, the Executive Director shall:

   (a) ensure the day-to-day administration of ENISA;

   (b) implement decisions adopted by the Management Board;

   (c) ensure compliance with the financial rules of ENISA;

   (d) prepare the draft single programming document and submit it to the Management Board for approval before its submission to the Commission for an opinion;

   (e) implement the single programming document and report to the Management Board on its implementation;

   (f) prepare ENISA's consolidated annual activity report, including the implementation of ENISA's annual work programme, and present it to the Management Board for assessment and adoption;

   (g) prepare an action plan that follows up on the conclusions of the retrospective evaluations of ENISA as referred to in Article 121, and reporting on progress every two years to the Commission;

   (h) prepare an action plan that follows up on conclusions of internal or external audit reports and evaluations, and from investigations of OLAF and of the EPPO and report on progress biannually to the Commission and regularly to the Management Board;

   (i) prepare the draft financial rules applicable to ENISA as referred to in Article 50;

   (j) prepare ENISA's draft statement of estimates of revenue and expenditure and implement its budget;

   (k) protect the financial interests of the Union by applying preventive measures against fraud, corruption and any other illegal activities, without prejudicing the investigative competence of OLAF and the EPPO, by effective checks and,

if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by imposing effective, proportionate and dissuasive administrative and financial penalties;

(l) prepare an anti-fraud strategy, an efficiency gains and synergies strategy, a strategy for cooperation with third countries or international organisations and a strategy for the organisational management and internal control systems for ENISA, and present it to the Management Board for approval;

(m) develop and maintain contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;

(n) exchange views and information regularly with relevant Union entities regarding their activities relating to cybersecurity to ensure coherence in the implementation of Union policy in that field;

(o) promote diversity and gender balance in the recruitment of ENISA's staff;

(p) adopt European individual cybersecurity skills attestation schemes, as referred to in Article 20(1);

(q) adopt decisions with respect to applicants to become authorised attestation providers or to renew their authorisation, as referred to in Article 22(3);

(r) carry out other tasks assigned to the Executive Director by this Regulation.

6. 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.

7. 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.

8. 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
Deputy Executive Director

Article 33
Deputy Executive Director

1. The Management Board may decide to create a function of a Deputy Executive Director to assist the Executive Director.

2. Where the Management Board decides to create a function of a Deputy Executive Director, the provisions of Article 31 shall apply to the Deputy Executive Director accordingly.

Article 34
Tasks and responsibilities of the Deputy Executive Director

The Deputy Executive Director shall assist the Executive Director in managing ENISA and in carrying out the tasks referred to in Article 32. If the Executive Director is absent or indisposed, or the post is vacant, the Deputy Executive Director shall take their place during the time of absence or until the post is filled.

Section 5
ENISA Advisory Group

Article 35
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. The ENISA Advisory Group shall be composed of recognised experts representing relevant stakeholders, such as the cybersecurity industry, ICT industry, SMEs, entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555, manufacturers of products with digital elements and open-source software stewards within the meaning of Regulation (EU) 2024/2847, conformity assessment bodies notified under the European Cybersecurity Certification Framework referred to in Article 93 and Regulation (EU) 2024/2847, entities operating in the area of electronic identification means, consumer groups, academic experts in the field of cybersecurity, European standardisation organisations, as well as law enforcement and data protection supervisory authorities. Those recognised experts shall be nationals of Member States. 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 and shall be renewable once. Members of the Management Board shall not be members of the ENISA Advisory Group. Experts from the Commission and experts from the Member States shall be entitled to be present at the meetings of the ENISA Advisory Group and to participate in its work. The Executive Director may invite representatives of other bodies that are not members of the ENISA Advisory

Group, 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 for the application of the provisions of Titles III, IV and V 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.

7. ENISA shall provide the logistical support necessary for the ENISA Advisory Group and provide a secretariat for its meetings.

Section 6
Board of Appeal

Article 36
Creation and composition of the Board of Appeal

1. ENISA shall establish a Board of Appeal by a decision of the Management Board.

2. The Board of Appeal shall be composed of a Chairperson and three other members. Each member of the Board of Appeal shall have an alternate. The alternate shall represent the member in their absence.

3. The Management Board shall appoint the Chairperson, the other members and their alternates from a list of qualified candidates established by the Commission. The list of qualified candidates shall be valid for four years. The validity of this list may be extended by the Management Board for additional four-year periods acting on a proposal from the Commission.

4. Where the Board of Appeal considers that the nature of the appeal so requires, it may request the Management Board to appoint two additional members and their alternates from the list referred to in paragraph 3.

5. The Board of Appeal shall adopt and make public its rules of procedure.

Article 37
Members of the Board of Appeal

1. The term of office of the members and alternates of the Board of Appeal shall be four years. Their term of office may be renewed by the Management Board for additional four-year periods acting on a proposal from the Commission.

2. The members of the Board of Appeal shall be independent and shall not perform any other duties within ENISA. In making their decisions they shall neither seek nor take instructions from any government, any other body or any private entity.

3. The members of the Board of Appeal shall not be removed from office or from the list of qualified candidates during their term of office, unless there are serious grounds for such removal and the Management Board takes a decision to that effect, acting on a proposal from the Commission.

Article 38
Exclusion and objection

1. The members of the Board of Appeal shall not take part in any appeal proceedings if they have any personal interest in the proceedings, if they have previously been involved as representatives of one of the parties to the proceedings, or if they participated in the adoption of the decision under appeal.

2. If, for one of the reasons listed in paragraph 1 or for any other reason, a member of a Board of Appeal considers that they should not take part in any appeal proceeding, they shall inform the Board of Appeal accordingly.

3. A party to the appeal proceedings may object to any member of a Board of Appeal on any of the grounds listed in paragraph 1, or if the member is suspected of partiality. Any such objection shall not be admissible if, while being aware of a reason for objecting, the party to the appeal proceedings has taken a procedural step. No objection may be based on the nationality of members of the Board of Appeal.

4. The Board of Appeal shall decide as to the action to be taken in the cases specified in paragraphs 2 and 3 without the participation of the member concerned. For the purposes of taking that decision, the member concerned shall be replaced on the Board of Appeal by their alternate.

Article 39
Appeals against decisions and failures to act

1. An appeal may be brought before the Board of Appeal against:

   (a) decisions adopted by ENISA pursuant to Article 22(3);

   (b) ENISA's failure to act within the applicable time limits laid down in Article 22(4).

2. An appeal brought pursuant to paragraph 1 shall be subject to interlocutory revision in accordance with Article 41 before being put to the Board of Appeal for examination.

3. An appeal brought pursuant to paragraph 1 shall not have a suspensive effect.

Article 40
Persons entitled to appeal, time limit and form

1. Applicants within the meaning of Article 21(3) may appeal against

   (a) a decision of ENISA addressed to them, pursuant to Article 22(3);

   (b) ENISA's failure to act in respect of an application submitted by them to ENISA within the applicable time limits laid down in Article 22(4).

2. In the case referred to in paragraph 1, point (a), the appeal, together with the statement of grounds thereof, shall be filed in writing in accordance with the rules of procedure referred to in Article 36(5) within two months of notification of the decision to the applicant concerned, or, in the absence thereof, of the day on which the decision came to the knowledge of the applicant.

3. In the case referred to in paragraph 1, point (b), the appeal shall be filed with ENISA in writing in accordance with the rules of procedure referred to in Article 36(5) within two months of the day of expiry of the time limit set out in Article 22(4).

Article 41
Interlocutory revision

1. If ENISA considers the appeal to be admissible and well founded, it shall rectify the decision or failure to act referred to in Article 40(1).

2. If ENISA does not rectify the decision within one month after receipt of the appeal, it shall immediately decide whether to suspend the application of its decision and shall refer the appeal to the Board of Appeal.

Article 42
Examination of decisions on appeals

1. The Board of Appeal shall decide within three months of the appeal being filed whether to grant or refuse that appeal. When examining an appeal, the Board of Appeal shall act within the deadlines laid down in its rules of procedure. It shall, as often as necessary, invite the parties to the appeal proceedings to file, within specified time limits, observations on its notifications or on communications from other parties to the appeal proceedings. Parties to the appeal proceedings shall be entitled to make oral representations.

2. Where the Board of Appeal finds that the grounds for appeal are founded, it shall remit the case to ENISA. ENISA shall take its final decision in compliance with the findings of the Board of Appeal and shall provide a statement of reasons for that decision. ENISA shall inform the parties to the appeal proceedings accordingly.

Article 43
Actions before the Court of Justice of the European Union

1. Actions for the annulment of decisions of ENISA adopted pursuant to Article 22(3), or actions for failure to act within the applicable time limits pursuant to Article 22(4), may be brought before the Court of Justice of the European Union, after the appeal procedure within ENISA laid down in Articles 39 to 42 has been exhausted or in the event of failure to act within the applicable time limit pursuant to Article 41(2).

2. ENISA shall take all necessary measures to comply with the judgment of the Court of Justice of the European Union.

Section 7
Operations

Article 44
Single programming document

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

2. Each year, the Executive Director shall draw up a draft single programming document, as referred to in paragraph 1, with the corresponding financial and human resources planning in accordance with Article 32 of Commission Delegated

Regulation (EU) 2019/715[74] 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, taking into account the opinion of the Commission referred to in Article 32(7) of Delegated Regulation (EU) 2019/715. If the Management Board decides not to take into account any elements of the opinion of the Commission, it shall provide thorough justification for that decision. The Management Board shall forward the single programming document 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.

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 multiannual 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 120.

CHAPTER IV
Establishment and structure of ENISA's budget

Article 45
Establishment of ENISA's budget

1. Each year, the Executive Director shall draw up a provisional draft estimate of ENISA's revenue and expenditure for the following financial year, including the establishment plan, and shall send it to the Management Board.

2. The provisional draft estimate shall be based on the objectives and expected results of the annual work programme, and shall take into account the financial resources

[74] Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

necessary to achieve those objectives and expected results, in accordance with the principle of sound financial management and performance.

3. On the basis of the provisional draft estimate, the Management Board shall adopt a draft estimate of ENISA's revenue and expenditure for the following financial year, and shall send it to the Commission by 31 January each year.

4. The Commission shall send the draft estimate to the budgetary authority together with the draft general budget of the Union. The draft estimate shall also be made available to ENISA.

5. On the basis of the draft estimate, the Commission shall enter in the draft general budget of the Union the estimates it considers 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 budgetary authority in accordance with Articles 313 and 314 TFEU.

6. The budgetary authority shall authorise the appropriations for the contribution from the general budget of the Union to ENISA.

7. The budgetary authority shall adopt ENISA's establishment plan.

8. The Management Board shall adopt ENISA's budget. It shall become final following the final adoption of the general budget of the Union, and, if necessary, it shall be adjusted accordingly.

9. For any building project likely to have significant implications for the budget of ENISA, Delegated Regulation (EU) 2019/715 shall apply.

Article 46
Structure of ENISA's budget

1. Estimates of all revenue and expenditure of ENISA shall be prepared each financial year and shall be shown in ENISA's budget. The financial year shall correspond to the calendar year.

2. ENISA's budget shall be balanced in terms of revenue and expenditure.

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

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

   (b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 50;

   (c) Union funding in the form of contribution agreements or *ad hoc* grants in accordance with ENISA's financial rules referred to in Article 50 and with the provisions of the relevant instruments supporting the policies of the Union;

   (d) the fees levied on the applicants for activities related to European individual cybersecurity skills attestation schemes referred to in Article 22(1);

   (e) the fees levied on the conformity assessment bodies for participation in and issuance of European cybersecurity certificates under a European cybersecurity certification scheme referred to in Article 47(2);

   (f) the fees levied on public authorities or private bodies for testing tools as referred to in Article 47(3);

(g) any contribution from third countries participating in the work of ENISA, as provided for in Article 70(4);

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

4. Member States that provide voluntary contributions, as referred to in paragraph 3, point (g) shall not claim any specific right or service as a result thereof.

5. The expenditure of ENISA shall include staff remuneration, administrative and infrastructure expenses, and operational expenditure.

Article 47
Fees

1. In relation to each European attestation scheme activity referred to in Article 22(1), the following fees shall be levied towards applicants within the meaning of Article 21(3) or to authorised attestation providers to contribute to covering the full costs of the activities performed by ENISA:

(a) issuing authorisations following examination of the requirements laid down in Article 21(3) and (4), including conducting evaluations;

(b) yearly maintenance of the authorisation;

(c) renewing authorisations for providers of European individual cybersecurity skills attestations, including conducting evaluations.

2. In relation to certification, the following fees shall be levied on the conformity assessment bodies for the maintenance of European cybersecurity certification schemes under which European cybersecurity certificates are issued, in particular:

(a) an annual fee for the participation in a European cybersecurity certification scheme;

(b) a fee for issuance of European cybersecurity certificates under European cybersecurity certification schemes.

The fees referred to in point b) shall be levied when the conformity assessment body submits European cybersecurity certificates to ENISA for publication on their website pursuant to Article 79.

3. In relation to testing tools referred to in Article 15(1), a fee shall be levied on any public authority or private body for their use.

4. Fees shall be expressed and payable in euro.

5. The Commission shall adopt implementing acts laying down detailed rules relating to determining the fees to be levied by ENISA, specifying in particular the estimated costs attributable to each of the matters for which fees pursuant to paragraphs 1, 2 and 3 are chargeable, and the individual fee amounts chargeable, as well as the ways and conditions under which the fees should be paid. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2). The Commission shall consult ENISA when preparing those draft implementing acts.

6. The fees determined by the implementing acts referred in paragraph 5 shall be set out in advance to be proportionate to the estimated costs of the activities performed or services delivered as determined in a cost-effective way and shall be sufficient to cover those costs. All expenditure of ENISA attributed to staff involved in activities

referred to in paragraphs 1, 2 and 3 shall be reflected in the costs to cover. Fees shall be set at such a level as to avoid a deficit or a significant accumulation of surplus in ENISA's budget. Budgetary surpluses generated through fees shall be carried over to fund activities of ENISA, in particular future activities related to fees, or offset the losses incurred. If a significant positive balance in the budget, resulting from activities covered by fees, becomes recurrent, or if a significant negative balance results from the provision of the services covered by fees, the Commission shall amend the implementing acts referred to in paragraph 5 to revise the method for calculating the fees in accordance with Article 118(2).

The amount of the fees for the tasks referred to in paragraph 1 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the costs of the activities related to the development and maintenance of European individual attestation schemes, the processing of applications and the delivery and renewal of authorisations and the necessary for those oversight activities by ENISA.

The amount of the fees for the tasks referred to in paragraph 2 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the full costs of the activities related to maintaining the European cybersecurity certification schemes set out in Article 75.

The amount of the fees for the tasks referred to in paragraph 3 shall be fixed at such a level as to ensure that the revenue in respect thereof sufficiently contributes to cover the costs of the activities related to the provision of testing tools as set out in Article 15(1).

7. ENISA shall provide a report on the fees levied and their impact on its budget as part of the procedure for the presentation of accounts laid down in Article 50.

8. ENISA shall put in place a set of indicators to measure the workload, effectiveness and efficiency in relation to activities financed through fees. ENISA shall adapt its staff planning and management of resources related to fees accordingly to be able to adequately respond to such demand and to any fluctuations in revenue from fees. ENISA shall share the report with the Commission, which the Commission may use for the purpose of the evaluation referred to in Article 120(1).

Article 48
Implementation of ENISA's budget

1. The Executive Director shall be responsible for the implementation of ENISA's budget and shall act as authorising officer.

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

3. Each year, the Executive Director shall send to the budgetary authority all information relevant to the findings of evaluation procedures.

Article 49
Presentation of accounts and discharge

1. 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).

2. ENISA's accounting officer shall also provide the required accounting information for consolidation purposes to the Commission's accounting officer, in the manner and format required by the latter by 1 March of year N + 1.

3. ENISA shall send the report on the budgetary and financial management for year N to the European Parliament, the Council, the Commission and the Court of Auditors by 31 March of year N + 1.

4. On receipt of the Court of Auditor's observations on ENISA's provisional accounts for year N, ENISA's accounting officer shall draw up ENISA's final accounts on their own responsibility. The Executive Director shall submit them to the Management Board for an opinion.

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

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

7. A link to the web pages containing ENISA's final accounts shall be published in the Official Journal of the European Union by 15 November of year N + 1.

8. The Executive Director shall send to the Court of Auditors, by 30 September of year N + 1, a reply to the observations made in its annual report. The Executive Director shall also send that reply to the Management Board and to the Commission.

9. 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 year N, in accordance with Article 267(3) of Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council.

10. On a recommendation from the Council acting by qualified majority, 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 year N.

Article 50
Financial rules

1. 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) 2019/715 unless such a departure is specifically required for the operation of ENISA and the Commission has given its prior consent.

2. ENISA shall establish and implement its budget in accordance with its financial rules and Regulation (EU, Euratom) 2024/2509.

Article 51
Combating fraud

1. In order to combat fraud, corruption and other unlawful activities, the provisions of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council [75] shall apply without restriction to the activities of ENISA.

2. ENISA shall 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)[76] within six months from *[OP please insert the exact date, as referred to in Art. 127]* and shall adopt the appropriate provisions applicable to its staff using the template set out in the Annex to that Agreement.

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

4. OLAF may carry out investigations, including on-the-spot checks and inspections 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, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96[77].

5. Without prejudice to paragraphs 1to 4, working agreements with third countries and 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 competencies.

6. In accordance with Council Regulation (EU) 2017/1939, the EPPO may investigate and prosecute fraud and other illegal activities affecting the financial interests of the Union as provided for in Directive (EU) 2017/1371 of the European Parliament and of the Council[78].

Article 52
Declaration of interests

1. Members of the Management Board, the Executive Director, the Deputy Executive Director, and officials seconded by Member States on a temporary basis, shall each

---

[75] 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, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

[76] OJ L 136, 31.5.1999, p. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.

[77] 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, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

[78] Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ L 198, 28.7.2017, p. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

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, the Deputy Executive Director, 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 53
Transparency

1. ENISA shall carry out its activities with a high level of transparency and in accordance with Article 55.

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 publicly available the declarations of interest made in accordance with Article 52.

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 54
Confidentiality within ENISA

1. Without prejudice to Article 55, ENISA shall not disclose 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 Deputy 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.

Article 55
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.

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 V
Staff and Liaison Officers

Article 56
General provisions

1. 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.
2. The staff of ENISA, liaison officers and seconded national experts to ENISA shall undergo appropriate security clearance procedure.

Article 57
Privileges and immunities

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

Article 58
Liaison officers

1. Each Member State shall designate at least two liaison officers from a national competent authority designated pursuant to Article 8(1) of Directive (EU) 2022/2555 as seconded national experts to ENISA to work at its seat or its local office, in accordance with Article 59(2). The Commission may also designate a liaison officer.
2. Liaison officers shall contribute to executing the tasks of ENISA, including by facilitating operational cooperation and exchange of information as referred to in Article 11. Liaison officers shall also support ENISA in disseminating information about its activities, findings and recommendations to relevant stakeholders across the Union. They shall also act as national contact points for questions from their Member States and relating to their Member States, either by answering those questions directly or by liaising with their national administrations.
3. Liaison officers designated by their Member States shall be entitled to request and receive all relevant information from their Member States, as provided for by this Regulation, while fully respecting the national law and the Member State's practices, in particular as regards data protection and confidentiality.

Article 59
Seconded national experts and other staff

1. ENISA may make use of seconded national experts or other staff not employed by ENISA, in any areas of its work. The Staff Regulations and the Conditions of Employment shall not apply to such staff.

2. The Management Board shall adopt a decision laying down rules on the secondment of national experts, including liaison officers, to ENISA.

CHAPTER VI
GENERAL PROVISIONS CONCERNING ENISA

Article 60
Legal status of ENISA

1. ENISA shall be a body of the Union with legal personality.
2. In each Member State, ENISA shall enjoy the most extensive legal capacity accorded to legal persons under that Member State's 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 61
Seat

ENISA shall have its seat in Athens, Greece.

Article 62
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 63
Administrative control

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

Article 64
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 disputes overcompensation for damages referred to in paragraph 3.

5. The personal liability of ENISA's staff towards ENISA shall be governed by the provisions laid down in the Staff Regulations or Conditions of Employment applicable to them.

Article 65
Language arrangements

1. Council Regulation No 1[79] 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. Translation and all other linguistic services required for the functioning of ENISA, other than interpretation, shall be provided by the Translation Centre for the Bodies of the European Union.

Article 66
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.

Article 67
Security rules on the protection of sensitive non-classified information and classified information

In agreement with 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[80] and 2015/444[81]. Those security rules shall include provisions for the exchange, processing and storage of such information.

Article 68
Cooperation with Union entities and national authorities

1. To ensure consistency, create synergies and address issues of common concern, ENISA shall cooperate on matters related to cybersecurity with CERT-EU and

---

79 Council Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).

80 Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

81 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, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

relevant Union entities, including Europol, the European Cybersecurity Industrial, Technology and Research Competence Centre established pursuant to Regulation (EU) 2021/887, and the European Data Protection Board established pursuant to Article 68(1) of Regulation (EU) 2016/679.

2. The cooperation referred to in paragraph 1 may be ensured by means of:

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

   (b) the provision of advice and issuance of guidance on matters related to cybersecurity;

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

3. ENISA shall engage in a structured cooperation with CERT-EU, in particular on matters related to capacity-building, operational cooperation, and long-term strategic analyses of cyber threats.

4. ENISA shall cooperate and exchange information with relevant market surveillance and supervisory authorities designated under Union legislation in the field of cybersecurity, including Regulation (EU) 2024/2847.

Article 69
Cooperation with stakeholders

1. Where necessary to achieve the objectives of this Regulation, ENISA shall cooperate with relevant stakeholders, such as the cybersecurity industry, the ICT industry, SMEs, entities operating in sectors listed in Annexes I and II to Directive (EU) 2022/2555, manufacturers, importers or distributors of products with digital elements within the meaning of Regulation (EU) 2024/2847, conformity assessment bodies notified under the European cybersecurity certification framework and Regulation (EU) 2024/2847, entities operating in the area of electronic identification means, consumer groups, and academic experts in the field of cybersecurity. To that end, ENISA may establish public-private partnerships.

2. ENISA shall, in consultation with the Commission, support cooperation between notified conformity assessment bodies pursuant to Article 93. In particular, it may establish a group of notified conformity assessment bodies for sharing of best practices, creating synergies with other relevant Union legislation, in particular Regulation (EU) 2024/2847.

Article 70
Cooperation with third countries and international organisations

1. To the extent necessary to achieve the objectives of this Regulation, ENISA may cooperate with the competent authorities of third countries or with international organisations or both, in line with the priorities of the Union. 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. The Management Board shall adopt a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent and in line with the priorities referred to in paragraph 1. The Commission shall ensure that

ENISA operates within its mandate and the existing institutional framework by concluding appropriate working arrangements with the Executive Director.

3. To support cooperation with third countries, in particular countries that are candidates for accession to the Union, ENISA may deliver its capacity-building expertise, in particular in the following areas:

   (a) assessment of the level of maturity of cybersecurity capabilities and resources;

   (b) growth and enhancement of the cybersecurity workforce, including by promoting the ECSF and the European individual cybersecurity skills attestation schemes, and providing learning and training activities;

   (c) supporting the planning and execution of cybersecurity exercises.

4. ENISA shall be open to the participation of third countries in ENISA's work that have concluded agreements with the Union to that effect. Under the relevant provisions of agreements concluded between third countries and the Union, working arrangements shall be established, subject to prior approval of the Commission, 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 and Conditions of Employment in any event.

5. ENISA shall regularly report to the Council and the Commission on the implementation of the working arrangements referred to in paragraphs 1 and 4.

TITLE III

EUROPEAN CYBERSECURITY CERTIFICATION FRAMEWORK

CHAPTER I
Objectives, Scope and Procedures

Article 71
Objectives and scope of the European cybersecurity certification framework

1. The European cybersecurity certification framework shall be established with a view of creating a digital single market for ICT products, ICT services, ICT processes, managed security services and entities. To that end, it shall increase the level of cybersecurity within the Union and enable a harmonised approach to European cybersecurity certification schemes as well as leverage certification to facilitate compliance with applicable Union legislation.

2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest the following:

   (a) 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 lifecycle;

(b) that managed security services that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and confidentiality of data which are accessed, processed, stored or transmitted in relation to the provision of those services, and that those services are provided continuously with the requisite competence, expertise and experience by staff with a sufficient and appropriate level of relevant technical knowledge and professional integrity;

(c) that the cyber posture of an entity that has been evaluated in accordance with such schemes complies with specified cybersecurity requirements.

3. European cybersecurity certification shall be voluntary, unless otherwise specified in Union or national law.

4. A European cybersecurity certificate and EU statement of conformity issued under the European cybersecurity certification framework shall be automatically recognised in all Member States.

Article 72
Public information and consultation

1. At least once a year, the Commission shall organise, with the support of ENISA, a European Cybersecurity Certification Assembly, inviting ECCG members and other relevant experts from Member States, relevant experts from Union entities and relevant stakeholders to discuss strategic priorities for harmonisation in the area of cybersecurity certification.

2. The Commission shall maintain and regularly update a dedicated website providing information on the following aspects:

(a) European cybersecurity certification schemes requested for development pursuant to Article 73;

(b) strategic priorities for harmonisation of ICT products, ICT services, ICT processes, managed security services, cyber posture of entities or security requirements of Union legislation, including potential areas for which a European cybersecurity certification scheme might be requested.

3. The Commission shall make publicly available on the website referred to in paragraph 2 of this Article the information on its request to ENISA to prepare a candidate scheme as referred to in Article 73 and its decision to accept, reject or discontinue a candidate scheme transmitted by ENISA in accordance with Article 74(7).

4. During the preparation of a candidate scheme by ENISA pursuant to Article 74, the European Parliament and the Council may request the Commission, in its capacity as chair of the ECCG, and ENISA to present relevant information on the draft candidate scheme. Upon the request of the European Parliament or the Council, ENISA, in agreement with the Commission and without prejudice to Article 54, may make available to the European Parliament and to the Council relevant parts of a draft candidate scheme in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner.

5. The European Parliament and the Council may invite the Commission and ENISA to discuss matters concerning the implementation of European cybersecurity

certification schemes for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.

Article 73
Requests for a European cybersecurity certification scheme

1. The Commission may request ENISA to prepare a candidate European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.

2. In duly justified cases, the ECCG may suggest to the Commission to put forward a request referred to in paragraph 1.

3. The request referred to in paragraph 1 shall detail the purpose, scope and modalities of meeting relevant security objectives and elements set out in Articles 80 and 81. The request shall also specify the development plan of the candidate European cybersecurity certification scheme and relevant technical specifications to be referenced or defined in the scheme.

4. When preparing the request referred to in paragraph 1, the Commission shall duly consult ENISA and the ECCG as well as take into account the views of all relevant stakeholders and other Union entities, including, where applicable, those that are relevant under Union legislation in which a European cybersecurity certification scheme is demonstrating compliance and providing presumption of conformity.

Article 74
Preparation and adoption of European cybersecurity certification schemes

1. No later than 12 months after receiving a request from the Commission pursuant to Article 73, unless otherwise specified in the request, ENISA shall prepare a candidate European cybersecurity certification scheme that meets the requirements set out in Articles 80 and 81.

2. For the preparation of each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 32(6) for the purpose of providing ENISA with expertise advice.

3. When preparing the candidate scheme, 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, where applicable, supporting technical specifications.

4. When preparing the candidate scheme, including, where applicable, supporting technical specifications, ENISA shall consult stakeholders in a timely manner by means of a formal, open, transparent and inclusive consultation process. ENISA shall also cooperate with relevant public authorities in the Member States and with relevant Union entities to gather their expert advice in relation to the preparation of the candidate scheme and, where applicable, supporting technical specifications. When transmitting the candidate scheme to the Commission pursuant to paragraph 6, ENISA shall describe the manner in which it has complied with this paragraph.

5. Before transmitting the candidate scheme and, where applicable, supporting technical specifications, to the Commission, ENISA shall request members of the ECCG to provide written opinions on the candidate scheme. The opinions shall be provided no later than 30 days from date of the request. ENISA shall take the utmost account of

the opinions of the ECCG members. The absence of such opinions shall not prevent ENISA from transmitting the candidate scheme to the Commission.

6. ENISA shall transmit the candidate scheme to the Commission no later than 60 days from the date of the request referred to in paragraph 5.

7. When receiving the candidate scheme, the Commission shall evaluate whether the scheme corresponds to the request made in accordance with Article 73. Within 30 days of the date of transmission of that candidate scheme the Commission shall take one of the following actions:

   (a) accept the candidate scheme;

   (b) return the candidate scheme to ENISA for revision together with a justification for this return and a deadline not exceeding 90 days, within which ENISA shall provide a revised candidate scheme;

   (c) discontinue the candidate scheme.

8. Where the Commission returns a candidate scheme to ENISA for revision in accordance with paragraph 7, point (b), paragraphs 4, 5 and 7 shall apply accordingly.

9. The Commission, based on the accepted candidate scheme prepared by ENISA, is empowered to adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that meets the requirements set out in Articles 80 and 81. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 118(2).

10. The Commission may reference technical specifications developed by ENISA in the implementing acts referred to in paragraph 9 of this Article, in accordance with Articles 18 and 77.

11. The Commission may specify the conditions for the international recognition of European cybersecurity certificates, in the implementing acts referred to in paragraph 9 of this Article, in accordance with Article 87.

Article 75
Maintenance of a European cybersecurity certification scheme

1. Each European cybersecurity certification scheme shall establish a maintenance strategy. The maintenance strategy shall outline expectations with regard to maintenance activities, in particular those related to the standards or technical specifications referenced in the scheme and to the interaction with relevant stakeholders.

2. ENISA, in cooperation with the Commission and supported by the ECCG and its relevant maintenance sub-group, shall ensure the maintenance of European cybersecurity certification schemes, including in view of the possible review of such schemes by the Commission. ENISA shall cooperate and exchange information with relevant Union entities and groups in relation to maintenance activities.

3. ENISA may organise the involvement of the private sector for the maintenance of a scheme in the form of an ad hoc working group in accordance with the maintenance strategy referred to in paragraph 1.

4. The maintenance activities of European cybersecurity certification schemes shall include the following:

(a) the preparation, update and endorsement of technical specifications and guidelines to support the harmonised and uniform operation of the schemes;

(b) the identification of standards or technical specifications that are relevant to the scheme;

(c) interactions and, where relevant, the establishment of liaisons, with relevant stakeholders, including European or international standardisation organisations, including for the purpose of making or receiving technical contributions;

(d) the issuance of recommendations to the Commission on necessary improvements and updates to the schemes, including in view of a possible review of the schemes;

(e) the exchange of information related to the practical implementation of the schemes between Member States;

(f) contributions to peer review and peer assessment mechanisms and analyses of the outcome of such assessments to improve the operation of the schemes and support their possible review.

5. The ECCG may issue an opinion on the maintenance of European cybersecurity certification schemes.

Article 76

Evaluation, review and withdrawal of a European cybersecurity certification scheme

1. At least every four years following the entry into application of a European cybersecurity certification scheme, ENISA shall evaluate the impact and effectiveness of that scheme, in cooperation with the relevant maintenance sub-group of the ECCG, and by taking into account the feedback received from stakeholders. ENISA shall conduct the evaluation by carrying out the market analysis in accordance with Article 8(1).

2. Following the evaluation referred to in paragraph 1, the Commission may review or withdraw implementing acts providing for a European cybersecurity certification scheme pursuant to Article 74(9).

3. When reviewing or withdrawing European cybersecurity certification schemes, the Commission shall consult ENISA, the ECCG and its relevant maintenance sub-group, as well as take into account the views of relevant stakeholders and other Union entities.

4. The ECCG may issue an opinion on the review or withdrawal of a European cybersecurity certification scheme. The Commission shall take due account of it when reviewing or withdrawing the European cybersecurity certification scheme.

Article 77

Technical specifications in European cybersecurity certification schemes

1. ENISA may develop technical specifications in view of a future European cybersecurity certification scheme or in support of the maintenance of a European cybersecurity certification scheme.

2. The technical specifications referred to in paragraph 1 of this Article shall be developed in a timely manner, with the support of the ECCG and its maintenance sub-groups and, where applicable, the corresponding ad hoc working group as referred to in Article 75(3). For this purpose, ENISA shall also seek contributions from relevant stakeholder groups taking into account the maintenance strategy referred to in Article 75(1).

3. Where technical specifications are referenced in a European cybersecurity certification scheme as referred to in Article 74(10), they shall be made available on the website referred to in Article 79.

4. In duly justified cases, in particular where the technical specifications contain information that could compromise the security of certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, they shall be distributed only to those stakeholders concerned by the requirements of the scheme. Such technical specifications shall not be referenced in a European cybersecurity certification scheme as referred to in Article 74(10).

Article 78
Facilitation of compliance with Union legislation

1. Where a specific Union legal act so provides, a certificate issued under a European cybersecurity certification scheme shall demonstrate compliance and confer a presumption of conformity with corresponding requirements set out in that legal act.

2. Evaluation activities under a European cybersecurity certification scheme shall be consistent with the corresponding Union legal act setting out the demonstration of compliance and the presumption of conformity. Where such evaluation activities are not specified in the corresponding Union legal act, the scheme shall specify them. A conformity assessment for certification granting the presumption of conformity with requirements set out in Union legislation shall be conducted by a third-party body.

3. In the absence of harmonised Union legislation, national law may also provide that a European cybersecurity certification scheme may be used for demonstrating the compliance and establishing the presumption of conformity with specific legal requirements set out in national law.

Article 79
Uptake of European cybersecurity certification schemes, ENISA website and publication of certificates

1. ENISA shall organise activities to promote the uptake of adopted European cybersecurity certification schemes, including by maintaining the website referred to in paragraph 2 of this Article.

2. ENISA shall maintain and regularly update a dedicated website providing public information on the following:

   (a) European cybersecurity certification schemes;

   (b) the fees associated with the maintenance of each European cybersecurity certification scheme;

   (c) relevant ENISA technical specifications;

(d) European cybersecurity certificates and EU statements of conformity, including information with regard to such certificates and statements which are no longer valid, or which are suspended, withdrawn or expired;

(e) relevant supplementary cybersecurity information provided in accordance with Article 84;

(f) summaries of peer reviews pursuant to Article 89(7);

(g) technical specifications referenced in a European cybersecurity certification scheme pursuant to Article 74(10).

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

CHAPTER II
Content of European Cybersecurity Certification Schemes

Article 80
Security objectives of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall pursue, as applicable, the following security objectives:

(a) to ensure that ICT products, ICT services, ICT processes and managed security services are secure by default and by design;

(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure using appropriate technical means, taking into account the entire lifecycle of the ICT products, ICT services or ICT processes;

(c) to protect the integrity of stored, transmitted or otherwise processed, personal or other data, commands, programmes and configurations against any manipulation or modification not authorised by the user, and report on corruptions, taking into account the entire lifecycle of the ICT products, ICT services or ICT processes;

(d) to ensure protection from unauthorised access by means of appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) to identify and document components and vulnerabilities, including, where appropriate, by drawing up a software bill of materials covering at the very least the top-level dependencies;

(f) to provide security-related information by recording and monitoring relevant internal activity, including access to or modification of data, services or functions, where applicable, with an opt-out mechanism for the user;

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

(h) to protect the availability of essential and basic functions, including after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) to minimise the negative impact on the availability of services provided by other networks and devices in the event of a physical or technical incident;

(j) to ensure that ICT products, ICT services and ICT processes are regularly tested and their security reviewed;

(k) to ensure that vulnerabilities are addressed and remediated without delay, including through security updates, and that information about fixed vulnerabilities is shared and publicly disclosed, unless the risks of publication outweigh the security benefits;

(l) to ensure that a policy on coordinated vulnerability disclosure is in place;

(m) to facilitate the sharing of information about potential vulnerabilities in ICT products, ICT services and ICT processes;

(n) to ensure that, where security updates are available to address identified security issues, those security updates are disseminated without delay;

(o) to ensure that the managed security services are provided with the requisite competence, expertise and experience, including that the staff tasked with providing those services have a sufficient and appropriate level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;

(p) to ensure that the ICT products, ICT services and ICT processes deployed in the provision of the managed security services are secure by design and by default and, where applicable, include the latest security updates and do not contain publicly known vulnerabilities;

(q) to ensure that the certified entity has appropriate internal procedures in place to ensure that services are provided at a sufficient and appropriate level of quality;

(r) to ensure that the certified entity is able to identify, protect against, detect, respond to, and recover from incidents;

(s) to ensure that the certified entity is able to manage the risks posed to the security of network and information systems used by the entity for its operations or for the provision of its services, and to prevent or minimise the impact of incidents on recipients of its services and on other services;

(t) to ensure that the certified entity is able to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, that it has in place the full range of ICT-related capabilities needed to address the security of the network and information systems that are used by the entity, and that support the continued provision of services and their quality, including throughout disruptions;

(u) to ensure that the certified entity is able to implement and maintain an information security management system;

(v) to resist any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, the network and information system used by the entity, and to ensure the continued provision of services and their quality, including throughout disruptions;

(w) to ensure that the entity is able to ensure the security of processing of personal data.

2. The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend paragraph 1 of this Article by adding or modifying security objectives in order to ensure that they reflect the latest technological development and new related threats as well as adoption of new Union legislation setting out the demonstration of compliance and the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation.

3. A European cybersecurity certification scheme addressing products with digital elements as defined in Article 3, point (1), of Regulation (EU) 2024/2847 shall be designed in alignment with the essential cybersecurity requirements set out in Annex I that Regulation and take into account available harmonised standards.

Article 81
Elements of European cybersecurity certification schemes

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

(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services, ICT processes or managed security services, or the entity's assets, services and functions covered in scope of certification;

(b) a clear description of the purpose of the scheme and, where applicable and the identification of Union legislation setting out requirements for which the European cybersecurity certificates demonstrate compliance and confer a presumption of conformity;

(c) the maintenance strategy specifying the approach to maintenance activities set out in Article 75;

(d) the specific cybersecurity requirements, evaluation criteria and methods to be used for evaluation of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, and references to the international, European or national standards applied in the evaluation of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities or, where such standards are not available or appropriate, to technical specifications drawn up by ENISA pursuant to Article 77 or, if such specifications are not available, to other technical specifications;

(e) the maximum period of validity of European cybersecurity certificates issued under the scheme.

2. A European cybersecurity certification scheme shall include at least rules and conditions concerning the following:

(a) the monitoring of compliance of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities with the requirements of the European cybersecurity certificates or the EU statements of conformity, including the mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;

(b) the issuing, confirming, withdrawing and renewing of the European cybersecurity certificates, the extension or reduction of the scope of certification and the recertification;

(c) the consequences for ICT products, ICT services, ICT processes, managed security services or entities 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;

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

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

(f) the period of 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, ICT processes or managed security services or by the entity the cyber posture of which is subject to certification;

(g) any peer assessment mechanisms established under the scheme for authorities or bodies issuing European cybersecurity certificates pursuant to Article 85(4), which shall be without prejudice to the peer review provided for in Article 90;

(h) the confidentiality of information and data obtained by all parties in carrying out tasks and activities related to the implementation of the provisions set out in this Title;

(i) the 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 84; and

(j) the continuity of certification activities during extraordinary crisis situations, that are unavoidable and hinder the possibility to apply the certification scheme's rules.

3. A European cybersecurity certification scheme shall, where appropriate, also include the following:

(a) one or more assurance levels and corresponding evaluation levels;

(b) protection profiles to specify the security requirements that are applicable to a given category of ICT products, ICT services, ICT processes or managed security services;

(c) extension profiles to set out additional security requirements, including, where applicable, security requirements set out in national provisions transposing Union law;

(d) clarification on which conformity assessment activities, including calibration, testing, certification and inspection, for assurance level 'high', or for the purpose of demonstrating compliance and granting presumption of conformity, are permitted outside the European Economic Area (EEA);

(e) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services, ICT processes, managed security services or cyber posture of entities;

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

(g) the information which is necessary for certification and which an applicant is to provide or otherwise make available to the conformity assessment bodies;

(h) marks or labels and the conditions under which such marks or labels may be used;

(i) conditions for the international recognition of European cybersecurity certificates in accordance with Article 87.

4. The specified requirements of the European cybersecurity certification scheme shall be consistent with the requirements of Union legislation.

5. The Commission is empowered to adopt implementing acts laying down common principles and model provisions for elements set out in paragraphs 1, 2 and 3 across European cybersecurity certification schemes. Where appropriate and available, a European cybersecurity certification scheme may include references to those principles and model provisions.

6. The implementing acts referred to in paragraph 5 shall be adopted in accordance with the examination procedure referred to in Article 118(2). When developing or revising the common principles and model provisions for the elements of European cybersecurity certification schemes, the Commission shall consult ENISA and take into account, as appropriate, views expressed by the ECCG, relevant stakeholders and other relevant bodies.

Article 82

Assurance and evaluation 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, ICT processes, managed security services or cyber posture of entities: “basic”, “substantial” or “high”. Those assurance levels shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process, managed security service, or with the nature of entities, the cyber posture of which is subject to certification, and their operational environment, in terms of the probability and impact of an incident.

2. European cybersecurity certificates shall refer to any assurance level specified in the European cybersecurity certification scheme under which those certificates are issued. EU statements of conformity shall refer to the assurance level “basic”.

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

4. The European cybersecurity 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, ICT processes, managed security services or cyber posture of entities for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security controls, 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 the 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, ICT processes, managed security services or cyber posture of entities for which that certificate is issued meet the corresponding security requirements, including security controls, and that they have been evaluated at a level intended to minimise known risks of incidents and cyberattacks and the risk of cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes, managed security services or entities correctly implement the necessary security controls. 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, ICT processes, managed security services or cyber posture of entities for which that certificate is issued meet the corresponding security requirements, including security controls, and that they have been evaluated at a level intended to minimise the risk of incidents and 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) a review to demonstrate the absence of publicly known vulnerabilities;

   (b) testing to demonstrate that the ICT products, ICT services, ICT processes, managed security services or entities correctly implement the necessary security controls at the state of the art;

   (c) an assessment of the resistance of the ICT products, ICT services, ICT processes, managed security services or entities to skilled attackers, using, where relevant, penetration testing.

   Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken. Any conformity assessment activities, including calibration, testing, certification and inspection, for assurance level 'high' shall be undertaken in the European Economic Area, unless otherwise provided for in a European cybersecurity certification scheme.

8. Where a European cybersecurity certification scheme is designed to demonstrate compliance and grant presumption of conformity with a specific Union legal act, a European cybersecurity certificate shall provide assurance that the certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities meet the corresponding cybersecurity requirements of that legal act. Any conformity assessment activities, including calibration, testing, certification and inspection, for the purpose of presumption of conformity shall be undertaken in the

European Economic Area, unless otherwise provided for in a European cybersecurity certification scheme.

9. A European cybersecurity certification scheme may specify several evaluation levels for a given assurance level. Each of the evaluation levels shall correspond to one of the assurance levels.

Article 83
Conformity self-assessment

1. A European cybersecurity certification scheme may allow for conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that present a low risk corresponding to assurance level "basic".

2. The manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the European cybersecurity certification scheme has been demonstrated. By issuing such a statement, that manufacturer or provider or entity assumes responsibility for the compliance of the ICT product, ICT service, ICT process, managed security service or cyber posture with the requirements set out in that scheme.

3. The manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services, ICT processes, managed security services or cyber posture with the European cybersecurity certification scheme available to the national cybersecurity certification authority designated pursuant to Article 89 for the period provided for in that scheme. A copy of the EU statement of conformity shall be submitted without undue delay to the national cybersecurity certification authority and to ENISA.

Article 84
Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes

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

   (a) the intended purpose of the relevant ICT product, ICT service or ICT process, including the security environment provided by the manufacturer or provider;

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

(c) the type of technical security support offered by the manufacturer or provider and the end date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

(d) if the manufacturer or provider decides to make available a software bill of materials to the user, information on where that can be accessed.

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

(a) the single point of contact where information about vulnerabilities can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;

(b) information about fixed vulnerabilities, including a description of the vulnerabilities, including information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity, and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.

3. The information referred to in paragraphs 1 and 2 shall be available in electronic form and shall remain available and be updated as necessary during the validity and at least for a period of five years after the expiry or withdrawal of the relevant European cybersecurity certificate or EU statement of conformity.

4. The obligations set out in paragraphs 1 and 2 shall not apply where the security of the relevant ICT product, ICT service or ICT process might be compromised if the information is made publicly available.

CHAPTER III
Governance for the European Cybersecurity Certification Framework

Section 1
General rules and management of European cybersecurity certification schemes

Article 85
Issuance of European cybersecurity certificates

1. ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that have been certified under a European cybersecurity certification scheme shall be presumed to comply with the requirements of such scheme.

2. The conformity assessment bodies referred to in Article 91 shall issue European cybersecurity certificates on the basis of criteria included in the European cybersecurity certification scheme adopted pursuant to Article 74.

3. By way of derogation from paragraph 2, a European cybersecurity certification scheme may provide that European cybersecurity certificates resulting from that scheme are to be issued only by one of the following public bodies:

   (a) a national cybersecurity certification authority referred to in Article 88 that is accredited as a conformity assessment body pursuant to Article 91(1);

   (b) a public body that is accredited as a conformity assessment body pursuant to Article 91(1).

4. Where a European cybersecurity certification scheme adopted pursuant to Article 74 establishes assurance level 'high' or where such scheme specifies otherwise, the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority as referred to in Article 88 that is accredited as a conformity assessment body pursuant to Article 91(1) or, in the following cases:

   (a) by a conformity assessment body on the basis of a prior approval model; or

   (b) by a conformity assessment body on the basis of a general delegation model.

5. The Commission is empowered to adopt implementing acts specifying procedures for prior approval or general delegation models referred to in paragraph 4 of this Article. In the preparation process for those implementing acts, the Commission shall consult the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

6. The natural or legal person who submits ICT products, ICT services, ICT processes or managed security services for certification, or the entity which applies for certification of its cyber posture, shall make available all information necessary to conduct the certification to the national cybersecurity certification authority designated pursuant to Article 89, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 91.

7. Conformity assessment bodies and, where applicable, national cybersecurity certification authorities shall inform ENISA without undue delay about their decisions that affect the status of European cybersecurity certificates and EU statements of conformity in accordance with Article 94.

8. The holder of a European cybersecurity certificate shall inform the conformity assessment body and, where applicable, national cybersecurity certification authority, referred to in paragraph 7, of any subsequently detected vulnerabilities or nonconformities concerning the certified ICT product, ICT service, ICT process, managed security service or cyber posture of entity that have a likely impact on its conformity with the certificate. That body shall forward that information without undue delay to the national cybersecurity certification authority concerned and assess the impact on the certificate in line with the scheme's conditions as referred to in Article 81(2), point (d).

9. For their certified ICT products, ICT services, ICT processes or managed security services identified, for their entirety or parts thereof, as key assets pursuant to Article 102, the holders of a European cybersecurity certificate shall not use, install or otherwise integrate ICT components or components that include ICT components from high-risk suppliers in certified ICT products, ICT services, ICT processes or managed security services.

10. 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.

11. The Commission shall cooperate with Member States to ensure the application of provisions related to the issuance of European cybersecurity certificates also in a view application of Article 100(4), point (b). The conformity assessment body and, where relevant, the national cybersecurity certification authority shall provide the Commission, on request and without undue delay, with all information relating to the issuance of the relevant European cybersecurity certificates or EU statements of conformity.

Article 86
National cybersecurity certification schemes and certificates

1. National cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities that are covered by the subject matter and scope of a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 74(9). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities that are not covered by the subject matter and scope of a European cybersecurity certification scheme may continue to exist.

2. Member States shall not introduce new national cybersecurity certification schemes or related procedures for the ICT products, ICT services, ICT processes, managed security services and cyber posture of entities already covered by the subject matter and scope of a European cybersecurity certification scheme.

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

4. Member States shall notify the Commission and the ECCG before adopting new national cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities.

5. The Commission may suggest to a Member State to withdraw a national cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, where the development of a European cybersecurity certification scheme covering such products, services, processes or cyber posture has already been requested in accordance with Article 73, taking into account the development plan of such scheme.

Article 87
International recognition of European cybersecurity certificates

1. Third country certificates of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities may be recognised, by means of an implementing act or through the conclusion of an agreement between the Union and the third country in question or an international organisation, as equivalent to European cybersecurity certificates if the requirements of the relevant third country scheme or international organisation scheme are considered equivalent to those in

European cybersecurity certification schemes. The Commission is empowered to adopt such implementing acts. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

2. The implementing acts and the agreements referred to in paragraph 1 shall be based on the conditions for international recognition of European cybersecurity certificates set out in accordance with Article 74(11).

3. Agreements on the recognition of third country certificates or the international organisation certificates referred to in paragraph 1 shall only be concluded if they also recognize European cybersecurity certificates as equivalent to the third country certificates.

Article 88
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, one or more national cybersecurity certification authorities 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. Each national cybersecurity certification authority shall be independent of the entities it supervises with regard to its organisation, funding decisions, legal structure and decision-making.

4. The activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates under this Regulation shall be strictly separated from their supervisory activities set out in this Article and in Article 85(4), points (a) and (b), 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. National cybersecurity certification authorities shall have the following tasks:

   (a) participate in the ECCG pursuant to Article 90(2);

   (b) supervise and enforce rules included in European cybersecurity certification schemes pursuant to Article 81(2), point (a), to ensure the compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with relevant market surveillance or supervisory authorities, including, competent authorities under Directive (EU) 2022/2555 of the European Parliament and of the Council[82] or Regulation (EU) 2024/2847;

[82] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No

(c) monitor, in cooperation with relevant market surveillance authorities, compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified set out in this Regulation that are established in their respective territories and that carry out conformity self-assessment in the corresponding European cybersecurity certification scheme;

(d) without prejudice to Article 91(3), actively assist and support the national accreditation bodies or other relevant authorities in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation;

(e) cooperate with the Commission where the competence of a conformity assessment body is challenged pursuant to Article 94;

(f) monitor and supervise the activities of the public bodies referred to in Article 85(3);

(g) where applicable, authorise conformity assessment bodies in accordance with Article 93, monitor compliance with and enforce the obligations of conformity assessment bodies with the additional or specific requirements set out in European cybersecurity certification schemes pursuant to Article 81(3), point (f), and restrict, suspend or withdraw existing authorisation where conformity assessment bodies do not meet the requirements of this Regulation;

(h) 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 85(4) or in relation to EU statements of conformity issued under Article 83, investigate the subject matter of such complaints to the extent appropriate, and inform the complainant of the progress and the outcome of the investigation within a reasonable period;

(i) provide an annual report on its main activities to the Commission, ENISA and the ECCG by 31 March [year of entry into force + 12 months] each year, and make these reports available to the peer review team where the national cybersecurity certification authority is subject to peer review in accordance with Article 89;

(j) cooperate with other national cybersecurity certification authorities, market surveillance authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes;

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

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

910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(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 the requirements set out in 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 legislation or national procedural law;

(e) to withdraw, in accordance with national law, European cybersecurity certificates issued by national cybersecurity certification authorities or by conformity assessment bodies in accordance with Article 85(4), 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 97, and to require the immediate cessation of infringements of the obligations set out in this Regulation.

8. 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, ICT processes, managed security services and the cyber posture of entities.

9. By [entry into force + 6 months], ENISA shall develop a template for the report referred to in paragraph 6, point (i), of this Article, in cooperation with the Commission and the ECCG.

Article 89
Peer review

1. 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 this Regulation are strictly separated from their supervisory activities set out in Article 88 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, ICT processes, managed security

services and cyber posture of entities with European cybersecurity certificates pursuant to Article 88(7), point (a);

(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services, ICT processes or managed security services or entities the cyber posture of which is certified, pursuant to Article 88(7), point (b);

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

4. Peer review shall be carried out at least once every five years by at least two national cybersecurity certification authorities of other Member States and by the Commission. ENISA shall also participate in the peer review as observer. The peer review team shall draw up the final report and the summary of the peer review.

5. ENISA shall support the organisation of the peer review mechanism and the peer reviews, including by developing relevant guidance documents and templates, in cooperation with the Commission and the ECCG.

6. The Commission is empowered to 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 peer review. In the preparation of those implementing acts, the Commission shall consult the ECCG and ENISA. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

7. The final report, including possible guidelines or recommendations, and the summary of the peer review shall be examined by the ECCG, which shall endorse the summary for publication on the website referred to in Article 79(2).

Article 90
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. The ECCG shall have the following tasks:

(a) to advise and assist the Commission in its work to ensure the consistent implementation and application the rules set out in this Title, cybersecurity certification policy issues, and the coordination of policy approaches;

(b) to advise and assist the Commission in the preparation of requests for European cybersecurity certification schemes pursuant to Article 73;

(c) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme pursuant to Article 74 and technical specifications pursuant to Article 77;

(d) to assist, advise and cooperate with ENISA and the Commission in relation to the maintenance activities pursuant to Article 75;

(e) to assist, advise and cooperate with the Commission in relation to the review or withdrawal of existing European cybersecurity certifications schemes pursuant to Article 76;

(f) to suggest that a request is submitted to the Commission with regard to the preparation of a candidate European cybersecurity certification scheme pursuant to Article 73(2);

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

(h) to examine relevant developments in the field of cybersecurity certification, including at national level pursuant to Article 86, and to exchange information and good practices on cybersecurity certification schemes;

(i) to facilitate the cooperation between national cybersecurity certification authorities under the rules set out in this Title through capacity-building and exchange of information, in particular relating to issues concerning cybersecurity certification;

(j) to support the implementation of the peer review mechanism pursuant to Article 89 and of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to Article 81(2), point (g);

(k) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including as part of the maintenance of existing European cybersecurity certification schemes and, where appropriate, to make recommendations to ENISA to engage with relevant European or international standardisation organisations to address insufficiencies or gaps in available European or internationally recognised standards.

4. With the assistance of ENISA, the Commission shall chair the ECCG and provide the ECCG with a secretariat.

5. The Commission may set up ECCG sub-groups for any of the following purposes:

(a) to examine specific questions on the basis of terms of reference established by the Commission;

(b) to maintain and review the European certification schemes in accordance with this Regulation and on the basis of terms of reference established by the Commission.

6. The sub-groups shall report to the ECCG.

7. The sub-groups shall be co-chaired by the Commission and ENISA, and the secretariat of the sub-groups shall be provided by ENISA.

8. The ECCG and its sub-groups shall adopt rules of procedure by simple majority of their members, based on a proposal by, and in agreement with the Commission.

Section 2
Conformity assessment bodies

Article 91

Competence of 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 Annex I to this Regulation.

2. Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to this Regulation, the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1.

3. 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, provided that the conformity assessment body 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 does not comply with this Regulation.

4. When establishing additional or specific accreditation requirements for a European cybersecurity certification scheme covering ICT products, pursuant to Article 92, synergies shall be sought, where appropriate, with the requirements relating to notified bodies under Regulation (EU) 2024/2847 and the accreditation requirements under the cybersecurity certification schemes which have already been adopted.

5. Where a conformity assessment body is accredited in accordance with Regulation (EU) 2024/2847, relevant authorities may reuse results from previous accreditation process regarding any overlapping requirements as evidence during the accreditation process under this Regulation.

Article 92

Additional harmonisation of the competence of conformity assessment bodies

1. Where a European cybersecurity certification scheme sets out additional or specific requirements pursuant to Article 81(3), point (f), conformity assessment bodies shall be authorised by a national cybersecurity certification authority appointed pursuant to Article 88(1) to carry out tasks under such scheme. Such authorisation shall be issued only where the conformity assessment body has been accredited and meets the additional or specific requirements set out under the European cybersecurity certification scheme.

2. Where a conformity assessment body requests an authorisation under this Article, it shall submit the request to the national cybersecurity certification authority of the Member State in which it is established or with the national cybersecurity certification authority to which that Member State has had recourse in accordance with Article 88(1).

3. A conformity assessment body may request authorisation by a national cybersecurity certification authority other than that referred to in paragraph 2 in any one of the following situations:

(a) where the national cybersecurity certification authority referred to in paragraph 1 does not perform authorisation in respect of the conformity assessment activities for which authorisation is sought;

(b) where the national cybersecurity certification authority referred to in paragraph 1 has not undergone peer review in accordance with Article 89 in respect of the conformity assessment activities for which authorisation is sought.

4. Where a national cybersecurity certification authority receives a request pursuant to paragraph 3, it shall inform the national cybersecurity certification authority of the Member State in which the requesting conformity assessment body is established. In such cases, the national cybersecurity certification authority of that Member State may participate in the authorisation as an observer.

5. A national cybersecurity certification authority may request another national cybersecurity certification authority to carry out parts of the assessment activity. In such a case, the authorisation certificate shall be issued by the requesting authority.

6. The authorisation referred to in paragraph 1 shall be valid for a period no longer than the period of validity of the accreditation, and may be renewed provided that the conformity assessment body meets the requirements set out in paragraph 1 and its accreditation has also been renewed.

7. National cybersecurity certification authorities shall, within a reasonable timeframe, take all appropriate measures to restrict, suspend or revoke the authorisation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the authorisation have not been met or are no longer met, or where the conformity assessment body does not comply with this Regulation.

8. The Commission is empowered to adopt implementing acts to lay down the procedures, including on cross-border cooperation, for authorisation of conformity assessment bodies. In the preparation process of implementing acts, the Commission shall consult ENISA and the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

Article 93
Notification of conformity assessment bodies

1. For each European cybersecurity certification scheme, the national cybersecurity certification authorities of a Member State shall notify the Commission and the other Member States of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 92.

2. The national cybersecurity certification authorities shall carry out the notification as referred to in paragraph 1 using the electronic notification tool developed and managed by the Commission.

3. The Commission is empowered to adopt implementing acts to lay down the circumstances, formats and procedures for notifications referred to in paragraph 1 of this Article, including the objection procedure by other Member States during the notification process, the unique identification of conformity assessment bodies, as well as the circumstances for restriction, suspension or withdrawal of notification. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

Article 94

Challenges with regard to the competence of conformity assessment bodies

1. The Commission shall investigate any cases in which it has doubts, or is made aware of doubts about the competence of a conformity assessment body to meet, or the continued fulfilment by a conformity assessment body of, the requirements and responsibilities to which it is subject.

2. The national cybersecurity certification authority shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the conformity assessment body concerned.

3. The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated confidentially.

4. Where the Commission ascertains that a conformity assessment body does not meet or no longer meets the requirements for its notification, it shall inform the national cybersecurity certification authority accordingly and request it to take the necessary corrective measures, including de-notification if necessary.

5. Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.

Article 95

Information and retention obligation on conformity assessment bodies

1. Conformity assessment bodies shall inform the national cybersecurity certification authority of the following:

   (a) any refusal, restriction, suspension or withdrawal of a certificate;

   (b) any circumstances affecting the scope of and conditions for the notification referred to in Article 93(1);

   (c) any request for information that they have received from market surveillance authorities regarding conformity assessment activities;

   (d) on request, any conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

2. Conformity assessment bodies shall also provide ENISA with the information referred to in paragraph 1 point (a) in view of facilitating the performance of its task under Article 79.

3. Conformity assessment bodies shall provide the other conformity assessment bodies under this Regulation carrying out similar conformity assessment activities covering the same ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified without undue delay with relevant information on issues relating to negative and, upon request, positive conformity assessment results.

4. Conformity assessment bodies shall maintain a record system, containing all the documents and evidence produced or received in connection with each evaluation and certification that they perform. The record shall be stored in a secure and accessible manner for the period necessary for the purposes of certification and for at least five years after the expiry or withdrawal of a relevant European cybersecurity certificate.

Section 3
Other provisions

Article 96
Rights to lodge a complaint and right to an effective judicial remedy

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 85(4), 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, of the decision taken, and of the right to an effective judicial remedy referred to in paragraphs 3 and 4.
3. 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 paragraph 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 paragraph 1.
4. 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 97
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
SECURITY OF ICT SUPPLY CHAINS

CHAPTER I
Trusted ICT supply chain framework

Article 98
Scope of the framework

1. The trusted ICT supply chain framework shall provide for a security mechanism at Union level to address non-technical risks in sectors of high criticality and other critical sectors as referred to in Directive (EU) 2022/2555. The mechanism shall identify key ICT assets in critical ICT supply chains and set out appropriate and proportionate mitigation measures on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555.

2. The obligations set out in this Title shall be without prejudice to obligations set out in Article 13 of Regulation (EU) 2024/2847 and in national provisions transposing Article 21 of Directive (EU) 2022/2555.

3. The provisions laid down in this Chapter shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity in ICT supply chains, provided that such provisions are consistent with their obligations under in Union law.

Article 99
Security risk assessments

1. The Commission or a group of at least three Member States may request the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 ('NIS Cooperation Group') to conduct the Union-level coordinated security risk assessments in accordance with Article 22 of that Directive. Where a security risk assessment is conducted following such request, it shall include in particular the proposed identification of the key ICT assets of the respective ICT supply chain as well as the main threat actors, risks and vulnerabilities affecting those assets. The Union-level coordinated security risk assessments shall develop risk scenarios and propose measures to mitigate the identified risks.

2. The Union-level coordinated security risk assessments shall be completed within six months from the request referred to in paragraph 1. Upon request of the Commission, the NIS Cooperation Group may agree to a shorter period.

3. Where the Commission has sufficient reason to believe that there is a significant cyber threat for the security of the Union in relation to an ICT supply chain and that action is required to preserve the proper functioning of the internal market, the Commission shall without delay:

   (a) consult the Member States on the need to take one or several of the mitigating measures referred to in Article 103; and

   (b) conduct a security risk assessment, taking into account the consultation of the Member States. The security risk assessment shall include the proposed identification of the key ICT assets as well as the main threat actors, risks and vulnerabilities affecting those assets. The security risk assessment shall develop risk scenarios and propose measures to mitigate the identified risks.

Article 100
Designation of third countries posing cybersecurity concerns

1. Where, as a result of the security risk assessment referred to in Article 99, or based on other sources, such as a public statement on behalf of the Union or a Member

State, it appears that a third country poses a serious and structural non-technical risk to ICT supply chains, the Commission shall verify the risk posed by that country, taking into account the following elements:

(a) the existence of laws in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(b) existing practices in the third country, demonstrated by independent sources, that require entities under the jurisdiction of the third country to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited;

(c) the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct the identified security concerns, including about existing practices referred to in point (b);

(d) substantiated information about one or more incidents of threat actors controlled from that country and operating out of the territory of that country carrying out malicious cyber activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors;

(e) relevant information stemming from Union-level coordinated security risk assessments or reports by Member States or international organisations.

2. When the Commission, following the verification referred to in paragraph 1, concludes that a third country poses serious and structural non-technical risks to ICT supply chains, it may, by means of an implementing act, designate that third country as a country posing cybersecurity concerns to ICT supply chains. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 118(2).

3. The Commission shall review regularly the implementing acts adopted in accordance with paragraph 2.

4. High-risk suppliers shall not be entitled to:

(a) participate in the development of, assessment, consultation or decisions concerning European standards and European standardisation deliverables referred to in Article 10(1) of Regulation (EU) 1025/2012 and common specifications referred to in Article 27 of Regulation (EU) 2024/2847 in the area of cybersecurity;

(b) apply for or be a holder of any European cybersecurity certificates pursuant to Title III;

(c) become accredited conformity assessment body pursuant to Title III;

(d) apply to become authorised attestation provider of any European individual cybersecurity skills attestations pursuant to Title II, Section 4;

(e) participate in public procurement procedures, organised in accordance with legislation transposing Directive 2014/24/EU and 2014/25/EU in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as identified in accordance with Article 102;

(f) participate in any activities under Union funding programmes and instruments implemented in direct and indirect management in accordance with Article 136 Regulation (EU, Euratom) 2024/2509 and Union sector-specific rules as well as in any Union funding activities implemented in shared management in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as identified in accordance with Article 102.

The authorities in charge of the procedures referred to in points (a) to (f) shall conduct the necessary assessments for the purpose of this paragraph. The authorities may also rely for this purpose on the list referred to in Article 104.

5. In cases where a high-risk supplier has already obtained a European cybersecurity certificate pursuant to Title III, the competent authority shall withdraw it without undue delay.

Article 101
General ICT supply chain security mechanism

Where the NIS Cooperation Group has conducted a Union-level coordinated security risk assessment pursuant to Article 99(1) of this Regulation, or after the completion of the procedure in case of significant cyber threat pursuant to Article 99(3) for an ICT supply chain, the Commission may take measures provided for in Articles 102 and 103(1) and (2).

Article 102
Identification of key ICT assets

1. Where the risk assessment conducted in accordance with Article 99(1) or (3) indicates significant cybersecurity risks in relation to an ICT supply chain, the Commission is empowered to adopt implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2) of this Regulation.

2. When identifying the key ICT assets referred to in paragraph 1, the Commission shall take into account the following elements:

   (a) whether those assets have essential and sensitive functions for the functioning of products manufactured or services provided by the entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555;

   (b) whether incidents, including such caused by exploited vulnerabilities concerning those assets can lead to serious disruptions of ICT supply chains across the internal market or lead to exfiltration of data;

   (c) whether there is a dependency on a limited number of suppliers of those assets;

   (d) the results of the risk assessments referred to in Article 99.

Article 103
Mitigation measures in the ICT supply chain

1. The Commission is empowered to adopt implementing acts establishing, where necessary to ensure high level of cybersecurity, cyber resilience and trust within the

Union, that specific type of entities referred to in Annex I and II to Directive (EU) 2022/2555 shall be prohibited to use, install or integrate in any form ICT components or components that include ICT components from high-risk suppliers as identified in accordance with Article 104 in key ICT assets identified in accordance with Article 102. Such implementing acts shall provide for appropriate transition periods, during which the Commission shall publish the list of high-risk suppliers referred to in Article 104, as well as additional time periods for phasing out the relevant ICT components and components that include ICT components. Such implementing act may also specify these ICT component or components that include ICT components.

2. The Commission is empowered to adopt implementing acts establishing, where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, that specific type of entities referred to in Annexes I and II to Directive (EU) 2022/2555 shall be subject to one or several of the following mitigating measures in relation to their ICT supply chain and in particular to key ICT assets identified in accordance with Article 102, to mitigate risks identified in the security risk assessments conducted pursuant to Article 99:

   (a) application of transparency requirements concerning the provision of information to the competent authority about the suppliers in the ICT supply chain for key ICT assets designated in accordance with Article 102;

   (b) prohibition related to transfers of data to third countries and remote data processing from a third country;

   (c) technical measures to be audited by a third party, including:

      (i) the use of on-device processing;

      (ii) specific segmentation of network systems;

      (iii) the disabling of any remote or physical access to key ICT assets;

      (iv) the disabling of non-essential features;

      (v) operational network monitoring;

      (vi) testing of hardware and software.

   (d) restrictions related to operational control, including outsourcing of organisational functions to managed service providers;

   (e) restrictions related to the contractual relations of the entity with its suppliers;

   (f) requirement for the service to be operated, managed, maintained or supported by personnel vetted by the relevant national competent authorities;

   (g) diversification of supply of ICT components or components included in ICT components.

3. When introducing measures referred to in paragraph 2, the Commission may lay down technical and methodological requirements for the measures.

4. Before adopting the implementing acts referred to in paragraphs 1 and 2, the Commission shall assess potential risks and dependencies and in particular:

   (a) where applicable, the level of risk associated with the use, installation or integration, in any form, of ICT components or components that include ICT components from high-risk suppliers in key ICT assets;

(b) the potential economic and societal impacts the obligation may have on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555;

(c) the availability of alternative suppliers to high-risk ones;

(d) the potential disruption of cross-border economic and societal activities caused by an incident affecting an entity's ICT supply chain.

5. The implementing acts referred to in paragraphs 1 and 2 of this Article shall be adopted in accordance with the examination procedure referred to in Article 118(2) and shall be reviewed at least every 36 months.

6. In exceptional circumstances, which justify an intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the use, installation or integration of ICT components or components that include ICT components from a specific entity established in or controlled by a third country or entities from a third country, or a national from a third country represent a significant non-technical cybersecurity risk for the economic or societal activities of at least three Member States, the Commission shall without delay consult the Member States on the need to take measures at Union level.

7. The Commission is empowered to adopt implementing acts to establish that specific type of entities referred to in Annexes I and II to Directive (EU) 2022/2555 shall be prohibited to use, install or integrate ICT components or components that include ICT components from an entity referred to in paragraph 6. To that end, it shall consult the entities of the types referred to in Annexes I and II to Directive (EU) 2022/2555 potentially concerned by the prohibition. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2). Where relevant, they shall include appropriate periods for the phasing out of these ICT components or components that include ICT components. Such implementing act may also specify these ICT component or components that include ICT components subject to the prohibition. This prohibition shall also concern ICT components or components including ICT components from all entities controlled by the specific entity referred to in paragraph 6.

8. The implementing acts referred to in paragraphs (1), (2) and (7) may also specify that the mitigation measures are only applicable to types of entities referred to in Annex I and II to Directive (EU) 2022/2555 of a specific size.

9. Article 100(4) shall apply to the specific entity established in or controlled by a third country or an entity from a third country, or a national from a third country referred to in paragraph 7.

10. The implementing acts adopted in accordance with paragraphs (1), (2) and (7) that are applicable to type of entities referred to in Annex I point 10 to Directive (EU) 2022/2555 shall apply mutatis mutandis to the European Institution, bodies, offices and agencies.

Article 104
Identification of high-risk suppliers

1. By way of implementing acts, the Commission shall establish lists of high-risk suppliers relevant for the prohibitions laid down in the implementing acts adopted in accordance with Article 103(1), Article 103(7) or the prohibition referred to in Article 111(1).

2. For that purpose, the Commission shall map the suppliers providing ICT components and components that include ICT components relevant for the prohibition referred to in paragraph 1.

   On this basis, the Commission shall do an initial assessment to identify which of the mapped suppliers are potentially established in a third country designated in accordance with Article 100 or controlled by such third country, by an entity established in such third country or by a national of such third country. The Commission shall also do an initial mapping on suppliers potentially controlled by the entity referred to in Article 103(6).

3. The Commission shall assess the place of establishment as well as the ownership and control structure of the suppliers initially identified in accordance with the second subparagraph of paragraph 2.

4. For the purpose of the assessment referred to in paragraph 3, the Commission shall be entitled to request the necessary information from the suppliers. In case the supplier does not provide the necessary information within the established deadline, the Commission may conclude that the supplier is established in a third country designated in accordance with Article 100 or controlled by such third country, by entities from that third country or by nationals of such third country. Where the Commission is carrying out an assessment for the purpose of Article 103(7) and the supplier does not provide the necessary information within the established deadline, the Commission may conclude that the supplier is controlled by an entity designated in line with that Article. The competent authorities referred to in Article 112 shall also share relevant information with the Commission upon request.

5. The Commission shall share preliminary findings concerning the establishment, control and ownership assessment with the concerned supplier. The Commission shall grant the supplier an opportunity to be heard on those preliminary findings.

6. The Commission may ask a competent authority to carry out the initial establishment, ownership and control assessment of a supplier, where justified in view of the characteristics of the operation of this supplier. A competent authority may offer to carry out such initial assessment. The Commission shall verify these initial findings in view of deciding whether the supplier should be included in the list of high-risk suppliers.

7. The Commission shall regularly update the list of high-risk suppliers in view of removing or adding high-risk suppliers. High-risk suppliers included in the list may request the Commission to re-assess their establishment, control and ownership structure upon provision of evidence that there have been relevant changes.

8. Where a competent authority becomes aware, including on the basis of information provided by an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555 that a supplier may need to be included in a list of high-risk suppliers, it shall inform the Commission without undue delay.

Article 105

Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns

1. An entity established in or controlled by entities from a third country posing cybersecurity concerns designated in accordance with Article 100 may make a reasoned request to the Commission to be exempted:

(a) from being subject to the prohibition imposed on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 to use, install or integrate in any form its ICT components or components that include its ICT components in key ICT assets of those entities by way of derogation from Article 111 or implementing acts adopted pursuant to Article 103(1);

(b) from being subject to the prohibition to participate in public procurement procedures, organised in accordance with legislation transposing Directive 2014/24/EU and Directive 2014/25/EU in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as defined in accordance with Article 102 in derogation to Article 100(4).

2. The request referred to in paragraph 1 shall:

(a) specify the interest of the entity established in or controlled by entities from a third country posing cybersecurity concerns designated in accordance with Article 100 in being granted the exemption referred to in paragraph 1 of this Article; and

(b) demonstrate with clear evidence that effective mitigating measures will be put in place to address non-technical risks and ensure the absence of any possible exercise of undue interference by the third country designated pursuant to Article 100 in relation to the provision of ICT components or components that include ICT components for the use, installation or integration in key ICT assets of an entity of the type referred to in Annexes I and II to Directive (EU) 2022/2555.

3. The Commission is empowered to adopt implementing acts to further specify the conditions referred to in paragraph 2 point (b), and to lay down detailed rules in respect of the procedures referred to in this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

4. The Commission shall assess the request referred to in paragraph 1 through a fair and transparent process, taking into account:

(a) the circumstances and additional elements referred to in Article 100(1) and (2) in relation to the designated country posing cybersecurity concerns to ICT supply chains where the entity is established or from where it is controlled;

(b) the effectiveness of the mitigating measures referred to in paragraph 2 point (b);

(c) whether the exemption for the entity established in or controlled by entities from a third country posing cybersecurity concerns to ICT supply chains would not be detrimental to the Union's interest.

5. When the Commission, following the assessment in paragraph 3, concludes that it is justified to grant an exemption, it shall do so by way of decision, which it shall notify to the applicant within 9 months of receipt of the request.

6. When adopting a decision referred to in paragraph 4, the Commission may limit the exemption to a specific period of time and may subject the exemption to conditions for the entity, including:

(a) a timeline for the implementation of mitigating measures referred to in paragraph 2, point (b);

(b) third-party audits on a regular basis to ensure the effective implementation of mitigating measures;

(c) reporting obligations regarding compliance.

7. When the Commission, following the assessment in paragraph 3, concludes that it is not justified to grant an exemption, it shall do so by way of a decision, and shall notify it to the applicants within 9 months of receipt of the request.

8. The Commission may, on its own initiative, withdraw or modify the decision referred to in paragraph 4 in one or more of the following situations:

(a) there has been a material change in the facts on which the decision was based;

(b) the entity which has requested the exemption acts contrary to its commitments;

(c) the exemption was based on incomplete, incorrect or misleading information provided by the entity making the request.

Article 106
Rights of defence

The Commission shall ensure that before it adopts an implementing act pursuant to Article 103(7) or before it adopts a decision refusing the granting of exemption pursuant to Article 105(7) on the basis of elements not submitted by the applicant or before it withdraws a decision pursuant to Article 105(8), the entity concerned is given the opportunity of being heard, taking into account the need, in some cases, for an urgency procedure.

Article 107
Register

The Commission shall maintain a publicly accessible register of its decisions referred to in Article 105(5). The register shall state the names of the entities that have been subject to such decisions. The Commission shall update the register on a regular basis.

Article 108
Confidentiality

Information received by the Commission pursuant to Articles 105 and 106 shall be used only for the purpose for which it was acquired.

Article 109
Fees

1. The Commission shall levy fees for requests submitted in accordance with Article 105(1).

2. Fees shall be expressed and payable in euro.

3. Fees shall be commensurate to the costs linked to the processing of requests referred to in Article 105(1), the assessment of the criteria and information referred to in Article 105(2), and the set-up, maintenance and operation of the register referred to in Article 107. All expenditure of the Commission attributed to staff involved in those activities, shall be included in such costs.

4. The Commission shall adopt implementing acts laying down detailed rules relating to the fees, specifying the amount of the fees and the way in which they are to be paid.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).

CHAPTER II
ICT supply chains in electronic communications networks

Article 110
Key ICT assets for mobile, fixed and satellite electronic communications networks

1. The key ICT assets for mobile, fixed and satellite electronic communications networks shall be as set out in Annex II.
2. ICT components or components that include ICT components provided by high-risk suppliers shall be phased out from the key ICT assets of mobile, fixed and satellite electronic communication networks.
3. The time period for the phasing out the ICT components or components that include ICT components provided by high-risk suppliers with regard to mobile electronic communications networks shall not exceed 36 months from the publication of the list of high-risk suppliers referred to in Article 104 relevant for the mobile electronic communications networks.
4. The Commission is empowered to adopt implementing acts in accordance with Article 118(2) to specify the time periods for the phasing out the ICT components or components that include ICT components provided by high-risk suppliers with regard to fixed and satellite electronic communications networks.
5. The Commission is empowered to adopt delegated acts in accordance with Article 119 to amend Annex II to this Regulation in order to adapt it to technological developments by taking into account the elements referred to in Article 103(4).

Article 111
Prohibitions for mobile, fixed and satellite electronic communication networks

1. Providers of mobile, fixed and satellite electronic communications networks shall not use, install or integrate, in any form, ICT components or components that include ICT components from high-risk suppliers in the operation of key ICT assets referred to in Annex II.
2. In cases where the competent authority designated under this Regulation in a Member State differs from the competent authority pursuant to Regulation (EU) XX/XXXX [DNA proposal], the competent authority designated under this Regulation shall inform without delay the competent authority pursuant to Regulation (EU) XX/XXXX [DNA proposal] about the measures imposed on providers of mobile, fixed and satellite electronic communications networks in accordance with Article 114. The authorities shall ensure close cooperation for the purposes of effective supervision and enforcement of those measures.

CHAPTER III
Competent authorities, supervision and enforcement, jurisdiction, rights of defence

Article 112
Competent authorities

1. Each Member State shall designate the competent authorities referred to in Article 8 of Directive (EU) 2022/2555 as authorities responsible for taking the supervisory and enforcement measures referred to in Article 114.

2. Competent authorities shall be structurally and functionally fully impartial and free from any external influence, whether direct or indirect; in particular they shall neither seek nor take instructions from any other public authority or any private party.

3. Member States shall ensure that their competent authorities have appropriate powers, sufficient human and technical resources and relevant expertise to effectively carry out the supervisory and enforcement measures referred to in Article 114.

4. Each Member State shall without undue delay notify the Commission of the names of the competent authorities designated in accordance with paragraph 1, of the respective tasks of those authorities and of any subsequent changes thereto. Each Member State shall also make public the names of the competent authorities designated in accordance with paragraph 1.

Article 113
Network for cooperation and support services of the Commission

In view of effective supervision, the Commission shall set up a network for cooperation of competent authorities of Member States referred to in Article 112 and the Commission to serve as a platform for cooperation and exchange of information, in particular for the purpose of the establishment, control and ownership assessment referred to in Article 104. The Commission shall provide the administrative support to the network.

Article 114
Supervisory and enforcement measures

1. The competent authorities as referred to in Article 112 are entitled to take the supervisory and enforcement measures on entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555. Member States shall ensure that the abovementioned measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case. Member States shall notify the Commission of the rules enacted to that end and their subsequent amendments.

2. When exercising their supervisory tasks in relation to entities referred to in Annexes I and II to Directive (EU) 2022/2555, competent authorities are entitled to subject those entities to the following:

   (a) requests for a detailed and up-to-date list of their relevant suppliers and service suppliers;

   (b) requests to access data, documents and information necessary to verify compliance with this Regulation;

   (c) on-site inspections and off-site supervision, including random checks conducted by trained professionals;

   (d) requests regarding the composition of hardware or software products installed or integrated in any form into the network or system, including components and transitive dependencies, in a commonly used and machine-readable format.

3. When exercising their enforcement powers in relation to entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555, competent authorities are entitled to:

(a) issue warnings about infringements of this Regulation by the entities concerned, setting out the relevant facts and legal considerations;

(b) adopt decisions requiring the entities concerned to remedy the infringement of this Regulation or the deficiencies identified in the implementation of mitigating measures;

(c) order the entities concerned to cease activities that infringe this Regulation and desist from repeating such activities; and

(d) impose penalties, in accordance with the rules relates to the amount laid down in Article 115 or request the imposition of such penalties by the relevant bodies, courts or tribunals, in accordance with national law.

4. When taking any of the enforcement measures referred to in the previous paragraph, the competent authorities shall consider the circumstances of each individual case and take due account of the following factors:

(a) the seriousness of the infringement and the importance of the provisions breached;

(b) the duration of the infringement;

(c) the turnover of the relevance of the entity concerned;

(d) any relevant previous infringement by the entity concerned;

(e) where applicable, any material or non-material damage caused by the infringement, including any financial or economic loss, effects on other entities and the number of users affected;

(f) any intent or negligence on the part of the entity concerned;

(g) any measures taken by the entity to prevent or mitigate the material or non-material damage;

(h) the level of cooperation with the competent authorities of the natural or legal persons held responsible.

For the purposes of the first subparagraph, point (a), the following shall constitute serious infringement:

(i) repeated violations;

(j) failure to notify or remedy significant incidents;

(k) failure to remedy deficiencies following binding instructions from competent authorities.

5. The competent authorities shall notify the entities concerned of their preliminary findings before taking enforcement measures. The entities concerned shall be given a reasonable time to submit observations on the preliminary findings. The competent authorities shall set out detailed reasoning for their enforcement measures.

6. The competent authorities shall respect the principles of confidentiality and of professional and commercial secrecy.

7. The competent authorities shall cooperate with each other and with the Commission for the purposes of supervision and enforcement under this Title in accordance with Article 116.

Article 115
Penalties

1. Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented.
2. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendments affecting them.
3. Penalties shall be imposed in addition to any of the measures referred to in Article 114(3), points (a), (b) and (c).
4. When deciding whether to impose a penalty and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the factors referred to in Article 114(4) first subparagraph..
5. Infringements of Article 103(2), point (a), shall, in accordance with paragraph 3 of this Article, be subject to penalties of a maximum of 1 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.
6. Infringements of Article 103(2), points (b) to (g), shall, in accordance with paragraph 3 of this Article, be subject to penalties of a maximum of 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.
7. Infringements of Article 103(1), and of Article 111 shall, in accordance with paragraph 3, of this Article be subject to penalties of a maximum of 7 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs.

Article 116
Mutual assistance

1. Where an entity of the type referred to in Annexes I or II to Directive (EU) 2022/2555 provides services in more than one Member State, or provides services in one or more Member States and its key ICT assets are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with each other and the Commission and shall assist each other and the Commission with a view to ensuring the effective and efficient application of the Regulation. To that end, the following rules shall apply as a minimum:
   (a) the competent authorities applying supervisory or enforcement measures in a Member State shall inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken;
   (b) a competent authority in a Member State may request another competent authority in another Member State to take supervisory or enforcement measures;

(c) a competent authority in a Member State shall, upon receipt of a substantiated request from another competent authority in another Member State, provide that other competent authority with mutual assistance, on a best-efforts basis, so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner.

2. The mutual assistance referred to in paragraph 1, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission.

3. Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.

4. In view of the obligation to comply with the principles of confidentiality and of professional and commercial secrecy as referred to Article 114(6), any information exchanged in the context of a request for assistance and provided pursuant to this Article shall be used only in respect of the matter for which it was requested.

Article 117
Jurisdiction and territoriality

1. Entities of a type referred to in Annexes I and II to Directive (EU) 2022/2555 falling within the scope of this Regulation shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of:

(a) providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;

(b) DNS service providers, top-level-domain (TLD) name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;

(c) public administration entities, which shall be considered to fall under the jurisdiction of the Member State to which they belong;

(d) air carriers, which shall be considered to fall under the jurisdiction of the Member State whose competent licensing authority granted the operating licence to the entity pursuant to Regulation (EC) No 1008/2008 of the

European Parliament and of the Council[83], or, where the operating licence or equivalent has not been granted in accordance with that Regulation, they shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2.

2. For the purposes of this Regulation an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where most of the cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

3. If an entity of a type referred to in Annexes I and II to Directive (EU) 2022/2555, is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. Where such an entity is an entity as referred to in paragraph 1, point (a), it shall be considered to fall under the jurisdiction of the Member State in which it provides its services. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Regulation.

4. The designation of a representative by an entity referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.

5. Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned where the entity provides services or has a network and information system on their territory.

TITLE VI
FINAL PROVISIONS

Article 118
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall have two configurations. In respect of Titles II and III, the Commission shall be assisted by a committee in the first configuration, whereas in respect of Title IV, the Commission shall be assisted by a committee in the second configuration. That committee shall be committee within the meaning of Regulation (EU) No 182/2011.

[83] Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (Recast) (OJ L 293, 31.10.2008, p. 3-20, ELI: https://eur-lex.europa.eu/eli/reg/2008/1008/oj/eng).

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

Article 119
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts according to Articles 80(2) and Article 110(5) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in Articles 80(2) and Article 110(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 80(2) and Article 110(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 120
Evaluation and review

1. By [DD MM YYYY], and every five years thereafter, the Commission shall commission an evaluation which shall be conducted in accordance with the Commission's guidelines.

2. The evaluation referred to in paragraph 1 shall include an assessment of the following:

   (a) ENISA's performance in relation to its objectives, mandate, mission, tasks, governance and location;

   (b) the effectiveness, efficiency and EU added value of the European individual cybersecurity skills attestations schemes as laid down in Title II, Chapter II, Section 4 of this Regulation;

   (c) 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, ICT processes, managed security

services and entities in the Union and improving the functioning of the internal market;

(d) the impact, effectiveness and efficiency of provisions of Title IV of this Regulation with regard to the objectives of the trusted ICT supply chain framework.

3. The evaluation referred to in paragraph 1, point (a), shall, in particular, address the possible need to modify the mandate of ENISA, and the financial implications of any such modification.

4. On the occasion of every second evaluation, referred to in paragraph 1, point (a), the Commission shall assess the results achieved by ENISA having regard to its objectives, mandate, mission, governance and tasks, including an assessment of whether the continuation of ENISA is still justified with regard to these objectives, mandate, mission, governance and tasks.

5. The Commission shall report to the European Parliament, the Council and the Management Board on the evaluation findings. The findings of the evaluation shall be made public.

Article 121
Repeal and continuation of activities

1. Regulation (EU) 2019/881 of the European Parliament and of the Council is repealed with effect from DDMMYYYY.

2. References to Regulation (EU) 2019/881, ENISA and European cybersecurity certification schemes as established by that Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table set out in Annex III to this Regulation.

3. ENISA as governed by this Regulation shall continue operations and activities of ENISA as established by Regulation (EU) 2019/881 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) 2019/881 shall remain valid, provided that they comply with this Regulation.

4. The Executive Director appointed pursuant to Article 15(1), point (n) of Regulation (EU) 2019/881 shall remain in office and exercise the tasks and responsibilities of the Executive Director as referred to in Article 32 of this Regulation for the remaining part of the Executive Director's term of office. The other conditions of their contract shall remain unchanged.

5. The candidate schemes whose preparation was requested pursuant to Article 49 of Regulation (EU) 2019/881 shall be considered to have been requested pursuant to the corresponding provisions of this Regulation. The provisions of Title III of this Regulation shall apply to those candidate schemes accordingly.

6. The members of the Management Board appointed by the Commission and alternate members appointed pursuant to Article 14 of Regulation (EU) 2019/881 shall remain in office and exercise the functions of the Management Board as referred to in Article 27 of this Regulation for the remaining part of their term of office. The members of the Management Board appointed by Member States pursuant to Article 14 of Regulation (EU) 2019/881 shall remain in office and exercise the functions of

the Management Board as referred to in Article 27 of this Regulation provided that they hold functions referred to in Article 24(3) of this Regulation.

Article 122
Entry into force

This Regulation shall enter into force on the […] day following that of its publication in the *Official Journal of the European Union*.

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

Done at Strasbourg,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL AND DIGITAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE 3
1.1. Title of the proposal/initiative 3
1.2. Policy area(s) concerned 3
1.3. Objective(s) 3
1.3.1. General objective(s) 3
1.3.2. Specific objective(s) 3
1.3.3. Expected result(s) and impact 3
1.3.4. Indicators of performance 3
1.4. The proposal/initiative relates to: 4
1.5. Grounds for the proposal/initiative 4
1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative 4
1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone. 4
1.5.3. Lessons learned from similar experiences in the past 4
1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments 5
1.5.5. Assessment of the different available financing options, including scope for redeployment 5
1.6. Duration of the proposal/initiative and of its financial impact 6
1.7. Method(s) of budget implementation planned 6
2. MANAGEMENT MEASURES 8
2.1. Monitoring and reporting rules 8
2.2. Management and control system(s) 8
2.2.1. Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed 8
2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them 8
2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure) 8
2.3. Measures to prevent fraud and irregularities 9
3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE 10
3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected 10

3.2. Estimated financial impact of the proposal on appropriations 12
3.2.1. Summary of estimated impact on operational appropriations 12
3.2.1.1. Appropriations from voted budget 12
3.2.1.2. Appropriations from external assigned revenues 17
3.2.2. Estimated output funded from operational appropriations 22
3.2.3. Summary of estimated impact on administrative appropriations 24
3.2.3.1. Appropriations from voted budget 24
3.2.3.2. Appropriations from external assigned revenues 24
3.2.3.3. Total appropriations 24
3.2.4. Estimated requirements of human resources 25
3.2.4.1. Financed from voted budget 25
3.2.4.2. Financed from external assigned revenues 26
3.2.4.3. Total requirements of human resources 26
3.2.5. Overview of estimated impact on digital technology-related investments 28
3.2.6. Compatibility with the current multiannual financial framework 28
3.2.7. Third-party contributions 28
3.3. Estimated impact on revenue 29
4. DIGITAL DIMENSIONS 29
4.1. Requirements of digital relevance 30
4.2. Data 30
4.3. Digital solutions 31
4.4. Interoperability assessment 31
4.5. Measures to support digital implementation 32

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

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

(Text with EEA relevance)

Short title: The Cybersecurity Act 2 (CSA2)

And

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

1.2. Policy area(s) concerned

Policy area: 09 – Communications networks, content and technology

Activity: 09.02 digital single market

1.3. Objective(s)

1.3.1. General objective(s)

The main objectives of the intervention are:

(1) Enhance cybersecurity capabilities and resilience

Contribute to strengthen the Union's cybersecurity governance and helping to ensure that relevant institutions, authorities and other stakeholders are better prepared to prevent, detect, and respond to cybersecurity threats in a coordinated and effective manner.

(2) Prevent fragmentation across the internal market by:

Supporting the development, implementation and uptake of common Union cybersecurity instruments, such as certification schemes and providing harmonised frameworks that build trust and interoperability across Member States.

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

1.3.2. Specific objective(s)

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

Specific objective No 1: Create the capacity to effectively implement of Union cybersecurity policies and continuous operational cooperation enabling more structured cooperation between Member States.

Specific objective No 2: Develop and implement the means and mechanisms to effectively support and address the needs of Member States, industry and other stakeholders.

To address the limited uptake and effectiveness of the European Cybersecurity Certification Framework (ECCF):

Specific objective No 3: Create the prerequisites for faster delivery of cybersecurity certification schemes, driven by market needs, by broadening the scope of the ECCF, ensuring effective maintenance and agile procedures and increasing transparency.

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

Specific objective No 4: Create mechanisms and conditions to facilitate compliance with cybersecurity requirements, thereby making and in that way make their implementation more coherent and effective.

To address cybersecurity risks in the supply chain:

Specific objective No 5: De-risk critical ICT supply chains from entities established in or controlled by entities from countries posing cybersecurity concerns (high-risk suppliers) and reduce critical dependencies by developing a coherent and effective framework at EU level to address ICT supply chain security risks.

1.3.3. Expected result(s) and impact

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The expected results are as follows:

(1) Functional reform of ENISA

(2) Reform of ECCF – scope extension, new procedure and revised governance

(3) Further simplification of compliance with relevant Union cybersecurity legislative framework

(4) Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks

Overall impact:

The proposal will have an immense impact on the cybersecurity in the Union as it tackles number of areas such as the needed reinforcement of the European Union Agency for Cybersecurity, strengthens the support for the implementation of the EU law, introduces reforms for smooth implementation of the European certification framework, supports the Union's joint understanding of the cyber threats and addresses the mitigation of cybersecurity risks according to the geopolitical reality. The implementation of the proposed provisions will ensure high levels of efficiency and coherence and avoid excessive regulatory burden. The package is designed to be resilient to implementation challenges and to support long-term policy coherence across the digital and cybersecurity ecosystem. It improves clarity, removing inefficiencies and aligning procedures across legal frameworks, while contributing to achieving high level of cybersecurity across the EU. As one of the main priority objectives of the EU Commission, the envisaged simplification efforts will yield significant economic benefits for businesses, including SMEs, of more than EUR 14.63 billion and for public authorities of EUR 7.5 million.

Specific results include:

- increased awareness and improved operational coordination, which could generate considerable costs savings related to faster incident detection and response for businesses, public authorities and citizens;
- providing clarity of the scope and remit of ENISA, while ensuring the necessary prioritisation of its primary tasks;
- ensure that the stakeholders receive adequate support for policy implementation, operational activities and overall coordination;
- Support Union's shared situational awareness
- enhanced cooperation with EU-CyCLONe, the CSIRTs network, the Commission, Europol and CERT-EU and relevant Union entities with the aim to develop a repositories of verified, reliable cyber threat intelligence;
- support the efforts of mitigating ransomware attacks;
- enhanced coordination with private sector on cybersecurity related topics;
- disseminating timely information through early alerts on significant or large-scale incident, or a cyber threat of a cross-border nature, in relation to sectors listed in Annexes I and II to Directive (EU) 2022/2555;
- foster effective synergies with other EU bodies and agencies;
- lower the price of skills certifications, including by increasing the offering on the market by introducing the European skills attestation schemes;
- support closing the skills gap in Europe through individual cybersecurity skills attestations and support Member States and industry in strengthening their workforce;
- addressing the lack of clarity of the ECCF framework and its limited impact, expanding its scope and improving its governance model;
- increase the reputation of adopted schemes by establishment of a maintenance structure and the introduction of a timely and transparent development process;
- introducing fees mechanism in relation to the costs occurring for developing and maintaining the European individual cybersecurity skills attestation schemes and processing applications and granting authorisations to providers, and for maintenance of schemes, adopted under ECCF, which will contribute to the Agency financial stability and create savings under the EU budget;
- aligned European certification schemes with the existing legislative framework and hence better serve implementation efforts and support compliance needs of businesses;
- enabling the adoption of currently blocked schemes;
- foster competitiveness of European companies by promoting alignment between international and European standards;
- limiting fragmentation in cybersecurity measures and requirements;
- providing for legal clarity and substantially reducing the administrative burden, without leading to significant legal uncertainty among stakeholders that are in the process of adapting to the recently adopted legal frameworks;

- facilitate compliance for NIS2 entities, which would also contribute to a better compliance rate overall and more meaningful cybersecurity measures put in place, while making the supervision process on the authorities' side more efficient;

Other

- SMEs would have numerous positive impacts from the initiative considering improved competitiveness within EU cybersecurity market, as well as reduced costs and administrative burden:

1. *Positive role on SMEs who would benefit from increased cyber resilience due to an enhanced role of ENISA and technical guidance, provided by the Agency.*
2. *SMEs as authorised provider to issue attestations under the European skills attestation scheme will gain visibility, reputation and gain customers. In addition, the European individual cybersecurity skills attestations will support SMEs in identifying candidates with the right skillset.*
3. *Well-functioning European certification schemes can ease the choice of trusted ICT technologies for SMEs and contribute to enhance their overall cyber resilience.*
4. *As DNS providers, SMEs will benefit from measures related to the implementation of the NIS2 Directive due to the exclusions from the scope of DNS providers.*
5 *SMEs would benefit from the scope clarifications that would limit the application of the obligations to certain entities in some sectors listed in NIS2 Directive.*
6. *For ICT supply chain security measures, SMEs in general, would benefit from the use of trusted technologies. As suppliers active in the sectors subject to restrictions, they would be impacted more heavily compared to larger companies by substitutions and transactions cost. However, SMEs as trusted suppliers will benefit from new market opportunities.*

- No significant environmental impact is expected for any of the objectives.
- With regard to the EU budget, efficiency gains can be expected by increased cooperation and coordination of the activities between EU institutions, agencies and bodies. Savings are expected in the long term through the introduction of fees mechanisms.

1.3.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Objective: Create the capacity for effective implementation of EU cybersecurity policies and regular/continuous operational cooperation enabling more structured cooperation between Member States.

- Number of relevant contributions from ENISA to the implementation of EU and national policies and legislative initiatives

- Positive feedback by stakeholders regarding the relevant ENISA contributions

- Increase by 25 % compared to 2023 baseline as reported in ENISA Annual Activity Report (for the number of relevant contributions) and as per ENISA's annual satisfaction survey (for the positive feedback)

- Usage statistics of EU Vulnerability Database

- Increase by 25 % of number of users compared to 2025

Availability, security and functioning of the CRA Platform

- Decrease by 25% downtime of the platform and number of incidents compared to 2025 Statistics on downtime and incidents in the platform

Objective: Develop and deploy the means and mechanisms to effectively support and address the needs of Member States, industry and other stakeholders.

- Number of stakeholders supported by ENISA and quality of the provided support.

- Number of measures deployed to support stakeholders.

- Increased by 10% number of supported stakeholders and increased by 10% satisfaction level of supported stakeholders compared to 2025

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

- Number of adopted schemes

- Decreased time to develop a scheme by 50% compared to 2025

- Number of valid certificates issued annually

- Increase by 25 % over 2025 baseline

- Positive feedback of stakeholders regarding their involvement in scheme development and transparency of the ECCF

- Increase by 25 % over baseline in ENISA's annual satisfaction survey compared to 2027

Objective: Establish mechanisms and conditions to help facilitate compliance with cybersecurity requirements and in that way make their implementation more coherent and effective.

- Percentage of SMEs cost for compliance with NIS2 and cybersecurity rules, as a proportion of all compliance costs

- >70 % SMEs reporting reduction in compliance costs for cybersecurity compared to 2025

- Number of ransomware attacks and amount of damages in EUR

- Reduce number of ransomware attacks by > 1% compared to 2027

- Percentage of cross-border incidents during or after which Member States' authorities used mutual assistance mechanisms

- Increase proportion of cases where mutual assistance was used by >20 percentage points compared to 2025

Objective: Reduce critical dependencies by developing a coherent and effective framework at EU level to address ICT supply chain security risks.

- *Number of measures adopted*

- *Increase by 25% of number of measures adopted and key assets identified compared to adoption date + 6 months*

- *Decrease of dependencies on high-risk suppliers in key ICT assets by 25% compared to 2025*

1.4. The proposal/initiative relates to:

☒ a new action *(Title IV Supply Chain, Title V Simplification)*

☐ a new action following a pilot project / preparatory action[84]

☒ the extension of an existing action (*Title II ENISA's mandate and Title III Certification*)

☐ a merger or redirection of one or more actions towards another/a new action

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

In July 2024, in its Political Guidelines[85], the President of the European Commission Ursula von der Leyen called for simplification, consolidation, and codification of EU legislation to eliminate any overlaps and contradictions while maintaining high standards. The Mission Letter to EVP Virkkunen[86] in particular mentions improving the adoption process of European cybersecurity certification schemes and the need to protect our industries, citizens and public administrations against internal and external threats. Furthermore, the 2024 Niinistö[87] report calls for de-risking undesirable supply chain dependencies in critical technologies. Central aspects of the commissioned by the EU President, Draghi[88] and Letta[89] reports reflected on the need the single market to stay competitive through simplification and ensure highest levels of security and strategic autonomy. Taking on this, the revision of the CSA is a cornerstone in the Commission's work on security and a roll out of an ambitious revision of the European cybersecurity regulatory ecosystem. The CSA2 proposal is introducing mechanisms to address cybersecurity risks in the supply chain and mechanisms to reduce the fragmented compliance landscape and complexity of horizontal and sectoral frameworks. It is expected that ENISA will be also a vehicle to lead to greater simplification in reporting obligations through integrating a Single Entry Point.

In addition, in view of the number of sectorial provisions introduced post 2019 adoption of the CSA, as well as the fast evolving cybersecurity threat landscape, ENISA's mandate needs to be reviewed, to lay down more focused and renewed set of tasks, with a view to effectively and efficiently supporting Member States, EU institutions and other stakeholders' efforts to ensure a secure cyberspace in the

84 As referred to in Article 58(2), point (a) or (b) of the Financial Regulation.
85 Political Guidelines 2024
86 Mission letter EVP Virkkunen
87 Report by Sauli Niinistö
88 The Draghi report on EU competitiveness
89 Enrico Letta - Much more than a market (April 2024)

European Union. Through the reinforcement of the European Cybersecurity Certification Framework (ECCF), the proposal is ensuring that the EU has a lean, modern and adaptable certification system that will serve the purposes of supply chain actions and the swift implementation of the Cyber Resilience Act. In conclusion, the suggested scope of the mandate is delineated, strengthening those areas where the Agency has shown clear added value and adding those new areas where support is needed in view of the new policy priorities and instruments and to reinforce the ECCF.

The CSA revision is therefore designed to be a major step-change in the EU cyber posture and the overall security, preparedness, and resilience of the European Union.

1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone.

Cybersecurity Act was adopted in 2019 with the legal basis of Article 114 TFEU, which empowers the EU legislator to adopt measures harmonising national laws and regulations that have as their objective the establishment and functioning of the internal market.

The revised CSA proposal aims at streamlining of the cybersecurity legislation at EU level, supplementing and reviewing the current Cybersecurity Act, in force as of 2019 (CSA1). The objectives under CSA1 to give permanent mandate to European Union Agency for Cybersecurity, dedicated to support the high common level of cybersecurity across the EU, as well as for the purpose of avoiding the fragmentation of the internal market regarding cybersecurity certification schemes, are kept in within the initiated revision. Those objectives, as already duly analysed within the proposal of Cybersecurity Act in 2017, cannot be sufficiently achieved by the Member States, but only at European Union level in accordance with Article 5 of the Treaty on European Union.

The proposal for the revision of the CSA has a clear focus on streamlining, prioritising and codifying tasks across cyber-related legislations could be achieved only at EU level and there isn't such initiative that currently exists. The new proposal further strengthens supply chain security and the cybersecurity sector within the EU and enhance the preparedness and resilience of the Member States and industry. Dependencies on entities established in or controlled by entities from third countries posing cybersecurity concerns (high-risk suppliers) affect entities across the Union, while significant supply chain cybersecurity incidents often spread across national borders. Addressing the issue at national level alone is not likely to be efficient.

The newly assigned tasks for ENISA are of pivotal importance to achieve high levels of cybersecurity across the EU. Despite the fact that the Agency is working in coordination with other EU security bodies, such as Europol, as well as the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), which is responsible for funding implementation, the Agency mission and tasks are unique and currently there is no other body carrying this type of responsibilities. In the EU cyber ecosystem all entities involved are working in tight synergies and within clear mandates. Therefore, the CSA2 proposal reinforces only those parts

where there is clear added value, making sure there are no ambiguities in terms of duplication of tasks, on substance, but also in funding with other bodies within the cyber ecosystem.

In more detail

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

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

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

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

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

By default, cyber-attacks have cross border nature, especially considering spillover effects that could arise from initially single affected entry point. The threats and risks to the cybersecurity have an impact for the whole European Union and therefore a collective situational awareness picture could significantly improve the levels of cybersecurity of the entities within the European Union. The proposals within the revised mandate of ENISA address this issue with the objective to significantly increase the EU cyber resilience.

In conclusion, EU intervention is crucial as cybersecurity threats and related challenges extend beyond individual Member States. Fragmented national solutions have proven insufficient to achieve market-wide trust and coordination. A revised EU legal framework is required to remove barriers, ensure consistent

implementation, and support Member States in an increasingly complex regulatory and threat environment.

1.5.3. Lessons learned from similar experiences in the past

ENISA has been founded in 2004 with a fix-term mandate. In 2019 the Cybersecurity Act entered into force, which provisions granted ENISA with a permanent mandate and an objective of becoming the centre of cyber expertise in Europe. Today, ENISA is a recognised brand and trusted partner among the EU stakeholders. The competences of the Agency were gradually built in the course of 25 years, reflecting the evolving cyber ecosystem.

According to Article 67 of the CSA, every five years the Commission shall evaluate the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need for modifications and the financial implications of such modifications. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions in relation to the European certification framework.

According to the provisions, the Commission has carried out an evaluation of the Agency and the European Cybersecurity Certification Framework, which included a public consultation and an independent study. In accordance with the better regulation practices, the Commission has also launched a public consultation specifically on the revision of the CSA, as well as call for evidence to gather data from the stakeholder groups. The evaluation came to the conclusion that ENISA has fulfilled its mandate by delivering nearly all planned outputs. Agency's objectives remain relevant today with especially recognised output by stakeholders during challenging times such as the COVID-19 pandemic and Russian war of aggression on Ukraine. Despite the generally positive feedback from stakeholders on ENISA's outputs, it was also shown that there is significant room for improvement to meet stakeholder expectations consistently.

The lessons learned have demonstrated that to raise the level of efficiency, ENISA would need more strategic focus, task prioritisation and strengthening its capacity of providing timely insights into emerging threats and strategic tools for addressing them. Moreover, as indicated by a number of stakeholders, ENISA could establish more structured and transparent methods of engaging with private entities, with an emphasis on supporting SMEs. In all external consultations, it was emphasised the importance of increasing ENISA's funding, staffing and operational capacity to enable it to meet the growing demands of the EU's cybersecurity landscape. In its evaluation report, following the study, the Commission services assessed a clear need of future-proof legislation that can adapt to the complex and fast evolving cyber threat landscape, and respectively to reinforce the Agency with the needed resources to ensure the support towards highest levels of cybersecurity in Europe. Based on gathered data and the experience from implementation of the CSA, it was drawn the conclusion that coordination with other bodies should be streamlined, as well as to put focus on the support from ENISA for the implementation of EU law and to the support to the Commission, upon request, for drafting of cybersecurity related legislation. The proposal is looking into synergies with the geopolitical priorities of the Commission to address risks such as the increasing dependencies from entities established in and controlled by countries posing cybersecurity concerns (high-risk suppliers) in Europe. As centre of expertise, ENISA is currently also an essential repository of information that is crucial for building a common understanding regarding the threats and risks posed to the EU entities. Therefore, the proposed

framework is building on the experience from CSA1 and is mobilizing the coordination of the information flows with the view of compiling a holistic situational awareness picture.

The evaluation of the ECCF reveals several strategic recommendations. Despite ENISA's pivotal role in fostering cooperation and operational cohesiveness among Member States and other stakeholders, constraints on the efficiency and effectiveness of the ECCF have been evident mainly due to the complexities of scheme adoption processes. These issues highlighted the necessity for a substantial revision in governance structures to enhance operational clarity and accountability at all levels, which the CSA proposal for revision is addressing. The experience of the functioning the current ECCF has shown the need to modernise and clarify the certification framework and introduce maintenance procedure for certification schemes to enable them to match the market needs and threat landscape. Finally, the original framework has not anticipated non-technical risks, which can be identified as a source of stalled implementation of ECCF on 5G and cloud schemes.

The complexity in the EU cyber ecosystem has been on the rise according to the evolving cyber threats. In the written submissions from stakeholders, there was a strong consensus on the need to reduce the administrative burden, particularly for SMEs and called for simplified compliance procedures. While the main simplification effort will be channelled through the Digital Omnibus initiative, the proposal reflects the stakeholders' needs by introducing changes to the NIS2 Directive to ease the implementation process

1.5.4. *Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments*

CSA2 introduces the needed revisions to equip the EU with tools and mechanisms to respond to the cybersecurity landscape and policy objectives. The proposed regulation will further reinforce ENISA with the necessary capabilities to support the Member States in the implementation of EU law and in countering cyber risks. Taking into consideration the already mentioned above Draghi and Letta reports, the proposal for Multiannual Financial Framework (MFF) 2028-2034 puts competitiveness, security and strategic autonomy in its centre.

As a result, the proposals within the MFF 2028-2034 horizontal package, notably the European Competitiveness Fund and the Horizon Europe proposals, introduce new eligibility criteria based on the principle of exclusion of "high-risk suppliers" from receiving EU funds. The CSA2 is fully aligned with this principle, and furthermore, it represents a tool to enable the implementation of the new "high risk supplier" requirements as it gives a procedural framework to designate countries posing cybersecurity concerns at the EU level. In this respect, CSA2 is a strategic proposal, in line with the Commission priorities for achieving technological sovereignty and boosting the competitiveness within Europe.

Overcoming existing fragmentation will be tackled through further harmonisation on the EU certification market, making the European certification process more efficient and sustainable.

The MFF proposals for 2028-2034 takes the simplification effort as a priority throughout the whole framework. The budgetary headings are compressed to 4 instead of 7, while the number of the horizontal funding programmes has been reduced significantly from 52 to 16, offering flexibility and adaptability to current

needs. The impact assessment for the revision of the Cybersecurity Act stressed exactly on these objectives: necessity to simplify the cybersecurity requirements across multiple legislative frameworks, codify and focus the tasks of ENISA on the areas with most impact for achieving enhanced resilience of the EU cyber ecosystem. Following these findings, the proposed provisions boost the competitiveness through simplification; ensure high levels of security by enhanced coordination and analysis of risks and vulnerabilities; support higher levels of harmonisation through overcoming fragmentation, posed by number of national schemes. Furthermore, ENISA is designed to be main vehicle that will drive digital simplification efforts as it will integrate the Single Entry Point for notifications, as outlined in the Digital Omnibus initiative[90].

An essential part of the MFF 28-34 package is the proposal for a new Competitiveness Fund (ECF), which brings under one roof more than 16 funding programmes such as Digital Europe Programme (DEP), Health4EU, European Defence Fund, etc. Horizon Europe (HEP) will continue to be a standalone programme, tightly interlinked with ECF. This new programming framework calls for strong coordination and funding that corresponds to current priorities. In this line, the proposed provisions in CSA2 are the foundation for deepening the coordination between ENISA and the ECCC, responsible for program implementation of the cybersecurity related parts of DEP and HEP. The proposed provisions ensure coherence and stress on the synergies between ENISA and the ECCC. The same approach has been taken towards the cooperation with other agencies and bodies, such as Europol.

Another aspect of alignment between the CSA2 proposal and MFF 28-34 is in the principle of flexibility. With the revision, the Commission proposes a "fee" mechanism, which will give ENISA an agile way to finance partly its activities, more specifically related to the cybersecurity skills attestation schemes' development and maintenance, and the processing and granting of authorisations to providers, and the maintenance of European cybersecurity certification schemes. With this change the Agency will have the flexibility and scalability to respond to the stakeholders' needs and have sustainable expenditure through refinancing its services.

1.5.5. Assessment of the different available financing options, including scope for redeployment

Since the last revision of ENISA's mandate in 2019, the trend has been towards an exponential growth of the Agency's expected contributions towards the support for the implementation of the EU law. This led to requests for yearly budget and staff reinforcements above the levels initially programmed. The proposed revision introduces important new tasks, as well as brings in the ENISA's mandate tasks, which were imposed by other legislative acts after the CSA1 was adopted, hereby extending ENISA's capabilities, which requires additional financial and human reinforcements. Driven by the aim to make digital security Europe's competitive advantage, the proposal calls for real impact within the cyber ecosystem. This could be only possible with significant investment that corresponds to the desire effect and most of all – needs of the Member States and other stakeholders. The new tasks include the need of technical and specialised personnel, as well as financial

[90] To be added once published

investments (i.e. for tools and platforms), which could be secured only through additional financial allocation from the EU budget.

With the objective for enhanced flexibility and in the same time long term sustainable budget of the Agency, the revision proposes a fee mechanism which will partially finance the services provided for maintenance of the cybersecurity certification framework and in relation to developing and maintaining European individual cybersecurity skills attestation schemes and processing and granting authorisations to providers.

All estimations for additional resources in the revision of CSA are made from the perspective of the baseline budget of ENISA in 2025 (operational costs and FTEs). Commission has made an extensive analysis for the redeployment possibilities within the Agency to accommodate the new tasks envisaged in the revised mandate. The fact that the Agency is working on its maximum capacities with no options for reduction of tasks and already a deprioritisation action taken by the Management Board in 2023, clearly leads to the conclusion that no new tasks can be accommodated under the current structure, without reinforcing both the budget and the human resources. In addition, many of the current tasks are covered by contribution agreements between ENISA and the Commission. Therefore, the proposal is aiming to add those tasks to the mandate of ENISA and receive stable budget for the upcoming years.

Without prejudice to the negotiations on the next MFF, the appropriations allocated to the Agency from 2028 onwards will be compensated via redeployments from programmes under the 2028-2034 MFF. If a compensatory reduction is needed, the resources allocated to the Agency and their funding streams and sources may need to be revised. The measures put in place in the proposed CSA2 framework also entail the take up of additional tasks for the partner DG of ENISA (Directorate-General Communications Networks, Content and Technology, DG CNECT). It should be especially noted that the ICT supply chain framework will be fully implemented at Commission level, including market analysis accompanying the risk assessments and preparation of implementing acts. Moreover, additional set of implementing acts drafted and adopted by the Commission will be required, in relation to modalities of the fee mechanisms. Additional supervision and assistance at Commission level will be required for the enforcement of the European cybersecurity certification framework, development of model provisions, maintenance of cybersecurity schemes, mutual recognition agreements with third countries and ENISA oversight.

1.6. Duration of the proposal/initiative and of its financial impact

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☒ **unlimited duration**

– Implementation with a start-up period from YYYY to YYYY,

– followed by full-scale operation.

1.7. Method(s) of budget implementation planned

☐ **Direct management** by the Commission

– ☐ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated

– ☐ international organisations and their agencies (to be specified)

– ☐ the European Investment Bank and the European Investment Fund

– ☒ bodies referred to in Articles 70 and 71 of the Financial Regulation

– ☐ public law bodies

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees

– ☐ bodies or persons entrusted with the implementation of specific actions in the common foreign and security policy pursuant to Title V of the Treaty on European Union, and identified in the relevant basic act

– ☐·bodies established in a Member State, governed by the private law of a Member State or Union law and eligible to be entrusted, in accordance with sector-specific rules, with the implementation of Union funds or budgetary guarantees, to the extent that such bodies are controlled by public law bodies or by bodies governed by private law with a public service mission, and are provided with adequate financial guarantees in the form of joint and several liability by the controlling bodies or equivalent financial guarantees and which may be, for each action, limited to the maximum amount of the Union support.

Comments

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

The monitoring and reporting will follow the principles outlined in the current CSA Regulation[91], Financial Regulation[92] and in line with the Common Approach on decentralised agencies[93].

According to Article 40 of the Financial Regulation, ENISA must send each year to the Commission, the European Parliament and the Council a Single Programming Document (SPD) containing multi-annual and annual work programmes and resources programming. In addition, the Commission proposal for amending ENISA mandate introduces the requirement for the Commission, as a member of the Management Board, to cast a positive vote for the Management Board of ENISA to adopt the SPD, for matters, related to human resources and budget. The Commission will also issue an opinion on the draft SPD before the voting procedure in the Management Board takes place, which should be implemented before adoption of the SPD[94].

ENISA must submit a Consolidated Annual Activity Report to the Management Board. This report notably includes information on the achievement of the objectives and results set out in the Single Programming Document. The report must also be sent to the Commission, the European Parliament and to the Council. ENISA's Executive Director should present to the Management Board an ex-post evaluation of ENISA's activities every two years. The Agency should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress bi-annually to the Commission. The Management Board should be responsible to monitor the adequate follow-up of such conclusions.

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

The data sources for planned monitoring would mostly be ENISA, the European Cybersecurity Certification Group, the NIS Cooperation Group, the CSIRTs Network and the Member States' authorities. Besides the data deriving from the reports (including the annual activity reports) of ENISA, the European Cybersecurity Certification Group, the NIS Cooperation Group and the CSIRTs Network and the Commission specific data gathering tools will be used when needed (for example surveys to national authorities, Eurobarometer, dedicated studies and reports from the pan-European exercises).

The Commission proposal for CSA2 continues the established review practice and evaluation of the Agency. As outlined in Article 119 of the proposal for CSA2, the Commission must commission an evaluation of ENISA by [DD MM YYY] and every five years after that. This evaluation will assess, in particular the possible need to modify the mandate of ENISA, and the financial implications of any such

91 The EU Cybersecurity Act | EUR-Lex

92 Financial regulation applicable to the general budget of the Union (recast) - Publications Office of the EU

93 https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf

94 Delegated regulation - 2019/715 - EN - EUR-Lex

modification. On the occasion of every second evaluation, there shall be an assessment of the results achieved by ENISA having regard to its objectives, mandate, mission, governance and tasks, including an assessment of whether the continuation of ENISA is still justified with regard to these objectives, mandate, mission, governance and tasks.

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

The evaluation shall also assess the impact, effectiveness and efficiency of provisions of Title IV of the Regulation with regard to the objectives of the ICT supply chain security framework.

The Commission shall report to the European Parliament, the Council on all the findings and to the Management Board on the evaluation findings for Title II of the Regulation. The findings of the evaluation shall be made public.

2.2. Management and control system(s)

2.2.1. Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

Considering that the proposal impacts the annual EU contribution to ENISA, the EU budget will be implemented via indirect management.

Pursuant to the principle of sound financial management, the budget of ENISA shall be implemented in compliance with effective and efficient internal control. ENISA is therefore bound to implement an appropriate control strategy coordinated among appropriate actors involved in the control chain.

Regarding ex-post controls, ENISA, as a decentralised agency, is notably subject to:

- internal audit by the Internal Audit Service of the Commission
- annual reports by the European Court of Auditors, giving a statement of assurance as to the reliability of the annual accounts and the legality and regularity of the underlying transactions
- annual discharge granted by the European Parliament
- possible investigations conducted by OLAF to ensure, in particular, that the resources allocated to agencies are put to proper use.
- As partner DG to ENISA, DG CNECT will implement its Control Strategy on decentralised agencies to ensure reliable reporting in the framework of its Annual Activity Report (AAR). While decentralised agencies have full responsibility for the implementation of their budget, DG CNECT is responsible for regular payment of annual contributions established by the Budgetary Authority.
- Finally, the European Ombudsman provides a further layer of control and accountability at ENISA.

Based on the evaluation of the Agency and the Impact Assessment that was conducted presenting the proposal for CSA2 Regulation, it was determined that it is

of utmost importance to ensure adequate financial resources in order for ENISA to fulfil the tasks entrusted by the new mandate. An important novelty for the Agency revised mandate will be the introduction of fees mechanism that is envisaged to finance the costs for the maintenance of European cybersecurity certification schemes, adopted under the ECCF. The revised ECCF will formalise the maintenance procedure. The maintenance activity will be led by ENISA and partially financed by fees to cater for its scalable nature (more schemes require more personnel to maintain). The Agency will also be equipped with the ability to deliver testing tools to support the implementation of conformity assessment procedures both under the ECCF and other relevant EU cyber legislation. The modalities on the fees will be arranged in an implementing act, adopted by the Commission. Additionally, the revision is envisaging developing and maintaining European individual attestation schemes and issuing decisions on authorising providers to deliver European individual cybersecurity skills attestations.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The proposal for CSA2 as such aims at mitigating identified risks within ENISA mandate and the ECCF framework, including ICT supply chain security framework and simplification provisions. More specifically, ENISA is an European Union agency that already exists and in the revision, the mandate is further delineated, strengthening those areas where the Agency has shown clear added value and adding those new areas where support is needed in view of the new policy priorities and instruments, such as simplification through the integration of a Single Entry Point for reporting; support for a common European situational awareness picture and operational cooperation, reinforced and streamlined European Cybersecurity Certification Framework.

Another identified risk, and addressed in the proposal, is the number of contribution agreements that the Commission and the Agency have concluded in the recent years. Due to the current geopolitical situation and rapidly evolving cybersecurity threat landscape, the Commission has concluded contribution agreements with the Agency for more than EUR 75 million in total since 2019. Considering that the tasks entrusted to ENISA in those agreements have as of now permanent nature, the unstable flow of budget through contribution agreements poses a risk for the long-term delivery of the outputs of ENISA's activities.

Therefore, the current proposal is among others, reinforcing the Agency's resource capacity, redefining its tasks and resulting in efficiency gains. In particular, the possibility to collect fees will in long term support a sustainable financial circuit of the Agency through refinancing the costs related to the maintenance of European certification schemes, adopted under ECCF, the testing of tools and to the development, maintenance and implementation of European individual cybersecurity skills attestation schemes. In the long run, it is estimated to achieve savings for the EU budget by reaching EUR 18.5 million per year. The Commission will be in the lead for the modalities of the fees and their composition through the adoption of implementing acts.

The increase of operational tasks for the Agency does not represent a real risk. These tasks would be complementing the action of Member States and supporting them,

upon request. They will also be limited to predefined services, by analogue of the Cybersecurity Act (EU) 2019/881[95]. The new elements/tasks in the proposal will bring the added value for the European stakeholders that would benefit from ENISA being an information hub, contributing to information sharing and providing alert notification to their constituents.

Furthermore, the proposed model of the Agency is aligned with the Common Approach of the Commission towards decentralised agencies, ensuring that there is a sufficient control to foresee that ENISA works towards its objectives. The operational and financial risks of the proposed changes seem to be limited, as the provisions are composed to mitigate current risks. Nevertheless, certain negative aspects might be expected in the long term, in relation to:

- strained operational resources due to increasing operational needs from Member States and constantly evolving cyber risks and threats in the area of cybersecurity.

- rapidly increased budget with expectations for fast implementation.

- lack of adequate levels of financial and human resources to match operational needs.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure)

The cost incurred by DG CNECT for the monitoring and the supervision of entrusted entities, including ENISA, is approximately EUR 5.25 million, as reported in the Annual Activity Report for 2024[96]. This amount includes primarily personnel costs and represents 0.50% of the operational payments made to these entities during 2024. The overall rate of the cost of control slightly increased to 0.50% in 2024 from 0.46% in 2023, but remains relatively stable compared to previous years.

More specifically, what concerns ENISA, the costs of control in 2024 amounts to EUR 0.32 million or 0.70% cost of control in 2024, compared to 0.69% in 2023, and 1.22% in 2022. The analysis shows that higher costs of control are mostly associated to the preparation and monitoring of contribution agreements between the Commission and the Agency (human resources cost mainly), which is expected to be significantly reduced in the new mandate and as a result higher levels of efficiencies are expected. In terms of overall costs for DG CNECT compared to the other entrusted entities, ENISA is in the middle, compared to 11 other entities.

The proposal for CSA2 envisages increase in DG CNECT personnel with 50 FTEs, of which 1 additional FTE will be specifically assigned for the tasks in relation to DG CNECT being a partner DG to the Agency. This person will be supporting the preparation of Commission opinion on the ENISA single programming document and monitor its implementation; support the supervision of the preparation of the Agency's budget and monitor its implementation. Assist the Agency in developing its activities in line with the Union policies including by participating in relevant meetings. The action is justified by the increased monitoring tasks for DG CNECT, which among others envisage casting positive vote of the Commission on issues related to budget

95 https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
96 CNECT_AAR_2024_final

and HR. It should be noted that the implementation of the provisions in relation to the designation of countries posing strategic cybersecurity risks for specific key assets high-risk suppliers will be fully Commission driven process. The estimated personnel needed for the risk assessments in connection to the above are 25 FTEs. The action is justified by the volume of the work the implementation of the policy framework calls for, more specifically the support to the EU's coordinates risk assessments; economic analysis for each ICT product/service; the preparation of respective implementing acts and following the implementation of the framework; performing ownership and control assessments. The cost of controls for the Commission of implementing the supply chain framework is expected to be specifically impacted by the number of ownership and control assessments (OCA) the Commission will be performing. The results of this task, however, will contribute greatly to savings for the Member States when supervising the implementation of mitigating measures and obligations imposed on the NIS2 entities by the framework. Member States will be able to leverage the results of the OCA assessments directly, rather each one individually to spend resources on the same assessments needs. The reinforcement of the European Cybersecurity Certification Framework, standardisation and implementation of related activities, NIS2 Directive implementation(including respective implementation needs, fees implementing acts and support the maintenance of the certification schemes and skills attestation schemes) has been estimated at 19 FTEs, while the operational cooperation and situational awareness policies require additional 5 FTEs. Full description of the tasks in section 3.2.4.

ENISA, in its 2023 consolidated annual activity report[97], concluded positively on the assessment of their internal control systems and provided a clean declaration of assurance. In its annual report on EU agencies for the financial year 2023, the ECA issued a clean audit opinion on the accounts and a qualified opinion on the legality and regularity of payments underlying the accounts (also referred in 2.2.2). DG CNECT has taken note of the report, however concluded it does not have an impact on the effectiveness of CNECT's supervision. ENISA also reports regularly on the measures taken to prevent the reoccurrence of the findings and as for now, there are no indications that the error rate will worsen/be above 2% in the upcoming years.

Moreover, Article 80 (2) of ENISA's Financial rules[98] provides for the possibility for the agency to share an internal audit capability with other Union bodies functioning in the same policy area if the internal audit capability of a single Union body is not cost-effective.

In conclusion, considering the proposed increased size of the Agency by more than 100%, compared to the relatively low enhancement of the control costs, the analysis shows a satisfactory cost-effectiveness ratio. Having regard to all the available data, there is no indication that the expected error might be above 2%.

2.3. Measures to prevent fraud and irregularities

The European Union Agency for Cybersecurity will apply the highest standards applicable to preventing fraud and irregularities.

Payments for any service or studies requested are checked by the agency's staff prior to payment, taking into account any contractual obligations, economic principles and

97 enisa.europa.eu/sites/default/files/2024-11/2023 Consolidated Annual Activity Report_1.pdf

98 MB Decision 2019_8 Financial rules_adopted.pdf

good financial or management practice. Anti-fraud provisions (supervision, reporting requirements, etc.) will be included in all agreements and contracts concluded between the agency and recipients of any payments.

In order to combat fraud, corruption and other unlawful activities, the provisions of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council shall apply without restriction.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[99]	from EFTA countries [100]	from candidate countries and potential candidates [101]	From other third countries	other assigned revenue
	[XX.YY.YY.YY]	Non-diff.	YES	NO	NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

- New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries and potential candidates	from other third countries	other assigned revenue
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

99 Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
100 EFTA: European Free Trade Association.
101 Candidate countries and, where applicable, potential candidates from the Western Balkans.

	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

3.2. Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

– ☒ The proposal/initiative requires the use of operational appropriations, as explained below

3.2.1.1. Appropriations from voted budget

EUR million (to three decimal places)

Agency: ENISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
Budget line: <…….> / EU Budget additional contribution to the agency	€20,900	€20,594	€25,338	€26,801	€26,801	€26,301	€26,301	173,006

The appropriations / EU budget contribution to the agency will be compensated by a reduction of the envelope of the following programme <…….> / budget line: <…….> / in the year(s) : <…….> .

			Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**	
TOTAL operational appropriations	Commitments	(4)	€20,900	€20,594	€25,338	€26,801	€26,801	€26,301	€26,301	173,006	
	Payments	(5)	€20,900	€20,594	€25,338	€26,801	€26,801	€26,301	€26,301	173,006	
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	1,365	`1,365	1,470	1,785	2,100	2,415	2,625	**13,125**	
TOTAL appropriations under	Commitments		=4+6	€22,265	€21,959	€26,808	€28,586	€28,901	€28,716	€28,926	186,161

HEADING 2 of the multiannual financial framework										
	Payments	=5+6	€22,265	€20,890	€24,851	€26,254	€26,254	€25,754	€25,754	186,161

DG: CNECT	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
• Human resources	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**
• Other administrative expenditure	0	0	0	0	0	0	0	**0**
TOTAL DG CNECT Appropriations	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

TOTAL appropriations under HEADING 4 of the multiannual financial framework	(Total commitments = Total payments)	**2,328**	**2,328**	**3,104**	**3,492**	**3,880**	**4,268**	**4,850**	**24,25**

EUR million (to three decimal places)

	Year	Year	Year	Year	Year	Year	Year	**TOTAL MFF**

		2028	2029	2030	2031	2032	2033	2034	2028-2034
TOTAL appropriations under HEADINGS 1 to 4	Commitments	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38
of the multiannual financial framework	Payments	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

3.2.2. Estimated output funded from operational appropriations (not to be completed for decentralised agencies)

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2028**		Year **2029**		Year **2030**		Year **2031**		Enter as many years as necessary to show the duration of the impact (see Section1.6)						**TOTAL**	
	OUTPUTS																	
	Type [102]	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1[103]…																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		

[102] Outputs are products and services to be supplied (e.g. number of student exchanges financed, number of km of roads built, etc.).

[103] As described in Section 1.3.2. 'Specific objective(s)'

SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
TOTALS																		

3.2.3. *Summary of estimated impact on administrative appropriations*

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below

3.2.3.1. Appropriations from voted budget

(additional)

VOTED APPROPRIATIONS	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL 2028 - 2034
HEADING 4								
Human resources	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Other administrative expenditure	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Subtotal HEADING 4	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Outside HEADING 4								
Human resources	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**
Other expenditure of an administrative nature	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 4	**1,365**	**1,365**	**1,470**	**1,785**	**2,100**	**2,415**	**2,625**	**13,125**
TOTAL	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

3.2.4. *Estimated requirements of human resources (additional)*

– ☐ The proposal/initiative does not require the use of human resources

– ☒ The proposal/initiative requires the use of human resources, as explained below

3.2.4.1. Financed from voted budget

Estimate to be expressed in full-time equivalent units (FTEs)[104]

VOTED APPROPRIATIONS	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034
• Establishment plan posts (officials and temporary staff)							
20 01 02 01 (Headquarters and Commission's Representation Offices)	12	12	16	18	20	22	25
20 01 02 03 (EU Delegations)	0	0	0	0	0	0	0
(Indirect research)	0	0	0	0	0	0	0
(Direct research)	0	0	0	0	0	0	0
Other budget lines (specify)	0	0	0	0	0	0	0
• External staff (in FTEs)							

[104] Please specify below the table how many FTEs within the number indicated are already assigned to the management of the action and/or can be redeployed within your DG and what are your net needs.

20 02 01 (AC, END from the 'global envelope')		0	0	0	0	0	0	0
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0	0	0	0	0
Admin. Support line [XX.01.YY.YY]	- at Headquarters	0	0	0	0	0	0	0
	- in EU Delegations	0	0	0	0	0	0	0
(AC, END - Indirect research)		0	0	0	0	0	0	0
(AC, END - Direct research)		0	0	0	0	0	0	0
Other budget lines (specify) - Heading 4		0	0	0	0	0	0	0
Other budget lines (specify) - Outside Heading 4		13	13	14	17	20	23	25
TOTAL		**25**	**25**	**30**	**35**	**40**	**45**	**50**

The staff required to implement the proposal (in FTEs):

	To be covered by current staff available in the Commission services	**Exceptional additional staff**		
		To be financed under Heading 7 or Research	**To be financed from BA line**	**To be financed from fees**
Establishment plan posts		25		
External staff (CA, SNEs, INT)			25	

The estimated impact on expenditure and staffing for 2028 and beyond is indicative and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and annual budgetary procedure and the steering mechanism.

Description of tasks to be carried out by the sector DG within the Commission

Officials and temporary staff	**ENISA coordination (1)**: Represent the Commission in the Management Board of the Agency. Draw up Commission opinion on the ENISA single programming document and monitor its implementation. Supervise the preparation of the agency's budget and monitor its implementation. Assist the agency in developing its activities in line with the Union policies including by participating in relevant meetings. **Skills attestation schemes / Skills Academy (2)**: Additional personnel in CNECT will be needed to prepare implementing acts establishing fees that ENISA will charge applicants to become authorised providers, These implementing acts will be at least 12, one per each ECSF profile. **Supply chain** (25) Supporting preparation of the Union's coordinated risk assessments. Conducting economic analysis for each of the ICT product, service considered. Drafting the respective implementing acts on identification of key assets, proposed mitigation measures and designation of countries posing strategic cybersecurity risks for specific key assets, identification of high-risk suppliers, verifying exemption requests and preparing the Commission's decisions. Supporting implementation and supervision of adopted measures. **European Cybersecurity Certification Framework, standardisation and implementation of related activities, NIS2 Directive implementation (17)**: CSA enforcement, in particular governance of CABs (challenge of responsibilities) Stakeholder engagement (and Assembly) Mutual recognition with third countries Standardised implementing act development (detailed requests subject to consultations and development of model provisions) Scheme maintenance, legal review, comitology procedure Coordination with NIS CG and entity scheme maintenance Implementing acts under NIS2 Directive CABs alignment with CSA, presumption of conformity + standardisation¨ Coordination between market surveillance and NCCA Technical alignment between CRA and certification schemes **Operational coordination and situational awareness (5)**: Sectoral and threat actor expertise to contribute EU level situational awareness of threats to critical infrastructure including through emerging technologies Coordination with ENISA and other EU entities and networks to prepare for significant and large-scale cyber incidents
External staff	As above

Description of additional tasks to be carried out by ENISA:

Officials and temporary staff	Managing the EU Cybersecurity Reserve (country managers and support for the implementation, while the actual operational costs of the Reserve are covered as foreseen under the Cyber Solidarity Act) (10) CRA management of the Single Reporting Platform (SRP) (operation) (9) Vulnerability services linked to SRP (4) Extension of SRP to Single Entry Point (Development & operation) (8) Development of technical guidance, product security expertise and market analysis to support CRA implementation (7) Standardisation to support CRA implementation / Certification / NIS2 (4) Supporting the CRA market surveillance activities (4) Supporting conformity testing and security evaluations of products (4) Support the Member States in mutual assistance (3) Providing vulnerability management services, maintaining the EUVD and delivering advisory and enrichment functions (CVD) (15) Operational cooperation & Situational awareness - mitigating and support platforms such as CNW/CyCLONe; supporting the tasks in relation to alert notifications; support the enhanced coordination with other relevant entities to develop repositories of verified, reliable cyber threat intelligence (art. 11(1a) CSA2) (5) Support for critical sectors resilience (including healthcare cybersecurity Action Plan implementation) (4) Skills Attestation Scheme Development (2) Skills Attestation Scheme Maintenance and Oversight (6) Admin (Accountant for the fees/HR/IT) (8) Maintenance of certification schemes (11) Horizontal tasks - increased stakeholder engagement, drafting technical specifications and involvement in standardisation activities in support of schemes (1)
External staff	As above Two mandatory SNEs per Member State in order to support the activities of the Agency and serve as National Liaison Officers, with focus on operational cooperation, coordinated vulnerability disclosure. (13) The other 27 SNEs are envisaged as cost free and therefore have no budget implications.

Additional operational costs per year for ENISA 2028 2034:

Cost	Budget	Timeline	Explanation
Cybersecurity Skills website	EUR 750 000	50% in 2029 50% in 2030	To ensure transparency of procedures, the proposal requires ENISA to maintain a website with ECFS profiles,

			attestation schemes, information about fees for each scheme, recommended fees for each attestation and the list of authorised attestation providers.
Coordinated vulnerability disclosure (CVD)	EUR 1 million	As of 2028	The security of products and services used in our critical infrastructure depends very much on sharing in due time information about discovered vulnerabilities and how those can be mitigated.
Cybersecurity Threat Intelligence	EUR 3 million	As of 2028	For building a situational awareness picture done in cooperation, ENISA and the Commission.
Single Entry Point	EUR 8 million	EUR 6 million in 2028 EUR 500K in 2029 EUR 500K in 2030 EUR 500K in 2031 EUR 500K in 2032	To be able to deliver on the Commission's Digital Omnibus Proposal to simplify compliance with cybersecurity incidents and data breach reporting

			obligations by developing and maintaining a single-entry point.
CRA SRP maintenance and other	EUR 3 million	As of 2028	The SRP introduced by the co-legislators is the largest IT system ever developed in the history of ENISA and a key pillar of the CRA. The establishment is currently funded via a contribution agreement, but its day-to-day management will require FTEs (see above) as well as operational costs. ENISA has a key role to play to ensure the success of the Union's product security framework, the CRA.
Secure communication and cybersecurity maturity of ENISA	EUR 2 million +	EUR 1.1 million investment in 2028 (CyCLONe/CSIRTs platforms + sec comms) EUR 1 million per year maintenance as of 2029 EUR 1.5 million	Ensuring the cybersecurity of the Agency and communication tools.

		cyber maturity	
Cybersecurity Certification maintenance	EUR 1 400 000 million	2028 600K 2029 1 000 000 2030 1 200 000 2031 1 400 00 2032 1 400 000 2033 1 400 000 2034 1 400 000	Covered by fees (fully as of 2032)
Cybersecurity attestation schemes	EUR 212920	As of 2030 at 50% covered by EU budget	Fully covered by fees as of 2033

3.2.5. Overview of estimated impact on digital technology-related investments

Compulsory: the best estimate of the digital technology-related investments entailed by the proposal/initiative should be included in the table below.

Exceptionally, when required for the implementation of the proposal/initiative, the appropriations under Heading 4 should be presented in the designated line.

The appropriations under Headings 1-3 should be reflected as "Policy IT expenditure on operational programmes". This expenditure refers to the operational budget to be used to re-use/ buy/ develop IT platforms/ tools directly linked to the implementation of the initiative and their associated investments (e.g. licences, studies, data storage etc). The information provided in this table should be consistent with details presented under Section 4 "Digital dimensions".

TOTAL Digital and IT appropriations	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028 - 2034**
HEADING 4								
IT expenditure (corporate)	0	0	0	0	0	0	0	**0**
Subtotal HEADING 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Outside HEADING 4								
Policy IT expenditure on operational programmes	0	0	0	0	0	0	0	**0**

Subtotal outside HEADING 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Compatibility with the current multiannual financial framework

The proposal/initiative:

– ☒ can be fully financed through redeployment within the relevant heading of the multiannual financial framework (MFF)

Without prejudice to the negotiations on the next MFF, the appropriations allocated to the agency from 2028 onwards will be compensated via redeployments from programmes under the 2028-2034 MFF. If a compensatory reduction is needed, the resources allocated to the agency and their funding streams and sources may need to be revised.

– ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation

– ☐ requires a revision of the MFF

3.2.7. Third-party contributions

The proposal/initiative:

– ☒ does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Total
Specify the co-financing body					
TOTAL appropriations co-financed					

3.2.8 Estimated human resources and the use of appropriations required in a decentralised agency

Additional staff requirements (full-time equivalent units)

Agency: ENISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
Temporary agents (AD Grades)	5	11	17	19	19	19	19
Temporary agents (AST grades)	4	7	11	12	12	12	12
Temporary agents (AD+AST) subtotal	***9***	***18***	***28***	***31***	***31***	***31***	***31***
Contract agents	22	44	66	74	74	74	74

Seconded national experts	4	8	11	13	13	13	13
Contract agents and seconded national experts subtotal	26	52	77	87	87	87	87
TOTAL staff	35	70	105	118	118	118	118

Appropriations covered by the EU budget contribution in EUR million (to three decimal places)

Agency: ENISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 – 2034**
Title 1: Staff expenditure	4,488	8,466	12,507	13,648	10,584	10,012	9,537	**87,766**
Title 2: Infrastructure and operating expenditure								
Title 3: Operational expenditure	16,413	11,588	11,528	11,788	11,613	11,613	11,113	**85,240**
TOTAL of appropriations covered by the EU budget	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**

Appropriations covered by fees, if applicable, in EUR million (to three decimal places)

Agency: ENISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 – 2034**
Title 1: Staff expenditure		0,510	1,043	1,539	4,604	5,176	5,650	**18.522**
Title 2: Infrastructure and operating expenditure								**0.000**
Title 3: Operational expenditure								**0.000**
TOTAL of appropriations covered by fees	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**

Overview/summary of human resources and appropriations (in EUR million) required by the proposal/initiative in a decentralised agency

Agency: ENISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 – 2034**
Temporary agents (AD+AST)	9	18	28	31	31	31	31	*31*
Contract agents	22	44	66	74	74	74	74	74

Seconded national experts	4	8	11	13	13	13	13	13
Total staff	35	70	105	118	118	118	118	**118**
Appropriations covered by the EU budget	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**
Appropriations covered by fees (if applicable)	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**
Appropriations co-financed (if applicable)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
TOTAL appropriations	**20,901**	**20,564**	**25,078**	**26,976**	**26,801**	**26,801**	**26,801**	**173,922**

3.3. Estimated impact on revenue

– ☒ The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

  – ☐ on own resources

  – ☐ on other revenue

  – ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[105]						
		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
Article …….								

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

The fees mechanisms are related to three areas of activity of ENISA:

- Fees in relation to authorising providers under the European individual cybersecurity skills attestation schemes.

The fees in relation to this activity will be arranged in an implementing act, following the adoption of the revised Cybersecurity Act. However, to be able to estimate the investment needed and costs, calculations were made using an

[105] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20% for collection costs.

existing model in an EU Member State[106]. The model includes one off payment and an annual fee.

Fixed costs: EUR 8,540

Annual fee: EUR 800

The fees are meant to refinance the costs for this specific activity. The costs have been estimated at the level of EUR 1 064 600 over 5 years period. The specific costs of activities included in that number are related to the development and maintenance of schemes, including expenses of members of an ad hoc working group that would support ENISA in developing the schemes (reimbursement of expenses and payment of rapporteurs), missions to audit on-site providers, and training of assessors to ensure homogenous application of the schemes:

A) the ad hoc working group would cost EUR 800 000

B) training of two assessors per Member State would amount to EUR 129 600

C) auditing one entity per Member State would amount to EUR 135 000

(A + B + C) / 5 = EUR 212 920 costs per annum

The proposal envisaged a transition period and initial investment in the first three years. During the transition period the costs will be covered by the EU budget, and in year 4 and 5 we will have 50% coverage, year 6 and 7 – full application of the fees.

Year	Fees
2028	0
2029	0
2030	0
2031	106 460 (revenue)
2032	106 460 (revenue)
2033	212 920 (revenue)
2034	212 920 (revenue)

- Fees in relation to covering the costs for maintenance of a cybersecurity certification scheme, adopted within the European Cybersecurity Certification Framework (ECCF).

The fees in relation to this activity will be arranged in an implementing act, following the adoption of the revised Cybersecurity Act. The estimations for the costs of maintenance of a scheme are based on market analysis, included in the Impact Assessment of the proposal for revision of the Cybersecurity Act. The total costs of the activity for a 5 year span are calculated at EUR 5 600 000 for operational costs and EUR 7 100 000 for FTEs.

[106] Decision RR-02: Price list of SNAS services : https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf,

The annual cost of maintenance activities is being calculated based on the current experience as EUR 200 000 per one year of maintenance of a scheme[107] and 2 FTEs dedicated to such activities (with a yearly cost of EUR 125 887 per FTE), taking into account the envisaged year of adoption of such schemes. The expectations are the revenues from these fees to raise in progression with the adoption of every new scheme and with the gradual take-up of such schemes. So far there is one scheme adopted (EUCC) under the ECCF and first revenues from the maintenance of that scheme are expected in 2029. Costs are expected to be covered by 2032.

The estimated revenues have been calculated making specific assumptions for each potential scheme on following aspects: the expected uptake (number of certificates to be issued), length of validity of each certificate and number of active conformity assessment bodies. Substantial revenues are expected to arise from the uptake of a future cyberposture scheme.

Year Revenue (percentage of costs covered/Paid by EU budget)

2028 0

2029 250 000 (11%/ - EUR 1 350 000) – one scheme (EUCC)

2030 783 000 (29%/ - EUR 2 000 000) – three schemes (EUCC, ID Wallet, MSS)

2031 783 000 (25%/ - EUR 1 930 000) – three schemes (EUCC, ID Wallet, MSS)

2032 3 850 000 (122%/ - EUR 2 400 000) – five schemes (EUCC, ID Wallet, MSS, EUCS, 5G)

2033 4 000 000 (126%/ + EUR 685 000) – six schemes (EUCC, ID Wallet, MSS, EUCS, 5G, Cyberposture)

2034 4 500 000 (141%/ + EUR 825 000) – seven schemes

Fees in relation to testing tools to support conformity assessment procedures

The fees in relation to this activity will be arranged in an implementing act, following the adoption of the revised Cybersecurity Act. However, to indicate estimated costs and expected revenues, calculations were made based on estimates provided by ENISA and included in the Impact Assessment of the proposal for revision of the Cybersecurity Act. The costs related to support for testing and evaluation activities are estimated at:

FTEs: 4 per year

Operational costs: 800 K per year

Total costs: 6 500 000 M (5 years); per year: EUR 1 300 000

It is expected that for ENISA, the first year on-off investments would occur followed by maintenance costs. Those costs would be gradually covered by revenues collected from fees.

[107] Specifically, the maintenance considers 2 in person meetings with experts per year (EUR 100 000), costs of contractors supporting the development and review of supporting documentation for the scheme, the uptake of certification schemes, support the peer assessments and the implementation of conformity assessments (4 x 15 000 = EUR 60 000). The cost also includes operational part of the CEF platform and the ENISA certification website (EUR 40 000).

Year	Revenue
2028	0
2029	260 000
2030	260 000
2031	650 000
2032	650 000
2033	975 000
2034	975 000

4. DIGITAL DIMENSIONS

4.1. Requirements of digital relevance

High-level description of the requirements of digital relevance and related categories (data, process digitalisation & automation, digital solutions and/or digital public services)

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level Processes	Categories
Article 5(1)(a) Support for implementation of EU law	(a) assisting Member States in implementing Union policy and law regarding cybersecurity consistently, including by **issuing technical guidance and reports, by providing advice and sharing best practices, and by facilitating the exchange of best practices between competent authorities in this regard**;	- ENISA - Member States	- processing data in order to issue technical guidance, reports, providing advice, and sharing best practices and by facilitating the exchange of best practices between competent authorities - facilitating exchange of best practices	Data processing Data flow
Article 5(1)(b) Support for implementation of EU law	(b) supporting **information sharing within and between sectors, in particular regarding the sectors listed in Annexes I and II to Directive (EU) 2022/2555**, and products with digital elements falling within the scope of Regulation (EU) 2024/2847, **by providing best practices and guidance on available tools and procedures**	- ENISA - sectors listed in Annexes I and II to Directive (EU) 2022/2555 - stakeholders impacted by Regulation (EU) 2024/2847	providing best practices and guidance on available tools and procedures on information sharing	Data processing Data flow

Article 5(1)(c) Support for implementation of EU law	(c) at the request of the Commission, assisting Member States by providing support, such as **technical guidance, including on cybersecurity risk management measures, tools for cybersecurity maturity assessment, and incident response playbooks**, tailored to the sectors listed in Annexes I and II to Directive (EU) 2022/2555, with a view to facilitating the improvement of their cybersecurity maturity level and compliance with Union law regarding cybersecurity;	- EU Commission - ENISA - sectors listed in Annexes I and II to Directive (EU) 2022/2555	Providing technical guidance	Data processing Data flow
Article 5(1)(e)	(e) assisting Member States and relevant Union entities in **developing and promoting cybersecurity policies** related to sustaining the general availability and integrity of the public core of the open internet;	ENISA Member States EU entities	Assisting in developing and promoting cybersecurity policies	Data processing Data flow
Article 5(1)(f) Support for implementation of EU law	(f) in accordance with Regulation (EU) 2024/2847, **providing technical advice and support** on matters related to the implementation and enforcement of that Regulation	-ENISA - stakeholders impacted by Regulation (EU) 2024/2847	Providing technical advice and support requires processing and sharing information about regulatory requirements, implementation challenges, and compliance guidance.	Data processing Data flow
Article 5(1)(h)	(h) at the request of the European Data Protection Board, providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy.	ENISA EDPB	Providing advice at a request	Data processing Data flow

Article 5(2) Contribution to Union level cybersecurity risk assessments	ENISA shall contribute to coordinated Union level cybersecurity risk assessments, including those carried out pursuant to Article 22 of Directive (EU) 2022/2555.	ENISA Member States General Public	Contributing to coordinated risk assessments, which requires data processing and data flow	Data processing Data flow
Article 5(3) ENISA shall issue guidelines	ENISA shall **issue guidelines** regarding the interoperability of network and information systems used for information-sharing, including with regard to Cross-Border Cyber Hubs as referred to in Article 6(3) of Regulation (EU) 2025/38.	ENISA Member States	ENISA shall issue guidelines	Data processing Data flow
Article 5(5) Support to the Commission	At the **Commission's request**, ENISA shall **provide expertise, technical advice, information or analysis or carry out preparatory work** on specific cybersecurity matters with a view to informing the Commission's policymaking and monitoring of the implementation of Union legislation.	EU Commission ENISA	Preparing and sending information to the Commission	Data processing Data flow

Article 6 Capacity-building	ENISA shall assist by providing knowledge and expertise, best practices, etc.	ENISA Member States EU entities Public and private stakeholders Market surveillance authorities ECCG members ECCC	Providing knowledge and expertise	Data processing Data flow
Article 7 Awareness-raising and talent pool	ENISA shall assist Member States in their efforts to raise awareness of Union policies and legislation regarding cybersecurity and promote their visibility **by developing actionable tools and guidance**. ENISA shall support initiatives aimed at increasing the European cybersecurity talent pool, in particular by coordinating competitions.	ENISA Member States	Developing actionable tools and guidance	Data processing
Article 8(1) Market knowledge and analyses	ENISA shall **carry out and disseminate analyses** of the main market trends in the cybersecurity market on both the demand and supply sides, in particular related to the areas where European cybersecurity certification schemes exist or are planned, sectors listed in Annexes I and II to Directive (EU) 2022/2555 and product categories covered by Regulation (EU) 2024/2847, including Annexes III and IV to that Regulation.	ENISA Sectors listed in Annexes I and II to Directive (EU) 2022/2555 Product categories covered by Regulation (EU) 2024/2847	Perform and disseminate analyse	Data processing Data flow

Article 8(2) Market knowledge and analyses	ENISA shall **carry out and disseminate analyses** of technological cybersecurity trends, in particular in relation to activities and entities falling within the scope of Directive (EU) 2022/2555 and products with digital elements falling within the scope of Regulation (EU) 2024/2847.	ENISA General public, stakeholders within the sense of Directive (EU) 2022/2555 and Regulation (EU) 2024/2847	Perform and disseminate analysis	Data processing Data flow
Article 8(3) Market knowledge and support for ecosystems	ENISA shall build knowledge and **disseminate technical advice and analyses** on state-of-the-art cybersecurity tools, frameworks standards and best practices.	ENISA General public	Disseminate technical advice and analyses in state-of-the-art cybersecurity tools, frameworks standards and best practices.	Data processing Data flow
Article 9 International cooperation	ENISA shall contribute by analysing and reporting to the Management Board on the outcome of international exercises, facilitating the exchange of best practices, providing the Commission with expertise, advice.	International audience ENISA Management Board of ENISA EU Commission	Analysing and reporting; providing advice etc.	Data processing Data flow
Article 10(2) and (3) Operational cooperation	2. ENISA shall be a member of the network of national CSIRTs established pursuant to Article 15(1) of Directive (EU) 2022/2555 and shall **provide the secretariat** of the CSIRTs network pursuant to Article 15(2) of	ENISA CSIRTs (Article 15(1) of Directive (EU) 2022/2555) EU-CyCLONe (Article 16(2) of Directive (EU) 2022/2555)	Facilitating exchange of information, taking the duties of secretariat of networks	Data flow Digital solution Digital public service

	Directive (EU) 2022/2555. 3. ENISA shall **provide the secretariat** of the European cyber crisis liaison organisation network (EU-CyCLONe) pursuant to Article 16(2), second subparagraph, of Directive (EU) 2022/2555.			
Article 11(1)(b) Situational awareness Article 12 Early alerts	**issuing early alerts** in accordance with Article 12	EU Commission ENISA Europol EU-CyCLONe CSIRTs network CERT-EU Entities listed in Annexes I and II to Directive (EU) 2022/2555	Issuing early alerts	Data processing Data flow Digital public service
Article 10(4)(b) Operational cooperation	(b) at the request of one or more Member States, **providing advice and assessments in relation to a specific potential or ongoing incident or cyber threat**, including through the provision of expertise and **facilitating the technical handling of such incidents**, and through **supporting the voluntary sharing of relevant information and technical solutions between Member States;**	ENISA Member States	Providing advice and assessments in relation to a specific potential or ongoing incident or cyber threat; Facilitating the technical handling of such incidents; Supporting the voluntary sharing of relevant information and technical solutions between Member States	Data processing Data flow Digital public services

Article 10(4)(c) Operational cooperation	(c) analysing vulnerabilities, threats and incidents;	ENISA Member States	Data collection from public sources and data exchange with the Member States	Data processing Data flow
Article 10(4)(d) Operational cooperation	(d) at the **request of one or more Member States**, **providing support i**n relation to *ex-post* technical inquiries regarding significant incidents within the meaning of Directive (EU) 2022/2555;	ENISA Member States	Analysis and support in response to technical inquiries regarding incidents	Data processing Data flow
Article 10(4)(e) Operational cooperation	(e) contributing to supporting the coordinated management of large-scale cybersecurity incidents and crises at operational level, in particular by **assisting EU-CyCLONe in preparing reports to political level by facilitating and by facilitating timely information-sharing between the CSIRTs network, and EU-CyCLONe;**	ENISA EU-CyCLONe CSIRTs network	Analysing data to support the preparation of reports; facilitating timely information sharing between networks	Data processing Data flow Digital public service
Article 10(5) Operational cooperation	At the **request of a Member State** or a Union entity in cooperation with CERT-EU ENISA shall support consistent public communication relating to an incident or cyber threat.	ENISA Member States	Receiving request and communicate, if needed	Data flow

Article 10(6) Operational cooperation	ENISA shall **support** cooperation among Member States and, through CERT-EU, among Union entities, with regard to the **deployment of secure communications tools.** ENISA shall use within the CSIRTs network and EU-CyCLONe secure communications tools which are provided by legal entities that are not established in or controlled by third countries or by nationals of third countries.	ENISA EU Commission Member States EU entities CSIRTs network EU-CyCLONe	Support the deployment of secure communication tools and use such tools within the CSIRTs network and EU-CyCLONe.	Digital solution Digital public service
Article 11(1)(a) Shared cybersecurity situational awareness	a) **develop** in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, CERT-EU, Europol and other relevant Union entities **repositories** of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures;	EU Commission ENISA EU-CyCLONe CSIRTs network Europol EU entities CERT-EU	Develop repositories	Digital flow Digital solution Digital public service
Article 11(1)(c) to (g) Shared cybersecurity situational awareness	Provide timely *ad-hoc* analyses (some at request); provide analysis and technical advice; prepare technical situation report in cooperation with other entities; monitoring trends and sharing them	ENISA Member States EU Commission EU entities EU-CyCLONe CSIRTs network	Data analysis, sharing information and providing reports (some upon request)	Data processing Data flow

Article 11(2)(a) Shared cybersecurity situational awareness	ENISA shall **perform analyses** of cyber threats, incidents, trends, emerging technologies and their impacts, including a regular **analysis** addressing sectors listed in Annexes I and II to Directive (EU) 2022/2555 and relevant product categories covered by Regulation (EU) 2024/2847;	ENISA General public	Analyse data to provide information impactful for the cybersecurity; regular report	Data processing Data flow
Article 11(2)(b) Shared cybersecurity situational awareness	ENISA shall **issue, in cooperation with the Commission, and, where appropriate the CSIRTs network, 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 Annexes I and II to Directive (EU) 2022/2555;	EU Commission CERT-EU CSIRTs network General public	Issuing advice, guidance and best practice	Data processing Data flow
Article 11(2)(c) Shared cybersecurity situational awareness	ENISA shall carry out **long-term strategic analyses of cyber threats** and incidents in order to **identify** emerging trends and help prevent incidents.	ENISA General public	Analysis of data and identification of emerging threats	Data processing
Article 11(3) Shared cybersecurity situational awareness	ENISA may **make the analyses**, advice, guidance, best practices and reports referred to in paragraph 2 **public**, in agreement with the contributing entities referred to in paragraph 2.	ENISA General public	Making information public	Data flow Digital public service

Article 13(2) Support in Incident Response	2. At the request from the Commission or EU-CyCLONe, ENISA, with the support of the CSIRTs network and with the approval of the Member State concerned, shall **review and assess significant cybersecurity incidents** or large-scale cybersecurity incidents in accordance with Article 21 of Regulation (EU) 2025/38.	EU Commission ENISA EU-CyCLONe CSIRT Network Member States	Review and assess significant cybersecurity incidents	Data processing
Article 14(2) Cybersecurity exercises at Union level	2. ENISA shall **maintain a repository** of lessons learned from the exercises referred to in paragraph 1 and recommend to Member States and, where relevant, to Union entities how the lessons learned may be implemented effectively and efficiently.	ENISA Member States EU entities	Maintain a repository	Data processing Digital solution Digital public service
Article 14 Cybersecurity exercises at Union level	Receiving requests from EU-CyCLONe, the Commission, Member States, or CERT-EU, ENISA shall organise or contribute to the organisation of cybersecurity exercises. ENISA shall support the Commission in compiling an annual rolling programme of Union-level cybersecurity exercises.	ENISA Commission Member States EU entities CERT-EU	Receiving requests to organise or support the organisation of exercises	Data flow Data processing

Article 15 Provision on tools and platforms	1. **ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, including platforms** related to cybersecurity at Union level, in particular the single reporting platform for incident reporting established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation. 2. Where appropriate for the purposes of paragraph 1, **ENISA shall cooperate and exchange information** with the CSIRTs network and, where applicable, market surveillance authorities.	ENISA CSIRTs Network General public Market surveillance authorities	ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, such as platforms	Digital solution Digital public service Data flow
Article 16(2) Vulnerability management services	(a) maintaining the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555; (b) providing vulnerability management services to **stakeholders**, building on the European vulnerability database and making use of relevant information available to ENISA; (c) where appropriate, entering into structured cooperation with **organisations** providing programmes, registries or databases similar to the European vulnerability database; (d) actively supporting the **CSIRTs** designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 with regard to the management of the coordinated disclosure of vulnerabilities which may have a significant	ENISA National CSIRTs CSIRTs network National competent authorities Industry Research community General public International actors providing programmes, registries or databases	Providing vulnerability management services; entering into structured cooperation where appropriate; cooperation with stakeholders	Digital solution Digital public service Data flow

	impact on entities in more than one Member State; (e) developing and maintaining methodologies and governance mechanisms for vulnerability identification and coordinated disclosure, **in cooperation with national competent authorities, CSIRTs, industry and the research community**			
Article 17 Cybersecurity certification Article 18 Standardisation, technical specifications and guidance	Article 17(1) (a) **preparing candidate European cybersecurity certification schemes (‘candidate schemes’)** for ICT products, ICT services, ICT processes, managed security services and the cyber posture of entities, and related technical specifications in accordance with Article 74; (b) **maintaining adopted European cybersecurity certification schemes** in accordance with Article 75, including in view of a possible review of the adopted European cybersecurity certification schemes in accordance with Article 76; (c) promoting the uptake of adopted schemes and maintaining a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity in accordance with Article 79; Article 17(2) (e) **preparing** model provisions to be referenced in the European cybersecurity certification schemes (‘candidate schemes’) for	ENISA General public	Analysing data and exchanging data flows with the Commission and other stakeholders; preparing candidate certification scheme; maintaining ENISA website	Data processing Data flows Digital public service

	ICT products, ICT services, ICT processes, managed security services and cyber posture of entities in accordance with Article 81(5). Article 18 1. ENISA shall draft technical specifications and guidance to support the implementation of Union legislation in the field of cybersecurity. 2. ENISA shall **monitor, participate and lead in standardisation developments** activities at Union level and, in accordance with Article 9, at international level. 3. ENISA shall support the development and evaluation of cryptographic algorithms. Where an evaluated cryptographic algorithm is evaluated positively, ENISA shall cooperate, in accordance with Regulation (EU) No 1025/2012, with the European standardisation bodies to support its standardisation. 4. ENISA shall **provide technical expertise** to the Commission and the ECCG on appropriate standards or technical specifications in support of Union policies related to cybersecurity, in particular Regulation (EU) 2024/2847, including for Union harmonisation legislation in the field of cybersecurity and European cybersecurity certification schemes pursuant to point (d) of Article 81(1), point (d). 5. ENISA shall assist the Commission in the assessment of draft harmonised standards to support the implementation of Union harmonisation legislation in the field of cybersecurity.			

Article 19 – European Cybersecurity Skills Framework	ENISA **shall develop and make publicly available a European Cybersecurity Skills framework ('ECSF')**. Before making the ECSF publicly available or updating it pursuant to paragraph 4, ENISA shall **consult the Commission.** The use of the ECSF shall be **voluntary for public and private entities**. ENISA may **consult stakeholders** in the development and uptake of the ECSF.	ENISA Commission General public Member States EU entities Public and private stakeholders	Maintenance of the ECSF; consultation with stakeholders; uptake of the ECSF	Data processing Data flow Digital solution
Articles 20-23 – European individual cybersecurity skills attestation schemes	ENISA shall **develop, adopt and maintain European individual cybersecurity skills attestation schemes**. The use of European individual cybersecurity skills attestation schemes shall be **voluntary for national public bodies and private entities**, unless otherwise specified by national law. Prior to initiating a new European individual cybersecurity skills attestation scheme, ENISA shall **consult the Commission**. ENISA shall only adopt such a scheme following a positive **opinion from the Commission**. When preparing a European individual cybersecurity skills attestation scheme, ENISA may **consult relevant stakeholders.** ENISA shall ensure **close cooperation with Member States** throughout preparation of the European individual cybersecurity skills attestation schemes. Authorised attestation providers shall **assess whether individuals meet the requirements** of a European individual cybersecurity skills attestation scheme and, where those requirements are met, issue European individual	ENISA Commission General public Member States EU entities Public and private stakeholders (contributing to the development of an attestation scheme; applicants and European individual cybersecurity skills attestations providers, including assessors)	Developing and maintaining schemes; consultations with stakeholders; processing of applications; issue decisions; maintaining a website	Data processing Data flow Digital solution Digital public service

	cybersecurity skills attestations. ENISA shall **provide guidance to and conduct obligatory training of assessors** regarding the requirements and assessment methods included in the European individual cybersecurity skills attestation scheme as referred to in Article 20(3), point (b). Entities wishing to become authorised attestation providers or to renew their authorisation **('applicants') shall submit an application** to ENISA. Authorised attestation providers shall ensure that, **at the request of the individual,** electronic attestations of European individual cybersecurity skills attestations are issued as electronic attestations of attributes in a format that can be stored in the European Digital Identity Wallets set out in Regulation (EU) No 910/2014. Applicants and authorised attestation providers shall allow **ENISA to conduct evaluations** as part of the initial application process, maintenance of the authorisation or renewal thereof and share all relevant information to ensure the requirements laid down in paragraphs 3, 4 and the obligations laid down in paragraph 5 are met or continue to be met in accordance with Article 22(2). Authorised attestation providers shall immediately **inform ENISA** if any of the requirements listed in paragraph 3 is no longer met or if any doubt that those requirements are not met, arises, including regarding the independence of assessors.			

	Applicants shall **pay a fee to ENISA** for the assessment of their application. Authorised attestation providers shall **pay a fee to ENISA** for the maintenance of their authorisation. **ENISA shall evaluate** whether the requirements laid down in Article 21(3) and (4) and the obligations laid down in Article 21(5) are met or continue to be met by applicants and authorised attestation providers. After examining an application against the requirements laid down in Article 21(3) and (4), **ENISA may issue a decision**. **ENISA may amend, suspend or revoke such decisions**. **ENISA shall maintain and regularly update a dedicated website** providing public information on: (a) the ECSF, including the framework and its timeline for update; (b) the European individual cybersecurity skills attestation schemes, their progress and timelines for their development; (c) the fees associated with each European individual cybersecurity skills attestation scheme adopted pursuant to Article 47 of this			

	Regulation; (d) the indicative cost of a European individual cybersecurity skills attestation in accordance with Article 20(4); (e) the list of authorised attestation providers.			
Article 25 Composition of the Management Board	**Appointing members** to the Management Board of ENISA.	ENISA EU Commission Member States	Appointing members	Data flow Data processing
Article 28(1) Functions of the Management Board Article 30 Executive Board	b. adopt ENISA's draft single programming document referred to in Article 44, before its **submission to the Commission for an opinion**; (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 European Court of Auditors; make the annual report public; (i) ensure adequate **follow-up to findings** and recommendations stemming from internal or external audit reports and evaluations and from investigations of the European Anti-Fraud	ENISA EU Commission European Parliament Council of the EU Court of Auditors Member States General public	Submission of the SPD to the Commission for an opinion; 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; Follow-up the findings	Data flow Data processing

	Office (OLAF) and of the European Public Prosecutor's Office (EPPO);			
Article 31(8) Appointment, dismissal and extension of the term of office	The **Management Board shall inform the European Parliament** about its intention to extend the Executive Director's term of office in accordance with paragraph 6. 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.	ENISA Management Board of ENISA European Parliament	The Management Board shall inform the European Parliament	Data flow
Article 32(3) Tasks and responsibilities of the Executive Director Article 32(5)	3. The **Executive Director shall report to the European Parliament** on the performance of their tasks when invited to do so. The Council may invite the Executive Director to report on the performance of their tasks. Preparing draft budget plans strategies, strategic documents.	Executive Director of ENISA European Parliament	Reporting on the performance	Data flow Data processing
Article 35(5), (6) ENISA Advisory Group	5.The ENISA Advisory Group **shall advise ENISA** in respect of the performance of ENISA's tasks, except for the application of the provisions of Titles III, IV, and V 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.	ENISA Members of the ENISA Advisory Group Management Board of ENISA Executive Director of ENISA	Advise and inform on its activities	Data processing Data flow

	6. The ENISA Advisory Group **shall inform the Management Board** of its activities on a regular basis.			
Article 36-43 Board of Appeal	ENISA shall **establish a Board of Appeal** by a decision of the Management Board. The Board of Appeal shall be composed of a Chairperson and three other members. Each member of the Board of Appeal shall have an alternate. The alternate shall represent the member in their absence. The Management Board shall **appoint the Chairperson, the other members and their alternates** from a **list of qualified candidates established by the Commission**. The list of qualified candidates shall be valid for four years. The validity of this list may be extended by the Management Board for additional four-year periods acting on a proposal from the Commission. Where the Board of Appeal considers that the nature of the appeal so requires, it may request the **Management Board to appoint two additional members and their alternates** from the list referred to in paragraph 3. The Board of Appeal shall adopt and **make public its rules of procedure.** If, for one of the reasons listed in paragraph 1 or	ENISA Management Board of ENISA Commission Board of Appeal in the sense of Article 36 of CSA2 proposal Applicants (legal entities that wish to become authorised attestation providers, to maintain or to renew their authorisation)	Issuing decisions based on appeals Processing the appeals Preparing and publishing rules of procedures Information flows	Data processing Data flow Digital public service

	for any other reason, a member of a Board of Appeal considers that they should not take part in any appeal proceeding, they **shall inform the Board of Appeal accordingly**. The Board of Appeal shall **decide as to the action to be taken** in the cases listed in paragraphs 2 and 3 without the participation of the member concerned. For the purposes of taking that decision, the member concerned shall be replaced on the Board of Appeal by their alternate. An appeal brought pursuant to paragraph 1 shall be subject to interlocutory revision in accordance with Article 41 before being put to the Board of Appeal for examination. Applicants within the meaning of Article 21(3) may **appeal against: a decision of ENISA** addressed to them, pursuant to Article 22(3), ENISA's failure to act in respect of an application submitted by them to ENISA within the applicable time limits laid down in Article 22(4). In the case referred to in paragraph 1, point (a), the appeal, together with the statement of grounds thereof, shall be **filed in writing** in accordance with the rules of procedure referred to in Article 36(5) within two months of notification of the decision to the applicant concerned, or, in the absence thereof, of the day on which the decision came to the knowledge of the applicant. In the case referred to in paragraph 1, point (b) , the appeal shall be **filed with ENISA in writing** in accordance with the rules of procedure			

	referred to in Article 36(5) within two months of the day of expiry of the time limit set out in Article 22(4). If ENISA considers the appeal to be admissible and well founded, it **shall rectify the decision or failure to act** referred to in Article 40(1). If ENISA does not rectify the decision within one month after receipt of the appeal, it shall immediately **decide whether to suspend the application of its decision and shall refer the appeal to the Board of Appeal**. The **Board of Appeal shall decide** within 3 months of the appeal being filed whether to grant or refuse that appeal. When examining an appeal, the Board of Appeal shall act within the deadlines laid down in its rules of procedure. It shall, as often as necessary, **invite the parties to the appeal proceedings to file, within specified time limits, observations on its notifications or on communications from other parties to the appeal proceedings**. Parties to the appeal proceedings shall be entitled to make **oral representations.** Where the Board of Appeal finds that the grounds for appeal are founded, it **shall remit the case to ENISA.** ENISA shall **take its final decision** in compliance with the findings of the Board of Appeal and shall **provide a statement of reasons for that decision**. ENISA shall **inform the parties** to the appeal proceedings accordingly. Actions for the annulment of decisions of ENISA taken pursuant to Article 22(3), or for failure to act within the applicable time			

	limits pursuant to Article 22(4), may **be brought before the Court of Justice of the European Union** after the appeal procedure within ENISA laid down in Articles 39 to 42 has been exhausted or in the event of failure to act within the applicable time limit pursuant to Article 41(2). ENISA shall **take all necessary measures to comply** with the judgment of the Court of Justice of the European Union			
Article 44 Single Programming Document	2. Each year, the Executive Director shall draw up a draft single programming document, as referred to in paragraph 1, with the corresponding financial and human resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) 2019/715 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, taking into account the opinion of the Commission referred to in Article 32(7) of Delegated Regulation (EU) 2019/715. If the Management Board decides not to take into account any elements of the opinion of the Commission, it shall provide thorough justification for that decision. The Management Board shall forward the single programming document 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.	Executive Director of ENISA Management Board of ENISA EU Commission European Parliament Council	Drafting, adopting, and forwarding a single programming document every year	Data flow

Article 45 Establishment of ENISA's budget	4. The **Commission shall send the draft estimate to the budgetary authority** together with the draft general budget of the Union. The draft estimate shall also be made available to ENISA.	ENISA EU Commission	Sharing information	Data flow
Article 47 Fees	In relation to European individual attestation schemes activities laid down in Article 22(1), the **following fees shall be levied** towards applicants within the meaning of Article 21(3) or to authorised attestation providers to contribute to covering the full costs of the activities performed by ENISA: a. issuing authorisations following examination of the requirements laid down in Article 21(3) and (4), including conducting evaluations; b. yearly maintenance of the authorisation; c. renewing authorisations for providers of European individual cybersecurity skills attestations, including conducting evaluations. In relation to certification, the **following fees shall be levied on the conformity assessment bodies** for the maintenance of European cybersecurity certification schemes under which European cybersecurity certificates are issued, in particular: an annual fee for the participation in a European cybersecurity certification scheme; a fee for issuance of European cybersecurity certificates under European cybersecurity	Commission ENISA Attestation providers Conformity assessment bodies	Processing information; payment of fees; reporting on fees	Data processing Data flow

	certification schemes. The fees referred to in point b) shall be levied when the conformity assessment body submits European cybersecurity certificates to ENISA for publication on their website pursuant to Article 79. The **Commission shall adopt implementing acts** laying down detailed rules relating to fees levied by ENISA ENISA shall include a **report on the fees levied and their impact on the Agency's budge**t as part of the procedure for the presentation of accounts.			
Article 48 Article 49 Budget implications	Article 48 3. Each year, the Executive Director shall **send to the budgetary authority all information** relevant to the findings of evaluation procedures. Article 49 1. 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). 2. ENISA's accounting officer shall also **provide the required accounting information for consolidation purposes to the Commission's accounting offic**er, in the manner and format required by the latter by 1 March of year N + 1. 3. **ENISA shall send the report on the budgetary and financial management for year N to the European Parliament, the Council, the Commission** and the Court of	ENISA Management Board of ENISA EU Commission Council European Parliament	Processing and sharing information regarding ENISA budget.	Data processing Data flow

	Auditors by 31 March of year N + 1. 4. **On receipt of the Court of Auditor's observations on ENISA's provisional accounts for year N, the** agency accounting officer shall draw up ENISA's final accounts. 5. The **Management Board shall deliver an opinion** on ENISA's final accounts for year N. **Agency's accounting officer shall draw up ENISA's final accounts under his or her own responsibility. The Executive Director shall submit them to the Management Board for an opinion.**			
Article 52 Declaration of interests	The parties s**hall 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.	ENISA management (Executive Director, the Deputy Executive Director); Management Board, Seconded national experts	Processing and sharing data on declaration of interests	Data processing Data flow
Article 58 Liaison officers	1. **Each Member State shall designate at least two Liaison Officers** [from their national cybersecurity authority] as a seconded national expert to ENISA and to work at its seat or its local office, in accordance with Article 59(2). The Commission may also designate a Liaison Officer. 2. Liaison Officers designated by their Member State shall be entitled to **request and receive all relevant information from their Member**	ENISA Member States	Designation of liaison officers and sharing information	Data processing Data flow

	States, as provided for by this Regulation, while fully respecting the national law or practice of their Member States, in particular as regards data protection and the rules on confidentiality.			
Article 67 Handling 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.**	ENISA Management Board Commission	Handle classified information	Data processing Data flow
Article 68, 69, 70 Cooperation with Union entities and national authorities Cooperation with stakeholders Cooperation with third countries	ENISA shall cooperate and exchange information on matters related to cybersecurity with relevant Union entities, market surveillance and supervisory authorities; relevant stakeholders; competent authorities from third countries or international organisations	ENISA Europol ECCC European Data Protection Board General public Council	Sharing information	Data flow
Article 72 on Public information and consultation on the European cybersecurity certification schemes	2. The Commission shall maintain and regularly update a dedicated website providing information on the following aspects: (a) European cybersecurity certification schemes under requested for development; (b) strategic priorities for harmonisation of ICT products, ICT services, ICT processes, managed security services or security	EU Commission General public ENISA	Maintaining Information Website This mandates the Commission to provide information on a publicly available website and provide related data management activities on ongoing basis.	Digital Public Service Digital solution

	requirements of Union legislation, including potential areas for which a European cybersecurity certification scheme might be requested. 3. The Commission shall make publicly available on the website referred to in paragraph 2 of this Article the information on its request to ENISA to prepare a candidate scheme as referred to in Article 73 and its decision to accept, reject or discontinue a candidate scheme transmitted by ENISA in accordance with Article 74(7).			
Article 72 on Public information and consultation on the European cybersecurity certification schemes	During the preparation of a candidate scheme by ENISA pursuant to Article 74, the **European Parliament, the Council may request the Commission**, in its capacity as chair of the ECCG, and ENISA to present relevant information on the draft candidate scheme. U**pon the request of the European Parliament or the Council, ENISA, in agreement with the Commission** and without prejudice to Article 54, may make **available to the European Parliament and to the Council relevant parts of a draft candidate scheme** in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner. **The European Parliament, the Council may invite the Commission and ENISA to discuss** matters concerning the implementation of European cybersecurity certification schemes for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities.	ENISA Council of the EU European Parliament	Requesting and sending information on a draft candidate scheme prepared by ENISA	Data flows

Article 73 Request for a European cybersecurity certification scheme Article 74 Preparation and adoption of European cybersecurity certification schemes **(covered in Article 17)**	**Article 73** **1. The Commission may request ENISA to prepare a candidate European cybersecurity certification scheme** for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities. In duly justified cases, the ECCG may suggest to the Commission to put forward a request referred to in paragraph 1. 4. When preparing the request referred to in paragraph 1, **the Commission** shall duly consult ENISA and the ECCG as well as take into account the views of all **relevant stakeholders** and other Union entities, including, where applicable, those that are relevant under Union legislation in which a European cybersecurity certification scheme is providing presumption of conformity. Article 74 3. When preparing the candidate scheme, 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, where applicable, a supporting technical specification. **ENISA shall request members of the ECCG to provide a written opinion on the candidate scheme.** 4. **ENISA shall consult stakeholders**, in a timely manner by means of a formal, open, transparent and inclusive consultation process. **ENISA shall also cooperate with relevant public authorities in the Member States and**	EU Commission ENISA ECCG Expert stakeholders	Preparation of a request and certification scheme and related consultation of stakeholders	Data processing Data flows Digital Public Service (covered in Article 17)

	with relevant Union entities to gather their expert advice in relation to the preparation of the candidate scheme and, where applicable, a supporting technical specification. 6. **ENISA shall transmit the candidate scheme** to the Commission no later than 60 days from the date of the request referred to in paragraph 5. 7. When receiving the candidate **scheme**, the **Commission shall evaluate** whether the scheme corresponds to the request made in accordance with Article 73. 8. Where the Commission returns a candidate scheme to ENISA for revision in accordance with paragraph 7, point (b)revision, paragraphs 4, 5 and 7 of this Article shall then apply accordingly.			
Article 75 Maintenance of a European cybersecurity certification scheme	2. ENISA, in cooperation with the Commission and supported by the ECCG and its relevant maintenance sub-group, shall ensure the maintenance of European cybersecurity certification schemes, including in view of the possible review of such schemes by the Commission. ENISA shall cooperate and exchange information with relevant Union entities and groups in relation to maintenance activities. 5. The ECCG may issue an opinion on the maintenance of European cybersecurity certification schemes.	EU Commission ENISA ECCG Conformity assessment bodies	ENISA shall ensure maintenance. This includes periodical hybrid or online meetings, gathering information, analysing and sharing (in relation to a European cybersecurity certification scheme)	Data processing Data flow

Article 76 Evaluation, review and withdrawal of a European cybersecurity certification scheme	1. At least every four years following the entry into application of a European cybersecurity certification scheme, ENISA shall evaluate the impact and effectiveness that scheme, in cooperation with the relevant maintenance sub-group of the ECCG, and by taking into account the feedback received from stakeholders. ENISA shall conduct the evaluation by carrying out the necessary market analysis in accordance with Article 8(1). 3. When reviewing or withdrawing European cybersecurity certification schemes, the Commission shall consult ENISA, the ECCG and its relevant maintenance sub-group, as well as take into account the views of relevant stakeholders and other Union entities. 4. The ECCG may issue an opinion on the review or withdrawal of a European cybersecurity certification scheme. The Commission shall take due account of it when reviewing or withdrawing the European cybersecurity certification scheme.	EU Commission ENISA ECCG	The Commission shall review schemes whist consulting relevant stakeholders.	Data processing Data flow
Article 77 Technical specifications in European cybersecurity certification schemes	3. Where technical specifications are referenced in a European cybersecurity certification scheme as referred to in Article 74(10), they shall be made available on the website referred to in Article 79. 4. In duly justified cases, in particular where the technical specifications contain information could compromise the security of certified ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, they shall be distributed only to those	ENISA Member States Conformity assessment bodies	Making information available at ENISA certification website	Data flow Digital Public Service

	stakeholders concerned by the requirements of the scheme. Such scheme shall not be referenced in a European cybersecurity certification scheme as referred to in Article 74(10).			
Article 79 Website on European cybersecurity certification schemes	1. ENISA shall organise activities to promote the uptake of adopted European cybersecurity certification schemes, including by maintaining the website referred to in paragraph 2 of this Article. 2. ENISA shall maintain and regularly update a dedicated website providing public information on the following: (a) European cybersecurity certification schemes; (b) the fees associated with the maintenance of each European cybersecurity certification scheme; (c) relevant ENISA technical specifications; (d) European cybersecurity certificates and EU statements of conformity, including information with regard to such certificates and statements which are no longer valid, or which are suspended, withdrawn or expired; (e) relevant supplementary cybersecurity information provided in accordance with Article 84(2); (f) summaries of peer reviews pursuant to Article 89(7); (g) technical specifications referenced in a European cybersecurity certification scheme pursuant to Article 74(10).	ENISA Member States Conformity assessment bodies	Maintaining Information Website mandates ENISA to collect, process, and maintain comprehensive databases of certification information, requiring ongoing data management activities.	Digital Public Service Digital solution Data processing Data flow

	3. Where applicable, the **website referred to in paragraph 2 shall also indicate** the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.			
Article 81 Elements of European cybersecurity certification scheme	5. The Commission is empowered to adopt implementing acts laying down common principles and model provisions for elements set out in paragraphs 1, 2 and 3 across European cybersecurity certification schemes. Where appropriate and available, a European cybersecurity certification scheme may include references to those principles and model provisions. The implementing acts referred to in paragraph 5 shall be adopted in accordance with the examination procedure referred to in Article 118(2). **When developing or revising the common principles and model provisions for the elements of European cybersecurity certification schemes, the Commission shall consult ENISA and take into account, as appropriate, views expressed by the ECCG, relevant stakeholders and other relevant bodies.**	ENISA General public Member States authorities	Consultation of relevant stakeholders requiring data flows and processing	Data flow Data processing
Article 83 Conformity self-assessment	3. The manufacturer or provider of ICT products, ICT services, ICT processes, managed security services or the entity the cyber posture of which is subject to certification shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the	ENISA General public Member States authorities	Information being available; data sharing Shared data requires processing by ENISA and Member States authorities	Data flow Data processing

	ICT products, ICT services, ICT processes, managed security services or cyber posture with the European cybersecurity certification scheme available to the national cybersecurity certification authority designated pursuant to Article 89 for the period provided for in that scheme. **A copy of the EU statement of conformity shall be submitted without undue delay to the national cybersecurity certification authority and to ENISA.**			
Article 84 Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes	1. The manufacturer or provider of ICT products, ICT services or ICT processes for which an EU statement of conformity or European cybersecurity certificate has been issued **shall make publicly available the following supplementary cybersecurity information**.	Manufacturer or provider of ICT products, ICT services or ICT processes General public Conformity assessment bodies	Making information publicly available at electronic form.	Data flow
Article 85 Issuance of European Cybersecurity certificates	2. The conformity assessment bodies referred to in Article 91 shall issue European cybersecurity certificates on the basis of criteria included in the European cybersecurity certification scheme adopted pursuant to Article 74. 6. The natural or legal person who submits ICT products, ICT services, ICT processes or managed security services for certification or the entity which applies for certification of its cyber posture **shall make available all information necessary to conduct the certification to the national cybersecurity certification authority** designated pursuant to Article 89, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in	ENISA General public Member States authorities Conformity assessment bodies	Sharing information relevant to certification processes	Data flow Data processing

	Article 91. 7. Conformity assessment bodies and, where applicable, national cybersecurity certification **authorities shall inform ENISA** without undue delay about their decisions that affect the status of European cybersecurity certificates and EU statements of conformity in accordance with Article 94. 8. **The holder of a European cybersecurity certificate shall inform the conformity assessment body** and, where applicable, national cybersecurity certification authority, referred to in paragraph 7, of any subsequently detected vulnerabilities or nonconformities concerning the certified ICT product, ICT service, ICT process, managed security service or cyber posture of entity that have a likely impact on its conformity with the certificate. **That body shall forward that information without undue delay** to the national cybersecurity certification authority concerned and assess the impact on the certificate in line with the scheme's conditions as referred to in Article 81, point (f).			
Article 86 National cybersecurity certification schemes	4. **Member States shall inform the Commission and the ECCG before adopting new national cybersecurity certification schemes** for ICT products, ICT services, ICT processes, managed security services and cyber posture of entities.	ENISA Member States EU Commission	Information sharing	Data flow
Article 88 National cybersecurity certification authorities	2. Each Member State shall **inform the Commission of the identity of the designated national cybersecurity certification**	ENISA Member States authorities EU Commission	Member State shall inform the Commission of the designated NCCAs	Data flow Data processing

	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. 6. National cybersecurity certification authorities shall: (c) **monitor, in cooperation with relevant market surveillance authorities, compliance with and enforce the obligations of the manufacturers or providers** of ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified set out in this Regulation that are established in their respective territories and that carry out conformity self-assessment and in the corresponding European cybersecurity certification scheme; (d) without prejudice to Article 91(3), **actively assist and support the national accreditation bodies or other relevant authorities in the monitoring and supervision** of the activities of conformity assessment bodies, for the purposes of this Regulation; (e) cooperate with the European Commission where the competence of a conformity assessment body is challenged pursuant to Article 94; (f) **monitor and supervise the activities** of the public bodies referred to in Article 85(3); (g) where applicable, authorise conformity assessment bodies in accordance with Article 93, monitor compliance with and enforce the obligations of conformity assessment bodies	General public Conformity assessment bodies	Member states authorities shall conduct various tasks of monitoring, supervision and cooperation that require data flows and date processing	

	with the specific or additional requirements set out in European cybersecurity certification schemes pursuant to Article 81(3), point (f), and restrict, suspend or withdraw existing authorisation where conformity assessment bodies do not meet the requirements of this Regulation; (h) **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 85(4)] or in relation to EU statements of conformity issued under Article 83, investigate the subject matter of such complaints to the extent appropriate, and inform the complainant of the progress and the outcome of the investigation within a reasonable period; (i) provide an annual report on its main activities to the Commission, ENISA and the ECCG by 31 March [year of entry into force + 12 months] each year, and make these reports available to the peer review team where the national cybersecurity certification authority is subject to peer review in accordance with Article 89; (j) **cooperate with other national cybersecurity certification authorities**, market surveillance authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities with the			

	requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; (k) **monitor relevant developments in the field of cybersecurity certification**. 8. 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, ICT processes, managed security services and the cyber posture of entities. 9. By [entry into force + 6 months], ENISA shall develop a template for the report referred to in paragraph 6 point (i) of this Article, in cooperation with the Commission and the ECCG.			
Article 89 Peer review	5. **ENISA shall support** the organisation of the peer review mechanism and the peer reviews, including **by developing relevant guidance documents and templates**, in cooperation with the Commission and the ECCG. 7. The **final report including possible** guidelines or recommendations, the summary of the peer review shall be examined by the ECCG, which shall endorse the summary for publication on the referred to in Article 79(2).	EU ENISA ECCG	Making data available online	Data flow Data processing

Article 90 European cybersecurity certification group (ECCG)	3. The ECCG shall have the following tasks: [reference to other articles] (h) to examine relevant developments in the field of cybersecurity certification, including at national level pursuant to Article 86, and to exchange information and good practices on cybersecurity certification schemes; (i) to facilitate the cooperation between national cybersecurity certification authorities under the rules set out in this Title through capacity-building and exchange of information, in particular relating to issues concerning cybersecurity certification; [reference to other articles] (k) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including as part of the maintenance of existing European cybersecurity certification schemes and, where appropriate, to make recommendations to ENISA to engage with relevant European or international standardisation organisations to address insufficiencies or gaps in available European or internationally recognised standards.	Member States ENISA EU Commission	Analysis, sharing information and cooperation between Member States authorities and international organisations in relation to European cybersecurity certification	Data processing Data flow
Article 92 Additional harmonisation of the competence of conformity assessment bodies	4. Where a national cybersecurity certification authority receives a request pursuant to paragraph 3 it shall **inform the national cybersecurity certification authority of the Member State in which the requesting conformity assessment body is established**. In such cases, the national cybersecurity certification authority of that Member State may	Member States authorities Conformity assessment bodies	Information sharing and retention	Data flow Data processing

	participate in the authorisation as an observer.			
Article 93 Notifications of conformity assessments bodies	1. For each European cybersecurity certification scheme, the national cybersecurity certification **authorities of a Member State shall notify the Commission and the other Member States** of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 92. 2. **The national cybersecurity certification authorities shall carry out the notification as referred to in paragraph 1** using the electronic notification tool developed and managed by the Commission.	ENISA Member States EU Commission Conformity assessment bodies	Notifications of accredited and authorised conformity assessment bodies	Data flows Data processing
Article 94 Challenge of the competence of conformity assessment bodies	1. 1. **The Commission shall investigate** any cases in which it has doubts, or is made aware of doubts about the competence of a conformity assessment body to meet, or the continued fulfilment by a conformity assessment body of, the requirements and responsibilities to which it is subject. 2. **The national cybersecurity certification authority shall provide the Commission,** on request, with all information relating to the basis for the notification or the maintenance of the competence of the conformity assessment body concerned. 3. **The Commission shall ensure that all**	Commission Member States ENISA	Challenge of the competence of conformity assessment bodies	Data flow Data process Digital public service

	sensitive information obtained in the course of its investigations is treated confidentially. 4. Where the Commission ascertains that a conformity assessment body does not meet or no longer meets the requirements for its notification, it **shall inform the national cybersecurity certification authority accordingly** and request it to take the necessary corrective measures, including de-notification if necessary.			
Article 95 Information and retention obligation on conformity assessment bodies	1. Conformity assessment bodies **shall inform the national cybersecurity certification authority** of the following: (a) any refusal, restriction, suspension or withdrawal of a certificate; (b) any circumstances affecting the scope of and conditions for the notification referred to in Article 93(1); (c) any request for information that they have received from market surveillance authorities regarding conformity assessment activities; (d) on request, any conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting. 2. **Conformity assessment bodies shall also provide ENISA with the information** referred to in paragraph 1 point (a) in view of facilitating the performance of its task under Article 79. 3. **Conformity assessment bodies shall**	Member States authorities Conformity assessment bodies	Information exchange from the conformity assessment bodies	Data flow Data processing

	provide the other conformity assessment bodies under this Regulation carrying out similar conformity assessment activities covering the same ICT products, ICT services, ICT processes, managed security services or entities the cyber posture of which is certified without undue delay **with relevant information** on issues relating to negative and, upon request, positive conformity assessment results. 4. **Conformity assessment bodies shall maintain a record system**, containing all the documents and evidence produced or received in connection with each evaluation and certification that they perform. The record shall be stored in a secure and accessible manner for the period necessary for the purposes of certification and for at least five years after the expiry or withdrawal of a relevant European cybersecurity certificate.			
Article 96 Rights to lodge a complaint and right to an effective judicial remedy	2. The authority or body with which the complaint has been lodged **shall inform the complainant of the progress** of the proceedings, of the decision taken, and of the right to an effective judicial remedy referred to in paragraphs 3 and 4. 4. 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.	Member States authorities EU Commission General public Certificate holders	Information flow between authorities and general public regarding complaints Proceedings before the courts of the Member State	Data flow

Article 97 Penalties	**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.	Member States authorities EU Commission	Information flow related to notification from Member States to the Commission regarding penalties.	Data flow
Article 99 Security risk assessments	The Commission or at least three Member States may request NIS CG to conduct coordinated risk assessments within 6 months. The Commission may request shorter deadlines. The risk assessments shall develop risk scenarios and presume data analysis. The preparation of the coordinated security risk assessments In cases that justify an immediate intervention, the Commission shall without delay consult the Member States and conduct a risk assessment. Decisions for undergoing risk assessments (data processing/analysis).	EU Commission EU Member States NIS Cooperation Group ENISA	Requesting and receiving information; data analysis for the purposes of coordinated risk assessments Consultation with the Member States and conduct a risk assessment	Data processing Data flow
Article 100 (1) and (2) Designation of third countries posing cybersecurity concerns	1. Where, as a result of the security risk assessment referred to in Article 99, or based on other sources, such as a public statement on behalf of the Union or a Member State, it appears that a third country poses serious and structural non-technical risks to ICT supply chains, the Commission shall verify the threat posed by that country, taking into account a series of elements,	EU Member States EU Commission	Receiving information, analysing information, exchange of information.	Data flows Data processing

	leading to data processing/analysing. 2. When the Commission, following the verification referred to in paragraph 1, concludes that a third country poses serious and structural non-technical risks to ICT supply chains, it may decide, by means of an implementing act, to designate that third country as a country posing cybersecurity concerns to ICT supply chains, leading to data processing analysing and data flows.			
Article 101 General ICT supply chain mechanism Article 102 Identification of key ICT assets and Article 103	1. Where the NIS Cooperation Group has conducted a Union level coordinated security risk assessment pursuant to Article 99(1) and (2) of this Regulation, or after the completion of the procedure in case of significant cyber threat pursuant to Article 99(3), the Commission may take measures provided for in Articles 102 and 103. Commission is empowered to adopt implementing acts, which will define key ICT assets and mitigation measures, including restrictions and prohibitions of ICT supply chains (detailed in section 4.5 below). In preparation for this process, the Commission shall take into account and in consideration several aspects, which evoke **data processing/analysing and in some cases data flow**:	EU Commission NIS Cooperation Group Relevant stakeholders	Analysis of data/data processing; consultation with relevant stakeholders	Data processing Data flow

Mitigation measures in the ICT supply chains	Article 102 (a)-(f) Article 103 (4) (a)-(d) Article 103(6)			
Article 104 Identification of high-risk suppliers	By way of implementing acts, the Commission shall establish lists of high-risk suppliers relevant for the prohibitions laid down in the implementing acts adopted in accordance with Article 103(1) or the prohibition referred to in Article 111(1). The Commission shall map the suppliers providing ICT components and components that include ICT components and do an initial assessment, which suppliers are potentially established in or controlled from third countries designated in accordance with Article 100. The Commission shall assess the place of establishment as well as the ownership and control structure. The Commission shall be entitled to request the necessary information from the suppliers and shall share preliminary findings concerning the establishment, ownership and control assessment to the concerned supplier and grant them an opportunity to be heard.	EU Commission Competent authorities Suppliers	Analysis of data/data processing; consultation with competent authorities, consultation with suppliers	Data processing Data flow

	The Commission may ask a competent authority to carry out the initial establishment, ownership and control assessment of a supplier, where justified in view of the characteristics of the operation of this supplier. A competent authority may offer to carry out such initial assessment. The Commission shall verify these initial findings in view of deciding whether the supplier should be included in the list of high-risk suppliers. The Commission shall regularly update the lists of high-risk suppliers in view of removing or adding high-risk suppliers. High-risk suppliers included in the list may request the Commission to re-assess their establishment, control and ownership structure upon provision of evidence that there have been relevant changes.			
Article 105 Exemption of entities established in or controlled by entities from a third country posing cybersecurity concerns Article 108 Confidentiality	(1) An entity established in or controlled from a designated third country posing cybersecurity concerns **may make a reasoned request** to the Commission. (3) The Commission shall assess and adopt a decision **taking account of several aspects** leading to data analysis. (Article 105 (3 and 4)) Information received by the Commission	EU Commission Entities established in or controlled by entities from a designated third country posing cybersecurity concerns	Commission receiving request; analysing data.	Data flow Data processing

	shall be used only for the purpose for which it was acquired.			
Article 107 Register	The Commission shall maintain a publicly accessible register of its decisions referred to in Article 105. The register shall state the names of the entities that have been subject to the decisions.	EU Commission Entities established in or controlled from a designated third country posing cybersecurity concerns	Commission maintaining publicly accessible register.	Digital solution
Article 111 Prohibitions for mobile, fixed and salttelite electronic communication networks	The competent authority designated under this Regulation **shall inform** without delay the competent authority pursuant to Regulation (EU) XX/XXXX [DNA proposal] about the measures imposed on providers of mobile, fixed and satellite electronic communications networks.	Competent authority in the sense of Article 9 or 20 of Regulation (EU) XX/XXXX [DNA Proposal] Providers of mobile, fixed and satellite electronic communications networks	Information flow from competent authority to entities in relation to authorisations.	Data flow
Article 112 (1), (4) Competent authorities	(1) **Each Member State shall designate** one or more competent authorities responsible for the supervisory and enforcement tasks referred to in Article 114. (4) Each Member State shall without undue delay notify the Commission of the names of the competent authorities designated in	EU Member States EU Commission General public	Member States designating competent authorities and notifying the Commission.	Data flow

	accordance with paragraph 1, of the respective tasks of those authorities and of any subsequent changes thereto. Each Member State shall also make public the names of the competent authorities designated in accordance with paragraph 1.			
Article 113 Network for cooperation and support services of the Commission	1. The Commission shall set up a network for cooperation of competent authorities of Member State and the Commission to serve as a platform for cooperation and exchange of information. The Commission shall provide the administrative support to the network. 2. To support Member States in their supervisory tasks, the Commission shall assess whether suppliers that may be affected by specific prohibitions are established in or controlled from third countries posing cybersecurity concerns, designated pursuant to Article 100. For that purpose, the competent authority shall share relevant information with the Commission. 3. For the purpose of the assessment, the Commission shall be entitled to request the necessary information from the suppliers that may be affected by specific prohibitions that are established in or controlled from third countries designated pursuant to	Commission Competent authorities Entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555	Commission assessing suppliers and sharing with competent authorities that share with entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 Commission requesting information from suppliers Competent authorities informing the Commission	Data processsing Data flows

	Article 100. 4. When an assessment is completed, the Commission shall share the findings with the competent authorities within the network established pursuant to paragraph 1. The competent authorities shall in due time inform the concerned entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555 of the findings. 5. Where a competent authority becomes aware of a supplier which may be affected by specific prohibitions is established in or controlled from third countries posing cybersecurity concerns, and which has not undergone an assessment, it shall inform without undue delay the Commission.			
Article 114 Supervisory and enforcement measures	Requirements to Member States that will ensure flow of information with the entities referred to in Annex I and II of Directive (EU) 2022/2555. competent authorities. Before adopting measures, the competent authorities shall notify the entities concerned of their preliminary findings. The competent authorities shall cooperate with each other and with the Commission.	EU Member States EU Commission Entities within the context of Annex I and II of Directive (EU) 2022/2555	Requirements that ensure flow of information;	Data flow Data processing

Article 115 Penalties	Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendments affecting them.	EU Commission EU Member States	Member States notifying the Commission	Data flow
Article 116 Mutual assistance	Where an entity referred to Annex I or II of Directive (EU) 2022/2555 provides services in more than one Member State or provides services in one or more Member States and its key assets are located in one or more other Member States, **the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary**. The mutual assistance referred to in the first subparagraph, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if	EU Member States	Mutual assistance in supervision actions.	Data flow Data processing

	disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission. Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.			
Article 1, point 8, Directive Reporting of ransomware attacks (Article 27.13 NIS2)	in Article 23 the following paragraphs 12 and 13 are added: '13. Member States shall ensure that in case of a significant incident caused by a ransomware attack, the entities concerned inform, upon request of the CSIRT or, where applicable, the competent authority via a communication channel provided by the CSIRT or, where applicable, the competent authority: if the entity has received a ransom demand and, where applicable, by whom; if a ransom was paid and if yes, what amount in what means of payment and to which recipient or receiving end, including the crypto-asset and crypto-asset service provider, where applicable.'	EU Member States Essential and important entities	Reporting	Data flow

Article 1, point 10, Directive List of entities and registry (Article 27.1 NIS2)	**ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 2**.	ENISA EU Member States (essential and important entities under NIS2, entities providing domain name registration services)	ENISA shall create and maintain a registry	Digital Solution Digital public service
Article 1, point 11, Directive List of entities and registry (Article 27.4 NIS2)	**'4. Upon receipt of the information referred to in Article 3 (4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.'**	ENISA EU Member States	Member States sharing information with ENISA	Data flow
Article 1, point 12, Directive Mutual assistance (Article 37a NIS2 (1), (2), (3))	**1. ENISA shall assist Member States** in carrying out mutual assistance within the meaning of Article 37 and **help facilitate such cooperation processes** for essential and important entities (…). 2. ENISA shall **conduct a comprehensive analysis** (…) **ENISA shall, in cooperation with** the Commission and the Cooperation Group, develop a methodology. The report shall be updated yearly. (3.) ENISA shall, where appropriate, recommend; develop guidelines; assist (…)	ENISA EU Member States Important and essential entities in the sense of Directive NIS2 EU Commission	ENISA shall assist Member States and help facilitate cooperation process. Conducting analysis, guidelines, methodology, reports.	Data processing Data flow
Article 1, point 12, Directive Mutual assistance (Article 37a NIS2 (4))	4. For the purpose of paragraph (4) point (e) of this Article, the competent authorities of the **Member States concerned shall, where available, provide the following to ENISA** (....). 5. Where a Member State receives mutual	ENISA EU Member States	Information exchange	Data flow

	assistance as referred to in Article 37(1), first subparagraph, point (c), **the single point of contact shall inform ENISA** that mutual assistance took place.			
Article 119 Exercise of the delegation	3. As soon as it adopts a delegated act, the Commission shall **notify it simultaneously** to the European Parliament and to the Council.	EU Commission European Parliament Council	Information sent to EP and Council	Data flow
Article 120 Evaluation and review	1. By [DD MM YYYY], and every five years thereafter, the Commission shall commission an evaluation of ENISA's performance in relation to its objectives, mandate, mission, tasks, governance and location in accordance with Commission's guidelines. 5. The Commission shall report to the European Parliament, the Council and the Management Board on the evaluation findings. The findings of the evaluation shall be made public.	ENISA Commission General public	Gathering and analysis of data; making information publicly available	Data processing Data flow

4.2. Data

High-level description of the data in scope and any related standards/specifications

Type of data	**Reference(s) to the requirement**	**Standard and/or specification (if applicable)**

Data connected to analysis/reports of relevance to the cybersecurity resilience and society	**Article 5(1)(a), (b), (c), (e), (f), (h)** **Article 5(2), (3) and (4)** **Article 6** **Article 7** **Article 8** **Article 9** **Article 10** **Article 11 (2)(b), (c)** **Article 12 (4)** **Article 15** **Article 1, point 7, Directive**	In carrying out the activities listed in Article 11 paragraph 1, points (a) to (e), and paragraph 2, ENISA shall use its own analyses and, as appropriate, the information received in carrying out its tasks, including: (a) information provided in publicly available sources, including publicly known vulnerabilities in ICT products or ICT services available in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555; (b) information shared by Member States, Union entities, CERT-EU, private sector or non-governmental partners and third country and international organisations, subject to any limitations by means of a visible marking on further distribution of that information. ENISA shall issue guidelines regarding the interoperability of network information systems used for information-sharing, including with regard to Cross-Border Cyber Hubs as referred to in Article 6(3) of Regulation (EU) 2025/38.
Data of relevance to the operational cooperation and situational awareness	**Article 10(4)(a) – (g)** **Article 10(6)** **Article 11(1)(a) – (g)** **Article 11(2)(a), (b), (c)** **Article 11(3)** **Article 11(4)** **Article 13(2)** **Article 15** **Article 16(2)(e)**	**Standards for confidentiality and handling sensitive information** In carrying out the activities listed in Article 11 paragraph 1, points (a) to (e), and paragraph 2, ENISA shall use its own analyses and, as appropriate, the information received in carrying out its tasks, including: (a) information provided in publicly available sources, including publicly known vulnerabilities in ICT products or ICT services available in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555; (b) information shared by Member States, Union entities, CERT-

		EU, private sector or non-governmental partners and third country and international organisations, subject to any limitations by means of a visible marking on further distribution of that information.
Data with relevance to the European individual cybersecurity skills attestation schemes and authorisation of providers **Data with relevance to the objectives, purpose and content of European cybersecurity certification schemes**	**Article 17** **Article 18** **Articles 19-23** **Articles 72, 73, 74, 75, 76, 77, 79, 81, 83, 84**	A European individual cybersecurity skills attestation scheme shall include (…): rules concerning the retention of records by authorised attestation providers Authorised providers shall ensure that, at the request of the individual, electronic attestations of European individual cybersecurity skills attestations are issued as electronic attestations of attributes in a format that can be stored in the European Digital Identity Wallets set out in Regulation (EU) No 910/2014. . The Commission and ENISA should follow relevant provisions of Union legislation when establishing a European cybersecurity certification scheme for what pertains to data.
Data related to the governance of the European cybersecurity certification framework	**Articles 85, 86, 88, 89, 90, 92, 93, 94, 95, 96, 97**	ENISA, conformity assessment bodies and national cybersecurity certification authorities should ensure confidentiality of data and follow provisions of a relevant scheme referring to international standards that specify the requirements.
Data with relevance to the internal ENISA functions (budget, SPD, internal strategies)	**Article 25** **Article 28(1)** **Article 30** **Article 31(8)** **Article 32(3), (5)** **Article 35(5), (6)** **Article 36-43** **Article 44** **Article 45**	**Financial regulation templates and guidelines; internal guidelines**

	Article 47(10) **Articles 48-49** **Article 52, Article 58**	
Personal data	**Article 22** **Title II, Chapter III, Section 6 Board of Appeal** **Article 66** **Article 80 (1) (c), (x)** **Article 81 (2)** **Article 88 (6) (h)** **Article 95** **Article 96**	**Regulation (EU) 2018/1725** **Regulation (EU) 2016/679**
Data, gathered and analysed in the context of conducting coordinated risk assessments, developing of risk scenarios and identification of key ICT assets	**Article 98** **Article 99** **Article 102** **Article 103** **Article 105**	Without prejudice to Article 13 of Regulation (EU) 2024/2847 and Article 21 of Directive (EU) 2022/2555
Data regarding third countries/ entities of third countries	**Article 100 (1), (3), (4)** **Article 104** **Article 105** **Article 107** **Article 113**	N/A
Data concerning national authorities	**Article 112** **Article 114** **Article 116**	N/A

Data with relevance to the risk assessments	**Article 5(2)**	**Standards for confidentiality and handling sensitive information**
Mutual assistance between Member States	**5(1)(g) regulation and Article 1, point 12 Directive**	**/**

Alignment with the European Data Strategy

Explain how the requirement(s) are aligned with the European Data Strategy

The requirements within the CSA2 proposal are aligned with no specific impact insofar the European Data Strategy.

Alignment with the once-only-principle

Explain how the once-only-principle has been considered, how the possibility to reuse existing data explored

One of the objectives of the proposal is to maximise the simplification efforts of the Commission and reduce the administrative burden for Member States and stakeholders. In the recent years ENISA has become an information hub, holding information from different sources. In this sense, many of the tasks for ENISA are associated with reusing and recycling of information for the purposes of various analyses. For example: for some purposes reusing information notified pursuant to Articles 23 and 30 of Directive (EU) 2022/2555; notified, shared or analysed pursuant to Article 14(1)-(3), Article 15 and Article 17(1) and (3) of Regulation (EU) 2024/2847. The provisions of the supply-chain framework are presuming its implementation to be supported by the data received through Article 22 of Directive (EU) 2022/2555, which shows reuse of information and coordination.

Explain how newly created data is findable, accessible, interoperable and reusable, and meets high-quality standards

The legislative proposal explicitly indicates when data should be made publicly available. The proposal is considering the nature of the provisions with strictly security and confidentiality aspects and therefore not all the data created under CSA review will be for public

consumption. For the necessary provisions, alignment with the European Digital Identity Wallet has been ensured. ENISA is tasked to offer early alerts service in in a machine-readable format.

Data flows

High-level description of the data in scope and any related standards/specifications

Type of data	Explain the data flow	References
ENISA providing reports and analysis, technical guidance and best practices.	This is a dataflow that is directed to ENISA stakeholders, supporting the implementation of EU policy and law. In these dataflows, ENISA is gathering information, most of the time through public sources, making analysis and sharing the outcomes with its stakeholders. ENISA is implementing certain tasks also when requested by the Commission.	Article 5(1)(a), (b), (c), (e), (f), (h) Article 5(2); Article 5(3) ; Article 5(5) Article 6 Article 7 Article 8 Article 9 Article 10 Article 11(2) Article 11(4) Article 14
Data flows between Commission, ENISA, the Member States and other relevant actors within the EU cybersecurity ecosystem, within the sense of operational cooperation.	This type of dataflows are established for the purposes of operational cooperation and situational awareness. The information exchange is in both directions, in and out. The exchange is of operational data.	Article 10(4)(a)-(g) Article 11(1)(b)-(g) Article 11(2)(a), (b) Article 11(3) Article 15 Article 16(2)(e)

Data flows established to support the ECSF and the European individual cybersecurity skills attestation schemes and their implementation	These data flows support exchanges in and out for: - the maintenance and uptake of the ECSF, with flows between ENISA and its ad hoc working group members and between ENISA and the Commission; - the development and maintenance of European individual cybersecurity skills attestation schemes with flows between ENISA and its ad hoc working group members and between ENISA, the Commission and Member States; - the implementation of European individual cybersecurity skills attestation schemes with data flows between applicants and ENISA; - data flows between the Board of Appeals, ENISA, the Commission and applicants.	Article 19 to 23 Articles 36 to 43
Data with relevance to the objectives, purpose and content of European cybersecurity certification schemes	This type of data flows is relevant to planning, requesting, development, adoption and maintenance (including possible review) of European cybersecurity certification schemes. It is in particular related to engagement and expert advice of stakeholders, ENISA, Member State authorities through ECCG at various stage of procedure. Furthermore, additional data flows are related to provision of relevant information to general public through dedicated Commission and ENISA websites. Finally, framework envisages public availability of supplementary cybersecurity information by the manufacturers or providers of ICT products, ICT services or ICT processes for which an EU statement of conformity or European cybersecurity certificate has been issued by their own means.	Article 18 Article 19 Articles 72, 73, 74, 75, 76, 77, 79, 81, 83, 84

Data related to the governance of the European cybersecurity certification framework	These data flows support exchanges in and out for: - coordination and management of European cybersecurity certification schemes - accreditation and authorisation of conformity assessment bodies as well as their subsequent notification through relevant platform and related procedures - recourse procedures such as right to lodge a complaint, judicial remedy or appeal and change procedures	Articles 85, 86, 88, 89, 90, 92, 93, 94, 95, 96
Data flows in relation to the administrative activities of the Agency	Flows between ENISA, Management Board, Member States, Commission. The information is regarding the administrative activities of the Agency, both directions. Information is also being sent to European Parliament in some cases (data flow in that respect is presented below)	Article 25 Article 28(1) Article 30 Article 31(8) Article 32(3), (5) Article 35(5), (6) Article 36-43 Article 44 Article 45
Data sent to the European Parliament	Flows to the European Parliament regarding ENISA activities and performance of tasks; budget and financial management, cooperation with third countries and international organisations, hearing of the candidate for executive director; matters related to European cybersecurity certification	Article 28(1)(f), Article 31(8), Article 32(3), Article 44(3), Article 49(6), Article 49(9), Article 70(5), Article 72 (4) and (5), Article 119(3) Exercise of the delegation, Article 120 Evaluation and review
Data sent to the Council of the EU	Flows to the European Parliament regarding ENISA activities and performance of tasks; budget and financial management, cooperation with third countries and	Article 28(1)(f), Article 31(8), Article 32(3), Article 32(7), Article 49(6), Article 49(9), Article 70(5), Article 72 (4), (5), Article 119(3) Exercise of the delegation, Article 120 Evaluation and review

	international organisations, hearing of the candidate for executive director; candidate schemes under development pursuant to European cybersecurity certification framework.	
Data flows in relation to filing a complaint	To 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 84(4) or in relation to EU statements of conformity 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	Article 55(3); Article 88 (7) (f); Article 96
Data flows regarding ransomware attacks	Reporting of certain information in case of ransomware attacks	Article 1, point 8, Directive

Type of data	**Reference(s) to the requirement(s)**	**Actors who provide the data**	**Actors who receive the data**	**Trigger for the data exchange**	**Frequency (if applicable)**
Data flows between Commission and Member States in the context of conducting Union-level coordinated security risk assessments.	Article 99 Security risk assessments	Commission and Member States	Member States (NIS Cooperation Group)	Article 99 Security risk assessments	N/A

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
Data flows between Commission and Council in relation to the designation of third countries posing cybersecurity concerns	Article 100 Designation of third countries posing cybersecurity concerns	Commission	Council	Article 100 Commission verification of the threat posed by a third country	
Data flows between Commission and Member States in relation to mitigation measures in case of exceptional circumstances	Article 103 (6) Mitigation measures in the ICT supply chains	Commission	Member States	Exceptional circumstances	N/A
Data flows between Commission and suppliers and the Commission and competent authorities regarding assessment of establishment and ownership and control of suppliers	104 (4), (5), (6) Identification of high-risk suppliers	Suppliers Commission Competent Authorities	Competent Authorities Suppliers Commission	Implementing acts adopted in accordance with Article 103(1) and in relation to prohibition in Article 111(1)	N/A
Data flow between Commission and Member States in relation to supervisory powers in relation to the implementation of the trusted ICT supply chain security framework	Article 112 (1), (4) Competent authorities	Member States	Commission	Article 112 (1), (4) Competent authorities Article 114	N/A

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
	Article 114 Supervisory and enforcement measures			Supervisory and enforcement measures (Commission in cooperation with the Member States shall issue a list of entities affiliated to high-risk suppliers.)	
Data flow between Commission and third parties for exemptions	Article 105 Exemption of entities established in or controlled from a third country posing cybersecurity concerns	Third parties (Entities established in or controlled by entities from a third country posing cybersecurity concerns (in the sense of Article 100) (when submitting a request for exemption) EU Commission (when issuing decisions)	Commission (when receiving the request for exemption) Third parties (entities established in or controlled by entities from a third country posing cybersecurity concerns (in the sense of Article 100) (when receiving the Commission's	Decision under Article 100 Designation of third countries posing cybersecurity concerns	N/A

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
			decision)		
Data flow between Member States and third parties in relation to prohibitions in electronic communication networks	Article 111 Prohibitions for mobile, fixed and satellite electronic communication networks	Member States (Competent authorities)	Third parties (Providers of mobile, fixed and satellite electronic communications networks)	The competent authority designated under this Regulation shall inform without delay the competent authority pursuant to Regulation (EU) XX/XXXX [DNA proposal] about the measures imposed on providers of mobile, fixed and satellite electronic communications networks	N/A
Data flow between Commission and Member States in the context of the network for cooperation and support services	Article 113 Network for cooperation and support services of the Commission	Commission Member States (Competent authorities)	Commission Member States (Competent authorities)	Designation of third countries posing cybersecurity concerns	

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
Data flow between Member States and third parties in relation to supervisory and enforcement measures	Article 114 Supervisory and enforcement measures	Third parties (Entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555)	Member States (Competent authorities)	Implementation of the measures foreseen in Title IV	
Data flow between Member States for mutual assistance	Article 116 Mutual assistance	Member States	Member States	Where an entity referred to Annex I or II of Directive (EU) 2022/2555 provides services in more than one Member State or provides services in one or more Member States and its key ICT assets are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as	N/A

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
				necessary.	

4.3. Digital solutions

High-level description of digital solutions

For each digital solution, explanation of how the digital solution complies with applicable digital policies and legislative enactments

Digital solution	Reference(s) to the requirement(s)	Main mandated functionalities	Responsible body	How is accessibility catered for?	How is reusability considered?	Use of AI technologies (if applicable)
ENISA being the **secretariat of CSIRTs network and EU-CyCLONe** and deploy within the CSIRTs network and EU-CyCLONe **secure communications tools** which are provided by legal entities that are not established in or controlled by third countries or by nationals of third countries.	Article 10 (2), (3), (5)	Not public information	ENISA	Not public information	Not public information	Not public information
Develop in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, Europol and CERT-EU and relevant Union entities **repositories of verified, reliable cyber threat intelligence**, including trends in incidents, tactics, techniques and procedures.	Article 11(1)(a)	verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures	ENISA EU-CyCLONe, the CSIRTs network, the Commission, Europol and CERT-EU and	N/A	N/A	N/A

			relevant Union entities			
ENISA shall **maintain a repository of lessons learned.**	Article 14(2)	ENISA shall maintain a repository of lessons learned from exercises and recommend to Member States and, where relevant, to Union entities how the lessons learned may be implemented effectively and efficiently.	ENISA	N/A	N/A	N/A
ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, such as **platforms** related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], or testing tools to support the implementation of conformity assessment procedures in accordance with relevant Union legislation.	Article 15	Single Reporting Platform Article 16(1) of Regulation (EU) 2024/2847 [single-entry point Article 23a of Directive (EU) 2022/2555]	ENISA	N/A	N/A	N/A
Maintain the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555 and **provide vulnerability management services**	Article 16(2)	Article 12(2) of Directive (EU) 2022/2555 Maintain the database and provide vulnerability management services	ENISA	N/A	N/A	N/A

ENISA shall maintain and regularly update a dedicated website providing public information	Article 19-23	Maintain and regularly update a dedicated website providing public information on the ECSF, including the framework and its timeline for update; the European individual cybersecurity skills attestation schemes, their progress and timelines for their development; the fees associated with each European individual cybersecurity skills attestation scheme; the indicative cost of a European individual cybersecurity skills attestation; the list of authorised attestation providers.	ENISA	N/A	N/A	N/A
The **Commission shall maintain and regularly update a dedicated public website**	Article 72	Following information: (a) European cybersecurity certification schemes requested for development; (b) strategic priorities for harmonisation of ICT products, ICT services,	EU Commission	Compliance with guidelines	Compliance with guidelines	N/A

		ICT processes, managed security services or security requirements of Union legislation, including potential areas for which a European cybersecurity certification scheme might be requested.				
ENISA shall maintain a dedicated certification website	Article 79	Providing information on: (a) European cybersecurity certification schemes; (b) the fees associated with the maintenance of each European cybersecurity certification scheme; (c) relevant ENISA technical specifications; (d) European cybersecurity certificates and EU statements of conformity, including information with regard to such certificates and statements which are no longer valid, or which are suspended, withdrawn or expired;	ENISA	Compliance with guidelines	Compliance with guidelines	N/A

		(e) relevant supplementary cybersecurity information provided in accordance with Article 84(2); (f) summaries of peer reviews pursuant to Article 89(7); (g) technical specifications referenced in a European cybersecurity certification scheme pursuant to Article 74(10).				
Register (of exemptions for entities established in or controlled by entities from a third country posing cybersecurity concerns)	Article 107 Register	The Commission shall maintain a publicly accessible register of its decisions referred to in Article 105(4). The register shall state the names of the entities that have been subject to the decisions. The Commission shall update it regularly.	Commission	"The Commission shall maintain a publicly accessible register"	N/A	N/A

Platform (for cooperation and exchange of information between the Commission and competent authorities)	Article 113	The Commission shall set up a network for cooperation of competent authorities of Member State and the Commission to serve as a platform for cooperation and exchange of information. The Commission shall provide the administrative support to the network.	Commission	Not public, only for competent authorities	N/A	N/A
ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services	Article 1, point 11, Directive	Registry of essential and important entities as well as entities providing domain name registration services	ENISA	N/A	On the basis of the information received from the single points of contact in accordance with paragraph 2. (Article 27 NIS2 Directive)	N/A

Digital solutions included in the table above

Digital and/or sectorial policy (when these are applicable)	Explanation on how it aligns
AI Act	N/A
EU Cybersecurity framework	N/A
eIDAS	N/A
Single Digital Gateway and IMI	N/A
Others	N/A

High-level description of the digital public service(s) affected by the requirements

Digital public service or category of digital public services	Description	Reference(s) to the requirement(s)	Interoperable Europe Solution(s) (NOT APPLICABLE)	Other interoperability solution(s)
ENISA as secretariat of networks and deploying secure communication tools	ENISA shall provide the secretariat of the CSIRTs network pursuant to Article 15(2) of Directive (EU) 2022/2555. ENISA shall provide the secretariat of EU-CyCLONe pursuant to Article 16(2) of Directive (EU) 2022/2555 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555], and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation. ENISA shall deploy within the CSIRTs network and EU-CyCLONe secure communications tools which are provided by legal entities that are not established in or controlled by third	Article 11	//	N/A

	countries or by nationals of third countries.			
Early alerts	Issuing early alerts	Article 11 Article 12		
Support in relation to a specific potential or ongoing incident or cyber threat	At the request of one or more Member States, providing advice and assessments in relation to a specific potential or ongoing incident or cyber threat, including through the provision of expertise and facilitating the technical handling of such incidents, and through supporting the voluntary sharing of relevant information and technical solutions between Member States;	Article 10		
Supporting the coordinated management of large-scale cybersecurity incidents and crises at operational level	Contributing to supporting the coordinated management of large-scale cybersecurity incidents and crises at operational level, in particular by assisting EU-CyCLONe in preparing reports to political level by facilitating and by facilitating timely information-sharing between the CSIRTs network, and EU-CyCLONe.	Article 10		
Repositories of verified, reliable cyber threat intelligence	Develop in cooperation with EU-CyCLONe, the CSIRTs network, the Commission, Europol and CERT-EU and relevant Union entities repositories of verified, reliable cyber threat intelligence, including trends in incidents, tactics, techniques and procedures.	Article 11		
Repository of lessons learned	ENISA shall maintain a repository of lessons learned from those exercises and recommend to Member States and, where relevant, to Union entities how the lessons learned may be implemented effectively and efficiently.	Article 14		
ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, such as platforms	ENISA shall establish, provide, operate, maintain and update as necessary, operational technical tools, such as platforms related to cybersecurity at Union level, in particular the single reporting platform established pursuant to Article 16(1) of Regulation (EU) 2024/2847 [and the single-entry point for incident reporting established pursuant to Article 23a of Directive (EU) 2022/2555] and testing tools to support the implementation of conformity assessment procedures in accordance with the relevant Union legislation.	Article 15		
Maintain the European Vulnerability Database established pursuant to Article 12(2) of Directive (EU) 2022/2555	Maintain the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555. Provide vulnerability management services to stakeholders, building on the European vulnerability database and making use of relevant information available to ENISA.	Article 16		

	Enter into structured cooperation with organisations providing programmes, registries or databases similar to the European vulnerability database. Actively support the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555 with regard to the management of the coordinated disclosure of vulnerabilities which may have a significant impact on entities in more than one Member State. Develop and maintain methodologies and governance mechanisms for vulnerability identification and coordinated disclosure, in cooperation with national competent authorities, CSIRTs, industry and the research community.			
Preparing candidate European cybersecurity certification schemes 'candidate schemes'	Preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities, and related technical specifications in accordance with Articles 74. Maintaining adopted European cybersecurity certification schemes in accordance with Article 75, including in view of a possible review of the adopted European cybersecurity certification schemes in accordance with Article 76.	Article 17		
ENISA shall develop and maintain European individual cybersecurity skills attestation schemes	ENISA shall develop and maintain European individual cybersecurity skills attestation schemes. ENISA shall issue a motivated decision either granting an authorisation to the applicant to issue European individual attestations for the delivery and maintenance of the schemes and of the authorisation, not granting the authorisation, or closing the processing of the application due to insufficient information provided by the applicant, or its inaction following a request for additional information.	Articles 20-22		
ENISA shall maintain and regularly update a dedicated website.	ENISA shall maintain and regularly update a dedicated website providing public information on: (a) the ECSF, including the framework and its timeline for update; (b) the European individual cybersecurity skills attestation schemes, their progress and timelines for their development;	Article 23		

	(c) the fees associated with each European individual cybersecurity skills attestation scheme adopted pursuant to Article 47 of this Regulation; (d) the indicative cost of a European individual cybersecurity skills attestation in accordance with Article 20(4); (e) the list of authorised attestation providers.			
The Commission shall maintain and regularly update a dedicated public website	The Commission shall maintain and regularly update a dedicated website providing information on the following aspects: (a) European cybersecurity certification schemes requested for development; (b) strategic priorities for harmonisation of ICT products, ICT services, ICT processes, managed security services or security requirements of Union legislation, including potential areas for which a European cybersecurity certification scheme might be requested.	Article 72		
ENISA shall maintain a dedicated certification website	ENISA shall maintain and regularly update a dedicated website providing public information on the following: (a) European cybersecurity certification schemes; (b) the fees associated with the maintenance of each European cybersecurity certification scheme; (c) relevant ENISA technical specifications; (d) European cybersecurity certificates and EU statements of conformity, including information with regard to such certificates and statements which are no longer valid, or which are suspended, withdrawn or expired; (e) relevant supplementary cybersecurity information provided in accordance with Article 84(2); (f) summaries of peer reviews pursuant to Article 89(7); (g) technical specifications referenced in a European cybersecurity certification scheme pursuant to Article 74(10).	Article 79		
Investigations	The Commission shall investigate any cases in which it has doubts, or is made aware of doubts about the competence of a conformity assessment body to meet, or the continued fulfilment by a conformity assessment body of, the requirements and responsibilities to which it is subject. The Commission shall ensure that all sensitive information obtained	Article 94		

	in the course of its investigations is treated confidentially.			
ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services	Registry of essential and important entities as well as entities providing domain name registration services. Upon request, ENISA shall allow the competent authorities access to information concerning DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms stored in that registry, while ensuring that the confidentiality of information is protected where applicable.	Article 1, point 11, Directive		

4.4. Interoperability assessment

Impact of the requirement(s) as per digital public service on cross-border interoperability

Repositories/platforms/early alerts/secretariat/operational cooperation/CVD database

Assessment	Measures	Potential remaining barriers
Assess the alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	*Cybersecurity*	*No known barriers*
Assess the organisational measures for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	*ENISA Management Board* *CSIRTs Network* *EU-CyCLONe* *NIS Cooperation Group* *All of these are forums where issues can be raised.*	*N/A*
Assess the measures taken to ensure a shared understanding of the data	*N/A*	*N/A*

Please list such measures		
Assess the use of commonly agreed open technical specifications and standards **Please list such measures**	*N/A*	*N/A*

European individual cybersecurity skills attestation schemes

Assessment	Measures	Potential remaining barriers
Assess the alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	*The proposal builds on COM(2023)207 final (Cybersecurity Skills Academy) "ENISA will develop a pilot project, exploring the set-up of a European attestation scheme for cybersecurity skills"* *It makes use of Regulation (EU) 2024/1183 (EUDI wallet) by establishing that- "ENISA and authorised attestation providers shall ensure that the electronic attestations of the European individual cybersecurity skills attestation are issued to the European Digital Identity Wallets"* *Cybersecurity* *GDPR (retention of records by providers)*	*No known barriers*
Assess the organisational measures for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	*Consultation of stakeholders when preparing a European individual cybersecurity skills attestation scheme* *Separation of activities within ENISA to ensure independent performance thereof* *Board of Appeal*	*The use and recognition of European individual cybersecurity skills attestation schemes shall remain voluntary for public and private entities.*
Assess the measures taken to ensure a shared understanding of the data **Please list such measures**	*Developing schemes that detail inter alia rules concerning the content and format of the*	*Although the schemes should be as detailed as to ensure common understanding and ease implementation, and although ENISA will provide guidance to and conduct*

	attestations *Authorised providers shall ensure that, at the request of the individual, electronic attestations of European individual cybersecurity skills attestations are issued as electronic attestations of attributes in a format that can be stored in the European Digital Identity Wallets ENISA to provide guidance to and conduct obligatory training of assessors regarding the requirements and assessment methods included in the European individual cybersecurity skills attestation scheme* *Providing public information on a website* *Implementing acts on fees*	*obligatory training of assessors to ensure consistent implementation of the schemes, unforeseen dimensions could arise where authorised attestation providers need to interact with ENISA, other providers or assessors.*
Assess the use of commonly agreed open technical specifications and standards **Please list such measures**	*European individual cybersecurity skills attestation schemes are developed with the support of relevant stakeholders*	*N/A*

Preparing candidate European cybersecurity certification schemes 'candidate schemes'/ assigning numbers to CABs

Assessment	Measures	Potential remaining barriers
Assess the alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	*The proposal seeks alignment on governance with the New legislative framework, in particular for what pertains Regulation (EC) 765/2008*[26]. *The proposal aims to facilitate compliance with relevant cybersecurity sectoral legislation through development of dedicated European cybersecurity certification schemes.*	*No known barriers*

Assess the organisational measures for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	*European Cybersecurity Certification Group; ENISA;* *Ad hoc working groups;* *European Cybersecurity Certification Assembly;* *Consultation of stakeholders when requesting, developing and adopting European cybersecurity certification schemes;* *Comitology procedures for envisaged implementing acts related to European cybersecurity certification schemes.*	*The use of European cybersecurity certification shall be voluntary unless otherwise specified in European legislation.*
Assess the measures taken to ensure a shared understanding of the data **Please list such measures**	*Implementing acts listed section 4.5.*	*The use of European cybersecurity certification shall be voluntary unless otherwise specified in European legislation.*
Assess the use of commonly agreed open technical specifications and standards **Please list such measures**	*Implementing acts listed section 4.5.* *The specified requirements of the European cybersecurity certification scheme shall be consistent requirements of Union legislation.* *European cybersecurity certification schemes shall leverage and reference the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications drawn by ENISA.*	*N/A*

Publicly accessible websites

Assessment	Measures	Potential remaining barriers
Assess the alignment with existing digital and sectorial policies **Please list the applicable digital and sectorial policies identified**	*EU Accessibility Act and Web Accessibility Directive* *Cybersecurity*	*No known barriers*
Assess the organisational measures		

for a smooth cross-border digital public services delivery **Please list the governance measures foreseen**	*N/A*	*N/A*
Assess the measures taken to ensure a shared understanding of the data **Please list such measures**		*N/A*
Assess the use of commonly agreed open technical specifications and standards **Please list such measures**		*N/A*

4.5. Measures to support digital implementation

High-level description of measures supporting digital implementation

Description of the measure	**Reference(s) to the requirement(s)**	**Commission role** (if applicable)	**Actors to be involved** (if applicable)	**Expected timeline** (if applicable)
The Commission, based on the accepted candidate scheme prepared by ENISA, is empowered to adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes, managed security services or cyber posture of entities that meets the requirements set out in Articles 80 and 81. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 118(2).	Article 75(9)	Commission is empowered to adopt implementing acts		N/A
The Commission is empowered to adopt	Article 80(2)	Commission is		N/A

delegated acts in accordance with Article 119 to amend in paragraph 1 of this Article by adding or modifying security objectives in order to ensure that they reflect the latest technological development and new related threats as well as adoption of new Union legislation setting out the presumption of conformity through European cybersecurity certification with relevant cybersecurity requirements of that legislation.		empowered to adopt delegated acts		
The Commission is empowered to adopt implementing acts laying down common principles and model provisions for elements set out in paragraphs 1, 2 and 3 across European cybersecurity certification schemes. Where appropriate and available, a European cybersecurity certification scheme may include references to those principles and model provisions. The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 118(2). When developing or revising the common principles and model provisions for the elements of European cybersecurity certification schemes, the Commission shall consult ENISA and take into account, as appropriate, views expressed by the	Article 81(5)	Commission is empowered to adopt implementing acts	ENISA ECCG	N/A

ECCG, relevant stakeholders and other relevant bodies.				
The Commission is empowered to adopt implementing acts specifying procedures for prior approval or general delegation models referred to in paragraph 4 of this Article. In the preparation process for those implementing acts, the Commission shall consult the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	Article 85(5)	Commission is empowered to adopt implementing acts	ECCG	N/A
Third country certificates of ICT products, ICT services, ICT processes, managed security services and cyber posture of entities may be recognised, by means of an implementing act or through the conclusion of an agreement between the Union and the third country in question or an international organisation, as equivalent to European cybersecurity certificates if the requirements of the relevant third country scheme or international organisation scheme are considered equivalent to those in European cybersecurity certification schemes. The Commission is empowered to adopt such implementing acts. The implementing acts shall be adopted in accordance with the examination procedure	Article 87(1)	Commission is empowered to adopt implementing acts		N/A

referred to in Article 118(2).				
The Commission is empowered to 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 peer review. In the preparation of those implementing acts, the Commission shall consult the ECCG and ENISA. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	Article 89(6)	Commission is empowered to adopt implementing acts		N/A
The Commission is empowered to adopt implementing acts to lay down the procedures, including on cross-border cooperation, for authorisation of conformity assessment bodies. In the preparation process of implementing acts, the Commission shall consult ENISA and the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).	Article 92(8)	Commission is empowered to adopt implementing acts	ENISA ECCG	N/A
The Commission is empowered to adopt implementing acts to lay down the circumstances, formats and procedures for notifications referred to in paragraph 1 of	Article 93(3)	Commission is empowered to adopt implementing acts		N/A

this Article, including the objection procedure by other Member States during the notification process, the unique identification of conformity assessment bodies, as well as the circumstances for restriction, suspension or withdrawal of notification. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(2).				
The Commission may adopt implementing acts in accordance with Article 100 in order to designate a third country posing cybersecurity concerns to ICT supply chains.	Article 100 (2) Designation of third countries posing cybersecurity concerns	Adopting implementing acts		N/A No timeline but the implementing acts should be reviewed regularly
The Commission may adopt implementing acts to provide for one or several mitigation measures referred to in Article 103 (2).	Article 103 (2) Mitigation measures in the ICT supply chain	Adopting implementing acts	N/A	N/A No timeline, but to be reviewed every 36 months (in accordance with the examination procedure referred to in Article 118(2))
The Commission may adopt implementing acts in accordance with Article 102 in order to identify key ICT assets used for the manufacturing of products or the provision of services by the types of entity referred to Annex I and Annex II to Directive (EU)	Article 102 (1) Identification of key ICT assets	Adopting implementing acts	N/A	N/A

2022/2555.				
The Commission may adopt implementing acts prohibiting to use, install or integrate in any form ICT components or components that include ICT components from high-risk suppliers as designated in accordance with Article 100(2) in key ICT assets identified in accordance with Article 102.	Article 103 (1) Mitigation measures in the ICT supply chain	Adopting implementing acts	N/A	N/A
The Commission may adopt implementing acts to establish that entities of the types referred to in Annexes I and II to Directive (EU) 2022/2555 shall be prohibited to use, install or integrate ICT components or components that include ICT components from a specific entity.	Article 103 (7)	Adopting implementing acts	Consultation of Member States and the entities concerned	N/A
By way of implementing acts, the Commission shall establish lists of high-risk suppliers relevant for the prohibitions laid down in the implementing acts adopted in accordance with Article 103(1) or the prohibition referred to in Article 1110(1).	Article 104(1)	Adopting implementing acts	N/A	N/A
The Commission may adopt implementing actsto further specify the conditions referred to Article 105 paragraph 2 point (b), and to lay down detailed rules in respect of the procedures referred to in Article 105.	Article 105 Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns	Adopting implementing acts	N/A	N/A
The Commission may adopt implementing	Article 109	Adopting	N/A	N/A

acts laying down detailed rules relating to the fees, specifying the amount of the fees and the way in which they are to be paid.	Fees	implementing acts		
The Commission shall adopt implementing acts to specify the time periods for phasing out the the ICT components or components that include ICT components provided by high-risk suppliers with regard to fixed and satellite electronic communications networks .	Article 110 (4) Key ICT assets for mobile, fixed and satellite electronic communications networks	Adopting implementing acts	N/A	N/A
The Commission may adopt delegated acts in accordance with Article 119 to amend Annex II in order to adapt it to technological developments by taking into account the elements referred to in Article 103(3).	Article 110 (5)	Adopting delegated acts	N/A	N/A
7. Article 21(5) is amended as follows: (a) the second subparagraph is replaced by the following: ‘The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. The Commission shall regularly assess whether implementing acts referred to in this	Article 1, point 7, Directive Maximum harmonisation	Commission may adopt implementing acts		N/A

subparagraph shall be adopted for specific sectors or types of entities to improve the functioning of the internal market. Based on the outcome of those assessments, the Commission may propose such implementing acts for the identified sectors or types of entities. When preparing such assessments, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States.'; (b) the following subparagraph is inserted after the fourth subparagraph: 'Where the Commission adopts implementing acts referred to in the first and second subparagraphs of this paragraph, Member States shall not impose any further technical or methodological requirements of the measures referred to in Article 21 (2) of Directive (EU) 2022/2555 on the entities in scope of those implementing acts.'				