European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

# MANAGEMENT BOARD DECISION

**DECISION No. MB/2026/02**

**OF THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)**

**of date, 30 January 2026**

**on endorsing the draft Single Programming Document (SPD) 2027-2029, the draft statement of estimates for 2027 and the draft establishment plan for 2027**

## THE MANAGEMENT BOARD OF ENISA

**Having regard to**

- 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), in particular Article 15.1.(c), Article 24.3., Article 24.4., Article 29.3 and Article 29.7;
- Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council, in particular Article 32;
- Commission Communication C(2020) 2297 final of 20 April 2020 on the guidelines for single programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies.

**Whereas**

1. The Management Board should produce, on the basis of the draft drawn by the Executive Director, a statement of estimates of revenue and expenditure for the following year which will be forwarded by the Management Board to the European Commission by 31 January 2026;
2. The Management Board should endorse the draft programming document by 31 January 2026;
3. The Agency should send the draft programming document to the European Commission, the European Parliament and the Council no later than 31 January 2026;
4. The Executive Board has endorsed the draft single programming document 2027-2029 at its meeting held on 23 January 2026.

## HAS DECIDED TO ADOPT THE FOLLOWING DECISION

**Article 1**

The Programming Document 2027-2029 is endorsed as set-out in the Annex 1 of this decision.

**Article 2**

The statement of estimates of revenue and expenditure for the financial year 2027 and the establishment plan 2027 are endorsed as set-out in Annex 2 and Annex 3 of this decision.

**Article 3**

The present decision shall enter into force on the day of its adoption. It will be published on the Agency's website.

Done by written procedure 30.01.2026

On behalf of the Management Board

[signed]

Ms Fabienne Tegeler

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

# ENISA SINGLE PROGRAMMING DOCUMENT 2027-2029

## Including Multiannual planning, Work programme 2027 and Multiannual staff planning

ANNEX 1

# DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

| Date | Version | Modification | Author |
|---|---|---|---|
| December 2025 | V.01 | MB for consultation | ENISA |
| January 2026 | V.01.1 | MB comments | ENISA |
| January 2026 | V.1 | MB comments and ENISA updates | ENISA |
| January 2026 | V.1.1 | Corrected the establishment plan upon the draft Union budget of 2026 | ENISA |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

# LIST OF ACRONYMS

To be updated during proof reading & editing

| | |
|---|---|
| AAR | Annual Activity Report |
| ABAC | Accruals-based accounting |
| ACER | Agency for the Cooperation of Energy Regulators |
| AD | Administrator |
| AHWG | Ad-Hoc Working Group |
| AST | Assistant |
| BEREC | Body of European Regulators for Electronic Communications |
| CA | Contract agenda |
| CAB | Conformity Assessment Body |
| CDR | Career Development Review |
| Cedefop | European Centre for the Development of Vocational Training |
| CEF | Connecting Europe Facility |
| CEN | European Committee for Standardization |
| CENELEC | European Committee for Electrotechnical Standardization |
| CERT-EU | Cybersecurity Service for the Union institutions, bodies, offices and agencies |
| CISO | Chief information security officer |
| COVID-19 | Coronavirus disease 2019 |
| CNECT | Directorate-General for Communications Networks, Content and Technology |
| CSA | Cybersecurity Act |
| CSIRT | Computer Security Incidence Response Team |
| CTI | Cyber threat intelligence |
| CTF | Capture the Flag |
| CRA | Cyber Resilience Act |
| CSDP | The Common Security and Defence Policy |
| CSoA | Cyber Solidarity Act |
| CSPO | Cybersecurity Policy Observatory |
| EU-CyCLO -Ne | Cyber Crisis Liaison Organisation Network |
| DORA | Digital Operational Resilience Act (DORA) |
| DSP | Digital service providers |
| DSO | European Distribution System Operators |
| EBA | European Banking Authority |
| ECA | European Court of Auditors |
| ECATS | European Competent Authorities for Trust Services |
| EC3 | European Cybercrime Centre |
| ECCC | European Cybersecurity Competence Centre |
| ECSF | European Cybersecurity Skills Framework |
| EUCS | EU Cloud Certification Scheme |
| ED | Executive Director |
| ECCG | European Cybersecurity Certification Group |
| EDA | European Defence Agency |
| EEAS | European External Action Service |
| EECC | European Electronic Communications Code |
| EFTA | European Free Trade Association |
| eID | Electronic identification |
| eIDAS | Electronic Identification and Trust Services (eIDAS) Regulation |
| EIOPA | European Insurance and Occupational Pensions Authority |
| EIT | European Institute of Innovation & Technology |
| EMAS | Eco-Management and Audit Scheme |
| EMSA | European Securities and Markets Authority |
| ENISA | European Union Agency for Cybersecurity |
| ENTSO | European Network of Transmission System Operators for Electricity |
| ERA | European Railway Agency |
| ETSI | European Telecommunications Standards Institute |
| EUCC | European Union Common Criteria scheme |
| EUCI | European Union classified information |
| EU5G | European Union certification scheme for 5G networks |

| | |
|---|---|
| EU-LISA | European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice |
| Europol | European Union Agency for Law Enforcement Cooperation |
| FTE | Full-time equivalent |
| FWC | Framework Contract |
| ICT | Information and communication technology |
| IPR | Intellectual property rights |
| ISAC | Information Sharing and Analysis Centre |
| IT | Information technology |
| JCU | Joint Cyber Unit |
| KDT | Key digital technologies |
| MB | Management Board |
| MFF | Multi-annual financial framework |
| MoU | Memorandum of understanding |
| MT | Management Team |
| NCCA | National Cybersecurity Certification Authority |
| NIS | Networks and Information Systems |
| NISD | NIS Directive |
| NIS2 | NIS2 Directive |
| NIS CG | NIS Cooperation Group |
| NLO | National Liaison Officers |
| OOTS | The Once Only Technical System |
| SC | Secretary |
| SCCG | Stakeholder Cybersecurity Certification Group |
| SLA | Service-level agreement |
| SMEs | Small and medium-sized enterprises |
| SNE | Seconded national expert |
| SOCs | Security Operation Centres |
| SOP | Standard Operating Procedure |
| SPD | Single Programming Document |
| TA | Temporary agent |

# INTRODUCTION

## FOREWORD

To be updated during the course of 2026

## ABOUT THE SINGLE PROGRAMMING DOCUMENT (SPD)

The Single Programming Document (SPD) defines the strategic and operational framework guiding the Agency's work over the coming years. As the central planning and management tool, it aligns the Agency's strategic objectives stemming from the ENISA strategy and activities with the broader priorities of the European Union.

By integrating a multiannual perspective with a detailed annual work program, the SPD ensures that strategic goals are translated into actionable steps, measurable outcomes, and efficient resource allocation. Additionally, it enhances transparency and accountability by providing stakeholders with clear insights into how the Agency intends to fulfil its mandate and deliver the strategic objectives of the ENISA strategy.

**The SPD is structured in three key sections:**

Section I outlines the general context, including the policy environment, key developments, and challenges relevant to the Agency's mission.

Section II details the multiannual programming and resource planning over a three-year period.

Section III presents the annual work program, specifying planned activities, outputs, performance indicators and targets for the upcoming year.

Together, these sections create a cohesive link between ENISA's strategy, annual execution, and resource management, facilitating effective performance monitoring and reporting throughout the programming cycle.

## MISSION STATEMENT

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and Union institutions, bodies, offices and agencies on cybersecurity. It contributes to developing and implementing the Union's cybersecurity policies.

Our aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. We aspire to be an agile, environmentally and socially responsible organisation focused on people.

## ENISA STRATEGY

### Horizontal objectives:

### Strategic objective: "Empowered communities in an involved and engaged cyber ecosystem"

Cybersecurity is a shared responsibility. Europe strives for a cross-sectoral, all-inclusive cooperation framework. ENISA plays a vital role in fostering cooperation among cybersecurity stakeholders (Member States, Union entities, and other communities). ENISA in its efforts emphasises complementarity, engages stakeholders based on expertise and role in the ecosystem, and creates new synergies. The goal is to empower communities to enhance cybersecurity efforts exponentially through strong multipliers across the EU and globally.

### Strategic objective: "Foresight on emerging and future cybersecurity opportunities and challenges"

New technologies, still in their infancy or close to mainstream adoption, create novel cybersecurity opportunities and challenges that would benefit from the use of foresight methods. Strategic foresight is not only about technologies and should include additional dimensions, such as political, economic, societal, legal and environmental aspects, to name a few. Through a structured process enabling dialogue among stakeholders and in coordination with other EU initiatives on research and innovation, foresight would be able to identify the opportunities and support early mitigation strategies for the challenges improving the EU resilience to cybersecurity threats. To fully reach its goal, foresight should be addressed as a transversal principle across all ENISA's strategic objectives.

### Strategic objective: "Consolidated and shared cybersecurity information and knowledge support for Europe"

Efficient and effective, but also consolidated information and knowledge is the foundation of informed decision-making, as well as proactive and reactive protection and resilience by better understanding of the threat landscape. The much-needed common understanding and assessment of EU's cybersecurity maturity relies on information and knowledge. Consolidating and sharing cybersecurity information and knowledge strengthens the culture of cooperation and collaboration between communities and strengthens networks and partnerships.

### Vertical objectives:

### Strategic Objective: "Support for effective and consistent implementation of EU cybersecurity policies"

Cybersecurity is a cornerstone of the digital transformation and it is a requirement in the most critical sectors of the EU's economy and society. It is also considered across a broad range of policy initiatives. To avoid fragmentation and inefficiencies, it is necessary to develop a coherent approach, while taking into account the specificities of the different sectors and policy domains. ENISA's advice, opinions and analyses aim at ensuring consistent, evidence-based and future-proof implementation, focussed on building up cyber resilience in the critical sectors and supporting the EU Member States in tackling new risks for the Union.

### Strategic objective: "Effective Union preparedness and response to cyber incidents, threats, and cyber crises"

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to cyber threats incidents and potential cyber crises. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the Union entities for faster response and proper coordination of efforts at strategic, operational and technical levels. Understanding the ongoing situation is key to be effectively prepared and to be able to respond to cyber incidents, threats, and crises.

### Strategic objective: "Strong cyber security capacity within EU"

The frequency and sophistication of cyberattacks is on a steady rise, while at the same time the use of digital infrastructures and technologies is increasing rapidly. The needs for cybersecurity skills, knowledge and competences exceeds the supply. EU is investing in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional and across all sectors and age groups. ENISA address capacity building across the spectrum: start by investing in youth through competence building and training, whilst providing continuous up- and reskilling opportunities to professionals, to keep up with the fast-changing nature of cybersecurity. The focus is not only on increasing the cybersecurity skillset in the Member States and contributing to the objectives of the Cybersecurity

Skills Academy, but also on making sure that the different operational communities always possess the appropriate capacity to deal with the cyber threat landscape. Engaging closely with key players and multipliers in the EU is crucial to ensure adequate preparedness across sectors and borders, effectively utilising the lessons learned from well-planned exercises.

## Strategic objective: "Building trust in secure digital solutions"

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of assessing the security of Information and Communication Technologies (ICT) products, services and processes and ensuring their trustworthiness, a common European approach between societal, market, research and foresight, economic and cybersecurity needs, with the possibility to influence the international community by introducing a competitive edge. Using means such as cybersecurity-by-design, market surveillance, and certification will allow to both enforce and promote trust in digital solutions.

# SECTION I. GENERAL CONTEXT

[To be overall updated during the course of 2026]

The following aspects have been taken into account in drafting this single programming document as part the general context, having an impact on the programing of the Agency's work for the period of 2027-2029:

1) geopolitical developments, specifically:

- [impact of the Russian war of aggression]

2) cybersecurity threat dynamics and risks, incl:

- [trends as highlighted in 2026 ENISA Threat Landscape]
- [emerging trends regarding vulnerabilities and risks in products and technologies in TIR2026]

3) overall level of cybersecurity in the EU, the maturity and resilience of critical sectors:

- [2026 State of Cybersecurity in the Union Report]

4) Member States needs and challenges:

- [Based of the synthesis of the aggregated outcomes of ENISA's annual dialogues with Member States in 2025 & 2026], the key challenge for the member states are still revolving around ensuring effective and efficient **implementation of the NIS2 Directive**. Beyond areas where ENISA is expected to help MS in setting up common mechanisms and facilitating the identification of best practices (supervision/enforcement or entity identification and classification), direct action is necessary to support **incident reporting** (including by developing further and maintaining relevant taxonomies and templates) [list of limited high value-added actions tbc by MB in March 2026]

5) Legislative developments at the Union level:

- [Following the establishment of the **Single Reporting Platform** and the application of reporting obligations in September 2026] , the CRA will fully apply by end 2027. This will further highlight the expectations on the Agency within the programming period to develop and enhance work to help and assist Member States and the Commission, as well as European market actors to **ensure the cybersecurity of products and technologies**, as well as effectively **manage and coordinate vulnerabilities** at the Union level as well as throughout technology- and product stacks.
- Without prejudice to the final outcome of the legislative negotiations on the Digital Omnibus (as proposed by the Europen Commission in November 2025), ENISA may be expected to implement and maintain an integrated system, which would allow entities under the scope of different legislative acts, to report incidents via a **Single Entry Point**. This would further increase the expectations placed on the Agency to be capable and able to **develop, implement and maintain secure operational digital platforms and infrastructure**, for the benefit of Member States' authorities and entities.
- [Review of the CSA] conclusions made in this SPD are preliminary and those will be further adjusted taking into account the revision of the ENISA mandate (CSA 2)

Full list of statutory tasks in force from EU legislation which the Agency must be in a position to implement and which thus also have an impact in the context of programming of the Agency's resources in order to ensure the relevant minimum capacities and capabilities is presented in annex XV.

# SECTION II. MULTI-ANNUAL PROGRAMMING 2027 – 2029

The Management Board (MB) of ENISA reviewed and updated the Agency's strategy in November 2024, building on the Cybersecurity Act (CSA), and other legislative acts which give substantial tasks to ENISA (such as NIS2, CRA, CSoA). The revised strategy outlines how the Agency will strive to meet the expectation of the cybersecurity ecosystem in a medium to long-term perspective, and as such is now the baseline for the multiannual programming of the Agency's activities in 2027-2029, together with the Corporate Strategy, which was endorsed by the MB in 2023 [as it should be reviewed in 2026, this might bring changes to the below].

The conclusions made in this SPD are preliminary and those will be further adjusted taking into account the revision of the ENISA mandate (CSA 2)

## 1. Multi-annual work programme

ENISA strategy sets seven strategic objectives which the Agency should strive towards. The following table outlines the strategic objectives and maps them with the associated key performance indicators (strategic KPIs), defined by the MB to measure progress in achieving the strategic objectives, supporting continuous assessment and tracking toward the agency's long-term objectives.

| **Strategic objectives** | | *Vertical strategic objectives* | | | |
|---|---|---|---|---|---|
| | | *Effective and consistent EU policies implementation for EU cybersecurity policy* | *Effective Union preparedness and response to cyber incidents, threats, and cyber crises* | *Strong cyber security capacity within EU* | *Building trust in secure digital solutions* |
| *Horizontal strategic objectives* | *Empowered communities in an involved and engaged cyber ecosystem* | 1. Uptake of ENISA recommendations to support Member States (MS) and stakeholders in implementing EU legislation | 2. Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks | 3. Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings) | 4. Number of EU certification schemes developed and maintained, number EU regulations making reference to CSA, number of active Member States' NCCAs /…/ |
| | *Foresight on emerging and future cybersecurity opportunities and challenges* | 5. Number of identified future and emerging areas reflected in the policy initiatives and interventions | 6. Operationalization [and administration] of the EU Cybersecurity Reserve, [and its use] by MS, Union Entities and on a case-by-case basis DEP associated third countries | 7. Number of advise and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC | 8. Rate of satisfaction with ENISA's support to the implementation of the CRA /…/ and European cybersecurity certification framework (ECCG) |
| | *Consolidated and shared cybersecurity information and knowledge support for Europe* | 9. Uptake of recommendations stemming from NIS2 Art. 18 report | 10. EU Vulnerability Database is operationalized by ENISA [and MS are satisfied] /…/ with accurate and timely analyses of incidents, vulnerabilities and threats | 11. Percentage of MS that use ECSF | 12. Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and successfully operated |

In preparation of this multianual programming document, the Agency bearing in mind the context (see section II) and using the guidance of the MB members which was given in November/December 2025 – further clarified the scope of each of the strategic KPIs, to ensure better strategic focus on the deliverables where MS see most added value during 2027-2029, exploit any potential synergies and avoid duplication of activities.

As a result, the Agency defined a limited number of key actions (annual outputs) which it needs to implement over the years 2027-2029 in order to advance towards its strategic objectives. It reviewed the resource estimates of the key actions (annual outputs) and structured them into operational activities in light of the guidance

received by the MB members. The following table enlists all the key actions which are necessary and critical to achieve each of the the strategic KPIs and map those actions as outputs to operational activities – thus serving as baselines for the multi-annual resource estimations and planning of operational activities.

| ***Strategic KPIs** [as refined by MB]* | ***Key actions (annual outputs)*** | ***Activity*** |
|---|---|---|
| 1. Uptake of ENISA recommendations to support Member States ~~and stakeholders~~ in implementing EU legislation (focusing on NIS2) | Assist Member States to map and understand challenges and needs in implementing NIS2 within NCSS | ACTIVITY 1: POLICY MONITORING AND ANALYSIS |
| | Assist MS with horizontal and/or general measures in implementing NIS2 | ACTIVITY 2: RESILIENCE OF CRITICAL SECTORS |
| | Assist MS with sectorial and/or specific measures to implement NIS2 | ACTIVITY 2: RESILIENCE OF CRITICAL SECTORS |
| 2. Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks | Develop and maintain secure IT systems and platforms for operational activities | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Support the functioning of the operational networks | ACTIVITY 4: OPERATIONAL COOPERATION & COORDINATION |
| | Monitor and provide threat analysis & situational awareness to operational and strategic communities | ACTIVITY 5: OPERATIONAL & SITUATIONAL AWARENESS |
| | Support MS in European incident reporting and vulnerability management | ACTIVITY 5: OPERATIONAL & SITUATIONAL AWARENESS |
| | Maintain and enhance ENISA's security posture and implement the Agency's cybersecurity maturity plan | ACTIVITY 11: EFFECTIVE CORPORATE GOVERNANCE |
| 3. Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings) | Community and stakeholder development and support | ACTIVITY 3: CAPACITY BUILDING |
| | Maintaining and evolving relevant toolkits, methodologies and standards for capacity building | ACTIVITY 3: CAPACITY BUILDING |
| | Organizing limited capacity enhancing activities (e.g. exercises and trainings) | ACTIVITY 3: CAPACITY BUILDING |
| 4. Number of EU certification schemes developed, number of certificates issued per year, number of Member States issuing European certificates (focusing on timely delivery of draft schemas) | Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes | ACTIVITY 7: CYBERSECURITY CERTIFICATION |
| | Implementing, fostering and maintaining the established schemes. | ACTIVITY 7: CYBERSECURITY CERTIFICATION |
| 5. Identify and report on future and emerging threat areas ~~reflected in the policy initiatives and interventions~~ | Developing State of Cybersecurity in the Union (Art 18) report and maintaining EU cybersecurity index | ACTIVITY 1: POLICY MONITORING AND ANALYSIS |
| | Monitor and provide threat analysis & situational awareness to operational and strategic communities | ACTIVITY 5: OPERATIONAL & SITUATIONAL AWARENESS |
| | Develop and maintain a regular Technology and Innovation Radar (TIR) | ACTIVITY 8: MARKET, TECHNOLOGY AND PRODUCT SECURITY |
| 6. Operationalization of the EU Cybersecurity Reserve ~~of which administration and operation is to be entrusted fully or partly to ENISA and~~ used by MS, Union Entities and on a case-by-case basis DEP associated third countries | Support MS with incident response & -management services | ACTIVITY 6: OPERATIONAL SUPPORT |
| | Support MS with other related services | ACTIVITY 6: OPERATIONAL SUPPORT |
| | Maintain and enhance ENISA's security posture and implement the Agency's cybersecurity maturity plan | ACTIVITY 11: EFFECTIVE CORPORATE GOVERNANCE |
| 7. Number of advice and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC | Monitoring and analyzing emerging trends regarding cybersecurity risks in products with digital elements, and provide relevant input to Art 18 report | ACTIVITY 8: MARKET, TECHNOLOGY AND PRODUCT SECURITY |
| 8. Rate of satisfaction with ENISA's support for the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG) | Supporting the statutory bodies (ECCG/SCCG) in carrying out their duties with respect to governance roles and tasks | ACTIVITY 7: CYBERSECURITY CERTIFICATION |
| | Support market surveillance authorities and COM in implementing CRA | ACTIVITY 8: MARKET, TECHNOLOGY AND PRODUCT SECURITY |
| 9. Uptake of recommendations stemming from NIS2 Art. 18 report | Assist Member States to map and understand challenges and needs in implementing NIS2 within NCSS | ACTIVITY 1: POLICY MONITORING AND ANALYSIS |
| | Developing State of Cybersecurity in the Union (Art 18) report and maintaining EU cybersecurity index | ACTIVITY 1: POLICY MONITORING AND ANALYSIS |
| | Develop and maintain a regular Technology and Innovation Radar (TIR) | ACTIVITY 8: MARKET, TECHNOLOGY AND PRODUCT SECURITY |
| 10. EU Vulnerability Database is operationalized by ENISA and a satisfaction rate (by MS and stakeholders) with ENISA ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats | Develop and maintain secure IT systems and platforms for operational activities | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Monitor and provide threat analysis & situational awareness to operational and strategic communities | ACTIVITY 5: OPERATIONAL & SITUATIONAL AWARENESS |
| | Support MS in European incident reporting and vulnerability management | ACTIVITY 5: OPERATIONAL & SITUATIONAL AWARENESS |
| 11. Percentage of MS that use ECSF | Maintaining and evolving relevant toolkits, methodologies and standards for capacity building | ACTIVITY 3: CAPACITY BUILDING |
| 12. Reporting platform under CRA is ~~established within 21 months of the entry into force of the Regulation and~~ successfully operated (after its establishment in Q3 2026) | Support MS in European incident reporting and vulnerability management | ACTIVITY 5: OPERATIONAL & SITUATIONAL AWARENESS |
| | Monitoring and analyzing emerging trends regarding cybersecurity risks in products with digital elements, and provide relevant input to Art 18 report | ACTIVITY 8: MARKET, TECHNOLOGY AND PRODUCT SECURITY |
| | Develop and maintain secure IT systems and platforms for operational activities | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Develop and maintain ENISA's core IT infrastructure and capabilities (incl secure data center services) | ACTIVITY 9: SECURE INFRASTRUCTURE |

| | | |
|---|---|---|
| | Maintain and enhance ENISA's security posture and implement the Agency's cybersecurity maturity plan | ACTIVITY 11: EFFECTIVE CORPORATE GOVERNANCE |

[Highlighted text in the table reflects the changes as directed by the guidance received from MB members].

Though the Agency incorporated a number of clarifications of its strategic KPI's – incl to the scope and focus of the key actions and their resourcing approach – following clarifications had a particular impact on the way some operational activities and thus the Agency's work shall be structured.

First, reflecting on the fact that a number of strategic deliverables require the Agency to develop and/or maintain secure operational platforms which have high relevance to the operational community (see strategic KPIs 2, 10 and 12), and without prejudice to the final outcome of the negotiations of the legislators on the potential tasks which the Agency may need to be prepared to further implement under the Digital Omnibus (as proposed by the Europen Commission in November 2025), all the activties which concern the development or maintainence of core, corporate or operational digital platforms and/or infrastructure are structurally consolidated and brought under a single activity (**Activity 9: secure digital and physical infrastructure**). This would allow the Agency to avoid duplication of service functionalities (for example avoid separate IT help-desks for operational and corporate use), would exploit greater synergies in development and mainainance where feasible and relevant (without jeopardising the need to seggregate some functionalities or infrastructure to ensure greater security), ensure greater consistency in application of security measures and would make it possible to build stronger IT and technology development and mainainance capabilities and capacities in the Agency, in anticipation of the already present as well as emerging expectations (please see section I).

Secondly, **Activity 4: operational cooperation and coordination**, which in the 2026-2028 programming period was also responsible for the development and maintainance of operational platforms, would now additionally encompass the support for the functioning of the Agency's horizontal statutory bodies (NLO, AG), implementation of both the Agency's stakeholder's and international cooperation strategies (adopted by the MB in November/December 2025), as well as the Agency's overall outreach (incl. liaison and coordination functions with COM, Council (Member States) and European Parliament) and public communications activities. Again, this would allow the Agency to assist Member States in exploring (where relevant) alignment in operational activities between the Agency's statutory bodies and the bodies where ENISA is a member or a secretariat (NIS CG, CyCLONe and CSIRT network), or towards the HWP when relevant. It can help the Agency to exploit synergies from these bodies and networks incl by (when possible) reducing the number of ENISA driven consultations, feedback surveys or validation requests (each of which might now be run across a number of forums in parallel. This can be achieved by channelling such requests only to a single forum, while informing other forums appropriately, so that different representatives of a single Member State can channel their input and consolidate it via a responsible forum. Consolidation under a single activity can also help to avoid duplication of service functionalities (for example secretariat functions) and thus save and concentrate more resources to increase ENISA's support for the substance of the work of these forums and networks.

## 2. Corporate strategy as baseline for multiannual programming

[As the corporate strategy will be reviewed in 2026 text below might change] ENISA's corporate strategy outlines three dimensions which the Agency needs to tackle in order to address its most critical corporate risks: (a) lack of resources and talent, coupled with challenges in the management of human resources across the Agency; (b) lack of comprehensive implementation of ENISA's IT strategy across the Agency and (c) dependence on external providers (systems, services, people).

The following table outlines specific corporate objectives under the three dimensions – people centric organization, service centric organisation and sustainable organisation - endorsed by the MB to support continuous assessment and tracking towards achieving the corporate strategy of the Agency.

### Corporate objectives:

| Corporate strategy | Corporate strategic dimensions | | |
|---|---|---|---|
| | *PEOPLE CENTRIC ORGANISATION* | *SERVICE CENTRIC ORGANISATION* | *SUSTAINABLE ORGANISATION* |
| *Corporate objectives* | 13. Effective workforce planning and management | 16. Ensure efficient corporate services | 20. Ensure ENISA is climate neutral by 2030 |
| | 14. Efficient talent acquisition, development and retainment | 17. Introduce digital solutions that maximize synergies and collaboration within the Agency | 21. Promote and enhance ecologic sustainability across all the Agency's operations |
| | 15. Caring and inclusive modern organization | 18. Continuous innovation and service excellence | 22. Develop efficient framework for continuous governance to safeguard high level of IT and physical security |
| | - | 19. Developing service propositions with additional external resourcing | - |

Though the objectives within the current corporate strategy (and HR strategy) are established until 2029, the Agency's progress in attaining its objectives and the focus is expected to be assessed and reviewed in 2026. [Thus, some of the baselines underpinning the multiannual programming of the Agency might be further refined and clarified during this process, and thus also the scope of key actions (outputs) stemming from the corporate objectives, as well as the structure of the activities might be further refined during 2026].

The following table enlists the key actions which are necessary and critical to achieve the corporate objectives [as they currently stand] and map those actions as outputs to corporate activities – thus serving as baselines for the multi-annual planning of corporate or operational activities and their resource estimations.

| ***Corporate objectives*** | ***Key actions (annual outputs)*** | ***Activity*** |
|---|---|---|
| 13. Effective workforce planning and management | Support the workforce planning and annual reviews and implement relevant actions (contract renewals, recruitment, restructurings) | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| | Support the Agency's performance and talent management and implement annual CDR and reclassification exercises | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| 14. Efficient talent acquisition, development and retainment | Support the workforce planning and annual reviews and implement relevant actions (contract renewals, recruitment, restructurings) | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| | Support the Agency's performance and talent management and implement annual CDR and reclassification exercises | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| | Develop and maintain HR-related staff services (incl welfare) and help to support high level of psychological safety at work | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| 15. Caring and inclusive modern organization | Develop and maintain HR-related staff services (incl welfare) and help to support high level of psychological safety at work | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| | Develop and maintain secure facilities, conducive and sustainable physical and digital workspaces to support the Agency's operations | ACTIVITY 9: SECURE INFRASTRUCTURE |
| 16. Ensure efficient corporate services<br><br>17. Introduce digital solutions that maximize synergies and collaboration within the Agency | Plan and develop efficient HR, tendering, contract- and financial management services in support the Agency's operations | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| | Develop and maintain secure facilities, conducive and sustainable physical and digital workspaces to support the Agency's operations | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Ensure support for MB/EB and single administration and administrative services across the Agency | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Ensure consistency and synergies across all Agency's IT developments and maximize efficiencies | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Develop and maintain secure IT systems and platforms for corporate activities | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Develop and maintain ENISA's core IT infrastructure and capabilities (incl secure data center services) | ACTIVITY 9: SECURE INFRASTRUCTURE |
| 18. Continuous innovation and service excellence | Support the functioning of the NLO/AG and coordinate Agency's activities across NISCG and HWP | ACTIVITY 4: OPERATIONAL COOPERATION & COORDINATION |
| | Ensure that the Agency's rules and practices are fit for purpose, compliant and all risks are managed | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Ensure consistency and synergies across all Agency's IT developments and maximize efficiencies | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Develop and maintain HR-related staff services (incl welfare) and help to support high level of psychological safety at work | ACTIVITY 10: HUMAN CAPABILITIES, SKILLS AND RESOURCES |
| 19. Developing service propositions with additional external resourcing | Ensure efficient and effective operational programming, resource planning and reporting | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Ensure that the Agency's rules and practices are fit for purpose, compliant and all risks are managed | ACTIVITY 11: CORPORATE GOVERNANCE |
| | … | all activities |

| *Corporate objectives* | *Key actions (annual outputs)* | *Activity* |
|---|---|---|
| 20. Ensure ENISA is climate neutral by 2030 | Ensure that the Agency's rules and practices are fit for purpose, compliant and all risks are managed | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Ensure effective outreach, communications and implementation of the Agency's stakeholder's and international cooperation strategies | ACTIVITY 4: OPERATIONAL COOPERATION & COORDINATION |
| | Develop and maintain secure facilities, conducive and sustainable physical and digital workspaces to support the Agency's operations | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Ensure efficient and effective operational programming, resource planning and reporting | ACTIVITY 11: CORPORATE GOVERNANCE |
| 22. Develop efficient framework for continuous governance to safeguard high level of IT and physical security | Ensure consistency and synergies across all Agency's IT developments and maximize efficiencies | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Maintain and enhance ENISA's security posture and implement the cybersecurity maturity plan | ACTIVITY 11: CORPORATE GOVERNANCE |
| | Develop and maintain secure facilities, conducive and sustainable physical and digital workspaces to support the Agency's operations | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Develop and maintain secure IT systems and platforms for operational activities | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Develop and maintain secure IT systems and platforms for corporate activities | ACTIVITY 9: SECURE INFRASTRUCTURE |
| | Develop and maintain ENISA's core IT infrastructure and capabilities (incl secure data center services) | ACTIVITY 9: SECURE INFRASTRUCTURE |

## 3. Summary

Overall the Agency, with the help and guidance of MB members, has thus further clarified its focus and priorities within the two strategic frameworks that drive its work programming – ENISA strategy and its corporate strategy.

Though the number of activities remains the same as in the previous programing period (in total 11), **the Agency has reduced 25% the number of outputs (key actions)** from 44 (SPD 2026-2028) to 33 (SPD 2027-2029). This will allow the Agency to consolidate its efforts on priorities, exploit and foster synergies, and focus its actions where they matter most and bring more added value.

The table below summarises the activities and the outputs (key actions), which structure the work for the programming period 2027-2029:

| *Activity* | *Key actions (annual outputs)* |
|---|---|
| 1 | 1.1: Assist Member States to map and understand challenges and needs in implementing NIS2 within NCSS |
| | 1.2: Developing State of Cybersecurity in the Union (Art 18) report and maintaining EU cybersecurity index |
| 2 | 2.1: Assist MS with horizontal and/or general measures in implementing NIS2 |
| | 2.2: Assist MS with sectorial and/or specific measures to implement NIS2 |
| 3 | 3.1: Maintaining and evolving relevant toolkits, methodologies and standards for capacity building |
| | 3.2: Organizing targeted capacity enhancing activities (e.g. exercises and trainings) |
| | 3.3: Community and stakeholder development and support |
| 4 | 4.1: Support the functioning of the operational networks (CSIRT network, CyCLONe) |
| | 4.2: Support the functioning of the NLO/AG and coordinate Agency's activities across NISCG and HWP |
| | 4.3: Ensure effective outreach, communications and implementation of the Agency's stakeholder's and international cooperation strategies |
| 5 | 5.1: Monitor and provide threat analysis & situational awareness to operational and strategic communities |
| | 5.2: Support MS in European incident reporting and vulnerability management |
| 6 | 6.1: Support MS with incident response & -management services |
| | 6.2: Support MS with other related services |
| 7 | 7.1: Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes |
| | 7.2: Implementing and maintaining the established schemes |
| | 7.3: Supporting the Union's certification forums (ECCG/SCCG) |
| 8 | 8.1: Develop and maintain a regular Technology and Innovation Radar (TIR) |
| | 8.2: Monitor and analyze emerging trends regarding cybersecurity risks in products with digital elements, and give input to Art 18 report |
| | 8.3: Support MS market surveillance authorities and COM in implementing CRA |
| 9 | 9.1: Develop and maintain ENISA's core IT infrastructure and capabilities (incl secure data center services) |
| | 9.2: Develop and maintain secure IT systems and platforms for operational activities |
| | 9.3: Develop and maintain secure IT systems and platforms for corporate activities |
| | 9.4: Develop and maintain secure facilities, conducive and sustainable physical and digital workspaces to support the Agency's operations |
| 10 | 10.1: Support the workforce planning and annual reviews and implement relevant actions (contract renewals, recruitment, restructurings) |
| | 10.2: Support the Agency's performance and talent management and implement annual CDR and reclassification exercises |
| | 10.3: Develop and maintain HR-related staff services (incl welfare) and help to support high level of psychological safety at work |
| | 10.4: Plan and develop efficient HR, tendering, contract- and financial management services in support the Agency's operations |

| | |
|---|---|
| 11 | 11.1: Ensure efficient and effective operational programming, resource planning and reporting |
| | 11.2: Ensure that the Agency's rules and practices are fit for purpose, compliant and all risks are managed |
| | 11.3: Maintain and enhance ENISA's security posture and implement the cybersecurity maturity plan |
| | 11.4: Ensure consistency and synergies across all Agency's IT developments and maximize efficiencies |
| | 11.5: Ensure support for MB/EB and single administration and administrative services across the Agency |

# HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2027-2029

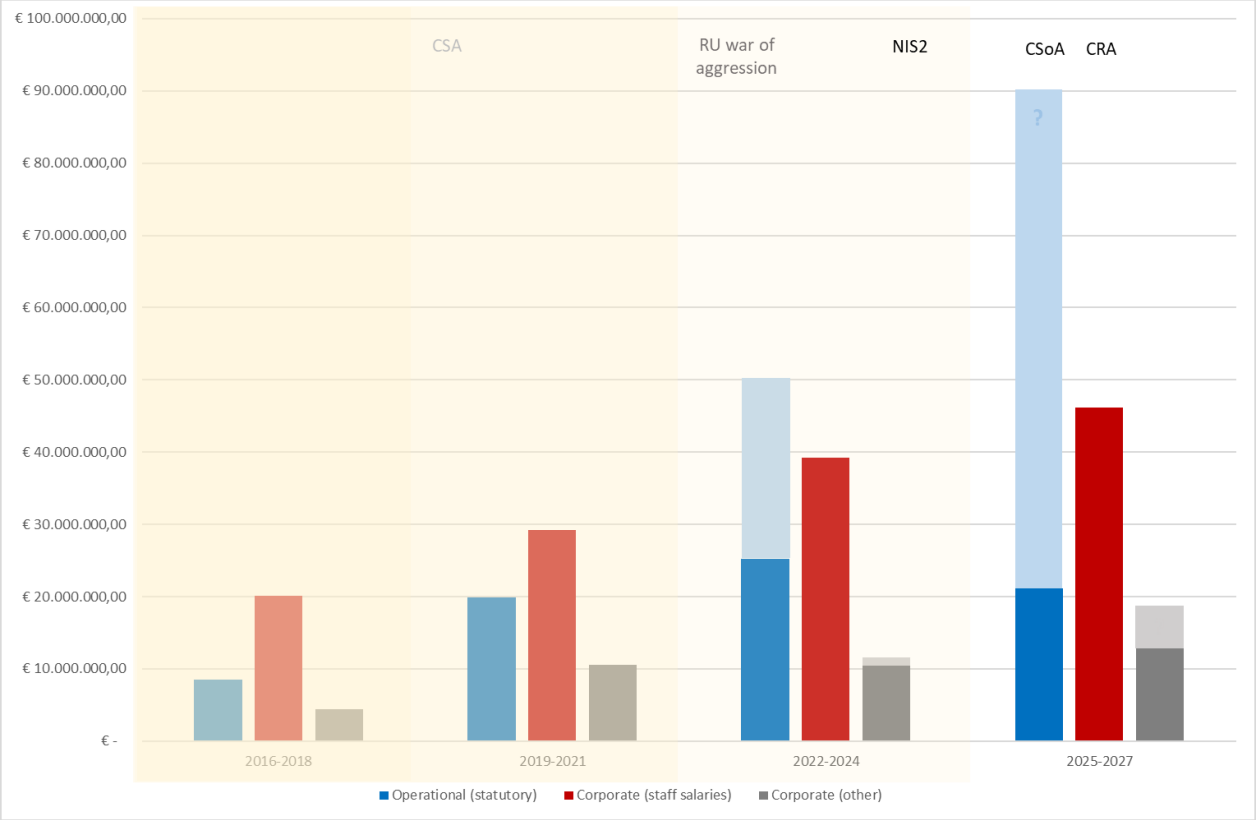
## 2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

Over the past programming periods, ENISA struggled to match the needs and expectations with the structural resources of its statutory budget. Though there were increases in the Union's subsidy – related to the adoption of CSA first and then NIS2 and CRA – those increases only partially covered the needs stemming from the new tasks placed on ENISA.

Recognizing this, the European Commission (Commission or COM) established several contribution agreements with the Agency, to address specific needs and/or support the financing of programs congruent with the mandate of ENISA. The first direct additional support (15MEUR), which was given by the Commission to the Agency's annual budget in 2022, was set up to develop services for the support of Member States in response to the Russian war of aggression. This was followed up by a multiannual contribution agreement in 2023 (20MEUR) to continue services until end 2025.

Henceforward, the Commission signed a series of multiannual contribution agreements with ENISA, to support its operational mandate and tasks across number of areas. In 2024 the Agency signed a series of contribution agreements with COM to support the development of the CRA single reporting platform - SRP (in total 12.4MEUR). This was extended in 2025 (additional 8MEUR) to support the implementation of the platform. In the same year COM and ENISA also agreed on a contribution agreements to implement: (a) the Cyber Reserve (36MEUR), foreseen in the Cyber Solidarity Act (CSoA); [(b) the action plan on the cybersecurity of hospitals and healthcare providers (6MEUR); (c) support for the development of national digital wallet schemas (1.7MEUR) and (d) a dedicated program to assist Western-Balkans (4MEUR)]. Further details of the contribution agreements can be found in annex XI.

As a result, both the emphasis in the Agency's budget as well as the structure of the Agency's financial resource planning has changed considerably. The graph below shows the summarized annual budgets of the Agency during four 3-year periods: 2016-2018 (before CSA came into force), 2019-2021 (after CSA was enacted), 2022-2024 (start of RU war of aggression, NIS2 came into force), and the current 3-year period 2025-2027 (CSoA, CRA).




Following observations are of note. First, the Agency's overall operational financing has roughly doubled in every 3-year period. However, when during the 2019-2021 the surge was due to increase in statutory resourcing (new CSA resources) and internal reprioritisation, then during the last two 3-year periods, the increase has been possible only because it is financed via additional external contributions as noted above (please see the light shaded parts of the column in the graph), budgeted in ENISA's annual expenditure under Title IV. In fact, in terms of its statutory operational expenditure (Title III – dark-blue column in the graph), the Agency has not been able to maintain it at proportionate level achieved after CSA came into force, and share from overall budget has steadily decreased and during the current 3-year period is actually lower also in real terms compared to last period.

Second, the growth in statutory staff expenditure (Title I – red column) has been slowing every period, congruent with when and how the Agency has been availed additional staff posts. Highest jump can be observed in 2019-2021 (almost 30% increase) when the CSA came into force. The next period (2022-2024) the increase was slower (around 25%) with more modest number of additional staff posts stemming from NIS2. In the current period the increase compared to the last is around 15% with two additional posts availed via CRA. Across the years the other major driver of increase of staff expenditure has been inflation and indexation, with Greek economy growing strongly after the crises. Naturally, this has put further strain on other statutory expenditure (both operational and corporate).

Finally, the financing of the Agency's statutory corporate expenditure (Title I – grey-coloured column), which was increased after CSA enactment (period 2019-2021), has more or less remained the same and any increase during this period is only possible due to the fact that the Agency retains 7% from all contribution agreements to finance indirect costs, related to maintaining functions sustaining the operational delivery of those programs. Thus, the external resourcing, is crucial not only in sustaining the Agency's operations but also its corporate capabilities, including critical efforts to develop its cybersecurity maturity which underpins capacity to deliver its operational tasks.

[In terms of staffing dynamics pending outcome of internal workforce review…]

## 2.2. OUTLOOK FOR THE YEARS 2027-2029

The agency's work is expected to be significantly influenced by legislative developments as outlined in Section I, notably supporting the ongoing implementation efforts of NIS2 as well as gradually rolling out ENISA tasks in CRA: related developments in vulnerability management at the EU level and support for the European economic entities and stakeholders in instilling cybersecurity throughout the development, lifecycle and management of products with digital elements. All necessary to raise the common level of cybersecurity in the Union through specific actions that strengthen resilience throughout the ecosystem, in anticipation to threats and risks as described in Section I. Beyond those needs, the targeting of resources will be influenced by the Agency's efforts to raise its organisational capabilities and capacities.

[placeholder – COM omnibus proposal] The Digital Omnibus proposed in November 2025 aims to simplify EU digital regulations for data, cybersecurity, and AI, including the NIS2 directive. It proposes that ENISA develops and maintains a single-entry point for incident reporting. As the Agency might be asked to implement parts of the proposal, it must take relevant actions and resource the development of capabilities to be in a position to do so. Beyond the CRA SRP, the Digital Omnibus proposal is the other main driver to consolidate ENISA's IT capabilities, resources and budget into a single activity (Activity 9), and increase budget and capacity around IT and cybersecurity governance (parts of Activity 11 – please also see below). As shown below, the major current risk is that a lot of these capabilities depend on external resourcing which is currently foreseen to end in 2028. [ENISA resource needs for Digital Omnibus]

Based on the proposal from COM on the Digital Omnibus and without prejudice to the decision of the legislators, the Staff Working Document accompanying the Digital Omnibus proposal estimated the initial costs for developing the single-entry point with EUR 6 million, while maintaining the single-entry point would require 8 FTEs within ENISA. The cost of onboarding each additional legal act into the single-entry point is estimated at EUR 500,000. The one-off investment will be used to support the implementation and deployment of the solution including integration in client environment. The maintenance and support including a helpdesk would be needed once application is live, including infrastructure/network needs plus application engineers for maintenance (bugs and security fixes) of the applications. Security operations and analysis will be needed for the systems

[placeholder – COM CSA review proposal] Additionally, the revision of the Cybersecurity Act is set to potentially expand the agency's mandate, potentially broadening its responsibilities and resourcing. Although it could impact on all operational activities, without prejudice to its adoption, the Agency would need to prepare to absorb and implement any potential restructuring of its tasks as well as onboarding potential new resources. This will put a strain on the resourcing of Activities 10 and 11, especially in 2027-2028. [ENISA resource needs for CSA review]

Moreover, as noted above, during the next three years the Agency will focus on two critical corporate initiatives—cybersecurity maturity plan and the developing and maintaining its data centre — both of which are essential for meeting regulatory obligations and improving corporate and operational resilience. The cybersecurity maturity plan will drive a multi-year effort to strengthen cybersecurity across all ENISA systems, ensuring compliance with evolving frameworks such as Regulation (EU) 2023/2841 and supporting platforms like the CRA SRP, EU Vulnerability Database, and potentially tasks stemming from Digital Omnibus proposal and the CSA revision. These projects will require coordinated resources from both operational and corporate activities, with a strong emphasis on continuous monitoring, compliance, and reassessment.

Simultaneously, building up its data centre presents a strategic opportunity to enhance IT infrastructure resilience while reducing maintenance costs. By aligning this with cybersecurity improvements, the Agency can streamline efforts, minimize disruptions, and ensure a seamless transition. These projects will demand careful resource allocation, risk management, and governance to maintain momentum while delivering long-term efficiency and cybersecurity benefits.

Again, as noted above, both multiannual efforts again depend to a large extent on external resourcing which is not foreseen to last in most cases beyond and after the end of 2028.

## 2.3 RESOURCE PROGRAMMING FOR THE YEARS 2027-2029

### 2.3.1. Financial resources

Below, the current multiannual financial resourcing plans for the Agency's activities are brought out. These do not take into account the direct resource needs stemming from Digital Omnibus or CSA review. Note should be taken that though 2027 budget is balanced, the resource needs for 2028 and 2029 are greater than the forecasted budget available to the Agency and will need to be reviewed in light of the CSA 2.0 proposal. This is due to the fact that the needs of the Agency (as they are currently defined) demand more from ENISA during those two years, even with the Agency's streamlined focus on only those key actions which are necessary to deliver the slimmed-down ENISA strategic objectives. Moreover, as shown in section 2.1. above, the statutory operational resources are foreseen to decline, putting a further strain on the statutory resourcing of activities which will need to be further scaled down. Also, as noted above, the current contribution agreements are phased out by the end of 2028 which means from 2029 onwards the Agency will face a significant funding gap.

**Table**: *Financial resource planning of the Agency's activities 2027-2029 (with statutory or external resourcing)*

| ACTIVITY | 2027 | | 2028 | | 2029[1] | |
|---|---|---|---|---|---|---|
| | Stat. | Ext. | Stat. | Ext. | | |
| 1 | 300.000 | 0 | 333.000 | 0 | 218.000 | |
| 2 | 550.000 | 112.500 | 550.000 | 177.500 | 510.000 | |
| 3 | 612.000 | 367.000 | 705.000 | 367.000 | 730.000 | |
| 4 | 1.291.400 | 701.000 | 1.404.470 | 583.300 | 1.610.444 | |
| 5 | 1.340.000 | 1.183.000 | 1.555.000 | 1.083.000 | 2.060.000 | |
| 6 | 0 | 10.000.000 | 0 | 10.000.000 | 0 | |
| 7 | 540.000 | 800.000 | 680.000 | 800.000 | 760.000 | |
| 8 | 458.000 | 0 | 520.000 | 0 | 620.000 | |
| 9 | 5.808.794 | 4.270.000 | 6.384.484 | 4.910.000 | 6.907.458 | |
| 10 | 1.410.697 | 314.848 | 1.481.232 | 330.848 | 1.555.293 | |
| 11 | 383.315 | 1.210.000 | 402.481 | 1.238.000 | 312.355 | |
| Salaries | 15.022.286 | 2.833.632 | 15.773.400 | 2.977.632 | 16.562.070 | |
| **Total** (-salaries) | 12.694.206 | 18.958.348 | 14.015.667 | 19.489.648 | 15.283.550 | |
| **TOTAL** (+salaries) | 27.716.492 | 21.791.980 | 29.789.067 | 22.467.280 | 31.845.620 | |

**Table**: *Consolidated financial resource planning of the Agency's activities 2027-2029*

| *ACTIVITY* | 2027 | 2028 | 2029[2] |
|---|---|---|---|
| 1 | 300.000 | 333.000 | |
| 2 | 662.500 | 727.500 | |
| 3 | 979.000 | 1.072.000 | |
| 4 | 1.992.400 | 1.987.770 | |
| 5 | 2.523.000 | 2.638.000 | |
| 6 | 10.000.000 | 10.000.000 | |
| 7 | 1.340.000 | 1.480.000 | |
| 8 | 458.000 | 520.000 | |
| 9 | 10.078.794 | 11.294.484 | |
| 10 | 1.725.545 | 1.812.080 | |
| 11 | 1.593.315 | 1.640.481 | |

[1] Figures to be updated and aligned with CSA 2.0 proposal
[2] Figures to be updated and aligned with CSA 2.0 proposal

| | | | |
|---|---|---|---|
| salaries | 17.855.918 | 18.751.032 | |
| **Total** (-salaries) | 31.652.554 | 33.505.315 | |
| **TOTAL** (+salaries) | **49.508.472** | **52.256.347** | |
| | | | |

### 2.3.2. Human resources

The Agency's statutory staffing posts are foreseen to remain stable [before the adoption of the CSA review as proposed by the Commission]. Thus any new needs which might arise from the Agency's tasks or obligations [incl from Digital Omnibus] will necessitate further resourcing (see last section).

The table below outlines the indicative allocation of FTE's per activity [to be reviewed]

| ACTIVITY | 2027 | | 2028 | | 2029[3] | |
|---|---|---|---|---|---|---|
| | Stat. | Ext. | Stat. | Ext. | | |
| 1 | 8,50 | 0,00 | 9,00 | 0,00 | 9,00 | |
| 2 | 10,00 | 3,00 | 10,00 | 3,00 | 10,00 | |
| 3 | 11,00 | 1,00 | 12,00 | 1,00 | 12,00 | |
| 4 | 13,00 | 6,00 | 15,00 | 6,00 | 16,00 | |
| 5 | 22,00 | 8,00 | 23,00 | 8,00 | 29,00 | |
| 6 | 4,00 | 9,00 | 4,00 | 9,00 | 4,00 | |
| 7 | 10,00 | 2,00 | 11,00 | 2,00 | 12,00 | |
| 8 | 8,00 | 0,00 | 8,00 | 0,00 | 8,00 | |
| 9 | 18,00 | 10,00 | 18,00 | 10,00 | 18,00 | |
| 10 | 13,50 | 2,00 | 13,50 | 2,00 | 13,50 | |
| 11 | 12,00 | - | 12,00 | - | 10,00 | |
| **Total** | **130,00** | **41,00** | **135,50** | **41,00** | **141,50** | |

[3] Figures to be updated and aligned with CSA 2.0 proposal

## 2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

ENISA Commitment to Efficiency (2027–2029)

Within its resource constraints, ENISA remains dedicated to improving operational and corporate efficiency while advancing its strategic and corporate objectives. Over 2027–2029, the Agency will rigorously pursue the following priorities:

- Strengthening talent and operational capacity as outlined in its Corporate and HR strategies.
- Optimizing administrative tasks through reprioritization, externalization, and shared services.
- Leveraging synergies (internal and external) to gain and efficiently use resources, including external partnerships.
- Maximizing budgetary resources using the multi-annual work programme and utilizing joint corporate services with other Agencies

Operational Alignment & Partnerships - ENISA will develop and review its work programme to ensure internal alignment and synergies.

Key actions include:

- Building partnerships with Member States (including by exploring short- and medium-term secondments and exchanges of staff with relevant national authorities).
- Strengthening collaboration with EU institutions by aligning objectives and KPIs in work programme.
- Engaging statutory and ad hoc expert groups (e.g., NLO Network, SCCG, NISD Cooperation Group) to avoid duplication, validate outputs, and ensure compliance with CSA Article 3(3).
- Sustainability & Digitalization - ENISA will assess existing processes, explore alternative support models, and optimize operational efficiency without compromising unit activities. Digitalization, self-service functionalities, and process reengineering will drive agility and cost-effectiveness. Joint corporate services, such as the (C)ISO Support Service pilot with CERT-EU, exemplify efficiency gains.
- IT - Synergies to enhance operational readiness, ENISA will streamline operational platforms to reduce redundancy and improve interoperability.

# SECTION III. WORK PROGRAMME 2027

This is the main body of the Work Programme describing what the agency aims to deliver in the respective year towards achieving its strategic objectives stemming from the ENISA strategy and to fulfil its mandate. In total eleven activities have been identified to support the implementation of ENISA's mandate in 2027.

The activities of the work programme seek to mirror and align with the tasks set out in chapter two of the CSA, demonstrating concretely not only the specific objectives, results and outputs expected for each task but also the resources assigned.

The 2027 work programme priorities will be developed during the course of 2026.

## 3.1 ACTIVITIES

### ACTIVITY 1 POLICY MONITORING AND ANALYSIS

**WHAT WE DO?**

In ENISA strategy, NIS2 implementation is stated as one of the priorities of MB, together with CRA implementation (addressed under Activity 8), and has set to measure the uptake of actions ENISA would take in 2026-2028 to support NIS2 implementation. Under the umbrella of supporting MS to assess and implement their national cybersecurity strategies (Art 7 of NIS2) and technical advice on policy, ENISA will run annual dialogues with all MS (using the NLO network and under the coordination of NLO chair) to map any gaps, challenges and needs in NIS2 implementation, using NISCG implementation matrix (9 areas) as basis. On the basis of the outcome of the dialogues, MB shall select limited number of specific actions where ENISA can add high-value and be impactful within its SPD, to supports MS and critical sectors.

ENISA's overall goal is to achieve a high common level of cybersecurity across Europe. Hence, all actions carried out by ENISA aim at increasing the uptake of relevant recommendations to increase the cybersecurity posture of the EU. The NIS2 Article 18 report assesses the state of cybersecurity in the EU and gives recommendations to increase this level. The report and crucially the uptake of the recommendations in the report therefore contribute directly to increasing the overall cybersecurity posture of the EU.

### ACTIVITY 1 KEY OUTPUTs

| DESCRIPTION | Strategic KPIs | Validation | Measurement of output | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 1.1 Assist Member States to map, understand and address gaps, challenges and needs in implementing NIS2 | Uptake of ENISA recommendations to support Member States ~~and stakeholders~~ in implementing EU legislation (focusing on NIS2) | NLOs | Percentage of MS covered with annual dialogues | Annual | 100% |
| | Uptake of recommendations stemming from NIS2 Art. 18 report | NLOs | Case study(ies) demonstrating the nature and scale of change in policy/practice stemming from at least 2 recommendations as a follow up of the Union Act18 report | Bi-Annual | 1 policy recommendation covered by a case study |

| | | | | | |
|---|---|---|---|---|---|
| 1.2 Developing State of Cybersecurity in the Union report (Art 18), and maintaining EU cybersecurity index | Identify and report on future and emerging threat areas ~~reflected in the policy initiatives and interventions~~ | COM, NIS CG and CNW (endorsement of EUCSI for Art18 report), NLO subgroup (validation of EU CSI) | 3 top areas identified in TIR have been incorporated into relevant ENISA reports (incl. Art. 18 report), and assessed in relation to the scope of these reports | Bi -Annual | 3 top areas |
| | | COM, NIS CG (endorsement for Art18 report) | At least one area has been covered by a relevant policy recommendation.<br>(when relevant, issuing recommendations in the NIS2 Art 18 report related to the 3 top areas identified in TIR in consultation with COM/NISCG) | Bi - Annual | 1 area covered by policy recommendation |
| | Uptake of recommendations stemming from NIS2 Art. 18 report | NIS CG | Case study(ies) demonstrating the nature and scale of change in policy/practice stemming from at least 2 recommendations | Bi -Annual | 1 policy recommendation covered by a case study |

| ACTIVITY 1 RESOURCE FORECASTS | | |
|---|---|---|
| Key action | Budget | FTEs |
| 1.1: Assist Member States to map, understand and address gaps, challenges and needs in implementing NIS2 | 100.000 | 3 |
| 1.2: Developing State of Cybersecurity in the Union report (Art 18), and maintaining EU cybersecurity index | 200.000 | 5,5 |
| **TOTAL** | **300.000** | **8,5** |

## ACTIVITY 2 RESILIENCE OF CRITICAL SECTORS

**WHAT WE DO?**

In ENISA strategy, NIS2 implementation is stated as one of the priorities of MB, (together with CRA implementation), and has set to measure the uptake of actions ENISA would take in 2026-2028 to support NIS2 implementation. Activity 2 shall support the MSs in implementing NIS2 by monitoring and providing risk assessments to strategic and operational communities, supporting critical sectors with lower maturity, supporting implementing sector specific policy files and measuring maturity through NIS investments and NIS 360 studies. ENISA is participating in all the NIS Cooperation Group workstreams providing technical advise and acting as a coordinator of activities.

## ACTIVITY 2 KEY OUTPUTS

| DESCRIPTION | Strategic KPIs | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 2.1: Assist MS with horizontal and/or general measures in implementing NIS2 | Uptake of ENISA recommendations to support Member States ~~and stakeholders~~ in implementing EU legislation (focusing on NIS2) | Input needed by activity | Uptake of ENISA recommendations/actions by MS<br>[specific results from NIS Investments] Increase investments on cyber sec; skills demand is lowering or balancing out; security measures are followed (i.e. patching) | Annual | Input needed by activity |
| 2.2: Assist MS with sectorial and/or specific measures to implement NIS2 | | Input needed by activity | Sectors moving out of the risk zone by 2030 based on NIS360 | Annual | Input needed by activity |

## ACTIVITY 2 RESOURCE FORECASTS

| Key action | Budget | FTEs |
|---|---|---|
| 2.1: Assist MS with horizontal and/or general measures in implementing NIS2 | 150.000 | 4 (+1 FTEs contribution agreements)[4] |
| 2.2: Assist MS with sectorial and/or specific measures to implement NIS2 | 400.000 + 112.500 contribution agreements[5] | 6 (+2 FTEs contribution agreements) [6] |
| TOTAL | 550.000 +112.000 | 10 + 3 |

[4] Support Cyber Situation and Analysis Centre
[5] Support action plan on the cybersecurity of hospitals and healthcare providers
[6] Support action plan on the cybersecurity of hospitals and healthcare providers

# ACTIVITY 3 CAPACITY BUILDING

**WHAT WE DO?**

ENISA will enhance the cybersecurity skills and capabilities in the EU by (1) empowering communities to execute their own capacity building programs using ENISA's relevant tools and methodologies, (b) organizing specific and limited number of capacity enhancing activities (e.g. Blueprint, ) to critical operational communities, and finally (c) helping users of ENISA tools/standards/methodologies to ensure impact, track progress and monitor results. Community empowerment through maintaining and evolving relevant toolkits, methodologies and standards" (for example: ECSF framework, AR-in-a-Box, ENISA exercises methodology, ENISA exercises blue-room solution, Challenges, etc.

To promote the adoption of ECSF in Member States, training organisations and academia, ENISA will maintain and regularly review the ECSF in line with the CyberSkills Academy Communication. Including the support the adoption and uptake of EU's Cybersecurity Skills Framework.

# ACTIVITY 3 KEY OUTPUTS

| DESCRIPTION | Strategic KPIs | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 3.1: Maintaining and evolving relevant toolkits, methodologies and standards for capacity building | Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings) | Input needed by activity | Number of MS using ENISA toolkits, methodologies and frameworks | Annual | Input needed by activity |
| | | Input needed by activity | Number of targeted stakeholders, including EUIBAS, using ENISA toolkits, methodologies and frameworks | Annual | Input needed by activity |
| | | Input needed by activity | Satisfaction of entities/communities using ENISA tools/standards/methodologies | Biennial | Input needed by activity |
| | Percentage of MS that use ECSF | Input needed by activity | Percentage of MS that use ECSF | Annual | more than 75% of MS use the ECSF |
| | | Input needed by activity | Number of actions from ENISA to promote the ECSF withing the relevant stakeholders group (i.e. industry) | Annual | Input needed by activity |
| 3.2: Organizing targeted capacity enhancing activities (e.g. exercises and trainings) | Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings) | Input needed by activity | Number of people impacted directly and/or indirectly by ENISA's capacity | Annual | Input needed by activity |
| | | Input needed by activity | satisfaction of entities/communities participating in the capacity building activities organized by ENISA | Annual | Input needed by activity |
| 3.3: Community and stakeholder development and support | Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings) | Input needed by activity | Number of participants in ENISA's events communities multiplying the sharing of frameworks, good practices and lessons learnt | Annual | Input needed by activity |
| | | Input needed by activity | Engagement rate, the percentage of active | Annual | Input needed by activity |

| | | | | | |
|---|---|---|---|---|---|
| | | | members who are contributing | | |

| ACTIVITY 3 RESOURCE FORECASTS | | |
|---|---|---|
| Key action | Budget | FTEs |
| 3.1: Maintaining and evolving relevant toolkits, methodologies and standards for capacity building | 180.000 | 4 |
| 3.2: Organizing targeted capacity enhancing activities (e.g. exercises and trainings) | 332.000 + 367.000 contribution agreements[7] | 5,5 + 1 contribution agreement[8] |
| 3.3: Community and stakeholder development and support | 100.000 | 1,5 |
| **TOTAL** | **612.000 + 367.000** | **11 + 1** |

[7] Support action plan on the cybersecurity of hospitals and healthcare providers
[8] Support action plan on the cybersecurity of hospitals and healthcare providers

# ACTIVITY 4 OPERATIONAL COOPERATION & COORDINATION

**WHAT WE DO?**

Activity 4 supports the operational networks (CSIRTs Network, EU CyCLONe) through assisting in the functioning of the the operational networks and broader implementation of the Agency's stakeholder strategy. ENISA through Activity 4 will support the funcing of the NLO and AG, including the coordination of the Agency's activities with the NIS Cooperation Group and the Horizontal level Working Party. In addition the Agency's communication and outreach actions will be coordinated within activity 4, including the stakeholder strategy and international strategy including other programs such as the Cyber partnership program.

## ACTIVITY 4 KEY OUTPUTS

| DESCRIPTION | Strategic KPIs / Corporate Objectives | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 4.1: Support the functioning of the operational networks (CSIRT network, CyCLONe) | Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks | Input needed by activity | Satisfaction with ENISA support for the functioning of CNW and CyCLONe | Annual | Input needed by activity |
| 4.2: Support the functioning of the NLO/AG and coordinate Agency's activities across NIS Cooperation Group and Horizontal Working Party | Continuous innovation and service excellence | Statutory bodies, Management Team and Committees | Number of feedback instantiations received per consultation | Annual | >6 |
| 4.3: Ensure effective outreach, communications and implementation of the Agency's stakeholder's and international cooperation strategies | Ensure effective outreach, communications and implementation of the Agency's stakeholder's and international cooperation strategies | MT | Stakeholder satisfaction with ENISA outreach<br>Number of total ENISA website visits<br>Stakeholder satisfaction with knowledge management and stakeholder management system.<br>Internal satisfaction with international coordination | Annual | >80%<br>1.5 million<br>>70%<br>>70% |

## ACTIVITY 4 RESOURCE FORECASTS

| Key action | Budget | FTEs |
|---|---|---|
| 4.1: Support the functioning of the operational networks (CSIRT network, CyCLONe) | 230.000 | 7 |
| 4.2: Support the functioning of the NLO/AG and coordinate Agency's activities across NISCG and HWP | 185.000 | 3 |
| 4.3: Ensure effective outreach, communications and implementation of the Agency's stakeholder's and international cooperation strategies | 876.400+ 701.000 contribution agreement[9] | 2 + 6 contribution agreements[10] |

[9] Pending contribution agreement for the support of the Western Balkans
[10] Pending contribution agreement for the support of the Western Balkans

| | | |
|---|---|---|
| **TOTAL** | **1.291.400 + 701.000** | **12 + 6** |

## ACTIVITY 5 OPERATIONAL & SITUATIONAL AWARENESS

**WHAT WE DO?**

ENISA will ensure the continuous functionality and durability (incl cybersecurity) of infrastructure and tools, which support operational cybersecurity networks (CSIRTs Network & EU-CyCLONe). Activity 5 will add value to the operational networks (CNW, CyCLONe, HWP) through synthesizing and curating various information sources into common situational awareness and supporting vulnerability management at the European level. Specifically,Activity 5 will collect, organise and consolidate information on threats, vulnerabilities and incidents and build a common situational awareness between Member States based on shared accurate data and underpinned by validated joint analysis. Activity 5 will ensure that the tasks which it needs to fulfill to support the operationalization of the single reporting platform (SRP) as defined in the CRA are supported and that it has both the capacities as well as capabilities to do so.

## ACTIVITY 5 KEY OUTPUTS

| DESCRIPTION | Strategic KPIs | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 5.1: Monitor and provide threat analysis & situational awareness to operational and strategic communities | Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks | Input needed by activity | Added value for operational networks and communities – CNW/CyCLONe/HWP | Annual | Input needed by activity |
| | Identify and report on future and emerging threat areas ~~reflected in the policy initiatives and interventions~~ | Input needed by activity | 3 top areas identified in TIR have been incorporated into relevant ENISA reports (incl. Threat Landscapes), and assessed in relation to the scope of these reports | Annual | Input needed by activity |
| | EU Vulnerability Database is operationalized by ENISA and a satisfaction rate (by MS and stakeholders) with ENISA ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats | Input needed by activity | Added value for operational networks and communities - CNW/CyCLONe/HWP | Annual | Input needed by activity |
| 5.2: Support MS in European incident reporting and vulnerability management | Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks | Input needed by activity | Satisfaction with ENISA vulnerability related activities – CNW/CyCLONe | Annual | Input needed by activity |
| | EU Vulnerability Database is operationalized by ENISA and a satisfaction rate (by MS and stakeholders) with | Input needed by activity | User satisfaction with ENISA analyses and support on CVD and vulnerability services | Annual | CNW satisfaction > 4 out of 5 |

| | | | | | |
|---|---|---|---|---|---|
| | ENISA ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats | | The integration of MS endpoints with the CRA SRP | | TBD |
| | Reporting platform under CRA is ~~established within 21 months of the entry into force of the Regulation and~~ successfully operated (after its establishment in Q3 2026) | Input needed by activity | Percentage of MS (CNW/CyCLONe) satisfied or highly satisfied with ENISA' support on CVD, incident reporting and vulnerability management related tasks under Art 15, Art 16 and Art 17(1,2&5) | Annual | 75% |

| **ACTIVITY 5 RESOURCE FORECASTS** | | |
|---|---|---|
| Key action | Budget | FTEs |
| 5.1: Monitor and provide threat analysis & situational awareness to operational and strategic communities | 1.240.000 + 783.000 contribution agreements[11] | 17 +3.5 FTEs contribution agreements[12] |
| 5.2: Support MS in European incident reporting and vulnerability management | 100.000 + 400.000 contribution agreements)[13] | 5 +4.5 FTEs contribution agreements[14] |
| **TOTAL** | **1.340.000 + 1.118.000** | **23 + 8** |

[11] Support action plan on the cybersecurity of hospitals and healthcare providers and Cyber Situation and Analysis Centre

[12] Support action plan on the cybersecurity of hospitals and healthcare providers and Cyber Situation and Analysis Centre

[13] Incident and Vulnerability Response Support and Reporting
[14] Incident and Vulnerability Response Support and Reporting

## ACTIVITY 6 OPERATIONAL SUPPORT

**WHAT WE DO?**

To reinforce MSs' capabilities to respond to large-scale cybersecurity incidents or crises, ENISA through Activity 6 will ensure the deployment of the European Cyber Reserve foreseen under the Cyber Solidarity Act (CSoA) in a manner which adds value to the end users. Activity 6 will support ex-post services, namely incident response and incident management services of selected entities within EU MS, EUIBAs, DEP associated 3rd countries. Activity 6 will also support ex ante services for EU MS from unused cyber reserve funds.

## ACTIVITY 6 KEY OUTPUTS

| DESCRIPTION | Strategic KPIs | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 6.1: Support MS with incident response & -management services | Operationalization of the EU Cybersecurity Reserve ~~of which administration and operation is to be entrusted fully or partly to ENISA and~~ used by MS, Union Entities and on a case-by-case basis DEP associated third countries | MSs, CERT-EU and DEP-associated third countries (if and where applicable) | All MS and other eligible beneficiaries of the Cybersecurity Reserve are supported by Trusted Service Providers | Annual | 100% coverage |
| | | MSs, CERT-EU and DEP-associated third countries (if and where applicable) | Increase of 10% annually of services demanded through the IR Retainer | Annual | 10 users of the Reserve make use of the IR retainers |
| | | Beneficiaries | Percentage of services delivered rated as satisfactory or highly satisfactory by the beneficiaries | Biennial | 75% |
| 6.2: Support MS with other related services | | MSs, CERT-EU and DEP-associated third countries (if and where applicable) | All MS and other eligible beneficiaries of the Cybersecurity Reserve are supported by Trusted Service Providers | Annual | 100% coverage |
| | | MSs, CERT-EU and DEP-associated third countries (if and where applicable) | Increase of 10% annually of services demanded through conversion of services | Annual | 70% of unused pre-committed IR person days are used through conversion into ex-ante services |
| | | Beneficiaries | Percentage of services delivered rated as satisfactory or highly satisfactory by the beneficiaries | Biennial | 75% |

### ACTIVITY 6 RESOURCE FORECASTS

| Key action | Budget | FTEs |
|---|---|---|
| 6.1: Support MS with incident response & -management services | 5.000.000 contribution agreement[15] | 2 + 5 contribution agreements[16] |

[15] EU Cybersecurity Reserve
[16] EU Cybersecurity Reserve

| | | |
|---|---|---|
| 6.2: Support MS with other related services | 5.000.000 contribution agreement[17] | 2 +4 contributions agreements[18] |
| TOTAL | 10.000.000 | 4 + 9 |

[17] EU Cybersecurity Reserve
[18] EU Cybersecurity Reserve

# ACTIVITY 7 CYBERSECURITY CERTIFICATION

**WHAT WE DO?**

To increase transparency and trust in ICT products, services and processes, ENISA through Activity 7 will ensure the timely delivery to the ECCG of all the requested draft cybersecurity certification schemes as well as the revisions thereof and maintenance of existing schemes under implementing acts to improve efficiency and effectiveness. To support the development and uptake of the cybersecurity certification schemes, Activity 7 will support and assist the ECCG/SCCG and engage regularly with all relevant stakeholders.

## ACTIVITY 7 KEY OUTPUTS

| DESCRIPTION | Strategic KPIs | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 7.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes | Number of EU certification schemes developed, number of certificates issued per year, number of Member States issuing European certificates (focusing on timely delivery of draft schemas) | Input needed by activity | Percentage of draft candidate schemes and updates submitted with MSs support in due time with regards to the requests received | Annual | Input needed by activity |
| 7.2: Implementing and maintaining the established schemes | | Input needed by activity | Sufficient number of supporting documents to allow schemes' implementation and uptake (number of guidelines and other supporting documents per scheme) | Annual | Input needed by activity |
| | | Input needed by activity | Sufficient ecosystem (number of conformity assessment bodies, of developers of certified solutions and providers of certified services, number of MS issuing certificates and number of certificates issued by MS at national level to implement certification) to cover the certification of ICT solutions for a safe Europe | Annual | Input needed by activity |
| 7.3: Supporting the Union's certification forums (ECCG/SCCG) | Rate of satisfaction with ENISA's support for the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG) | Input needed by activity | Satisfaction of ECCG with ENISA support | Annual | Input needed by activity |

| ACTIVITY 7 RESOURCE FORECASTS | | |
|---|---|---|
| Key action | Budget | FTEs |
| 7.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes | 360.000 + 800.000 contribution agreements[19] | 6 + 2 contribution agreements[20] |
| 7.2: Implementing and maintaining the established schemes | 80.000 | 2 |
| 7.3: Supporting the Union's certification forums (ECCG/SCCG) | 100.000 | 2 |
| **TOTAL** | **540.000 + 800.000** | **10 + 2** |

[19] Pending contribution agreement for the support of the EU digital wallet
[20] Pending contribution agreement for the support of the EU digital wallet

# ACTIVITY 8 MARKET, TECHNOLOGY AND PRODUCT SECURITY

**WHAT WE DO?**

Based on ENISA methodology, Activity 8 will scan for future and emerging cybersecurity areas of interest. Upon publication, the top 3 areas identified in the Technology and Innovation Radar (TIR) report should be taken into consideration across all following ENISA reports (incl. Threat Landscapes and the Report on the State of Cybersecurity in the Union – "NIS2 Art 18 Report"), to verify validity of the foresight and / or provide relevant related recommendations.

By identifying current and emerging ICT gaps, trends, opportunities and threats through thret landscape, market analysis and TIR and on the basis of gaps in MS cybersecurity posture, ENISA through Activity 8 will support the ECCC with advice and opinions, to operationalize this information with relevant funding programs.

Activity 8 will support the implementation of the CRA through relevant guidelines and support to the work of national market supervision authorities and COM. Activity 8 will monitor and analyze emerging trends regarding cybersecurity risks in products with digital elements, compile relevant reports (Art 17(3) of CRA, including analyses of data from SRP reported since its deployment under Art 14(1) and (3) and Art 15(1) and (2)) and support MSAs thereof.

# ACTIVITY 8 KEY OUTPUTS

| DESCRIPTION | Strategic KPIs | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 8.1: Develop and maintain a regular Technology and Innovation Radar (TIR) | Identify and report on future and emerging threat areas ~~reflected in the policy initiatives and interventions~~ | Input needed by activity | 3 top areas identified in TIR have been validated/endorsed by stakeholders (AG) operational and strategic communities (CNNW/CyCLONe) and policymakers (COM/NIS CG) | Annual | All validations finalised by … |
| | Uptake of recommendations stemming from NIS2 Art. 18 report | Input needed by activity | Pending | Annual | Input needed by activity |
| 8.2: Monitor and analyze emerging trends regarding cybersecurity risks in products with digital elements, and give input to Art 18 report | Number of advise and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC | Input needed by activity | Satisfacation from ECCC GB with ENISA recommendations and opinions towards ECCC in n+2 | Annual | Input needed by activity |
| | Reporting platform under CRA is ~~established within 21 months of the entry into force of the Regulation and~~ successfully operated (after its establishment in Q3 2026) | Input needed by activity | Percentage of target audience (NIS CG) satisfied or highly satisfied with the report under Art 17 (3) of CRA | Annual | 75% |
| 8.3: Support MS market surveillance authorities and COM in implementing CRA | Rate of satisfaction with ENISA's support for the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG) | Input needed by activity | satisfaction of MSA's with ENISA work | Annual | Input needed by activity |

| ACTIVITY 8 RESOURCE FORECASTS | | |
|---|---|---|
| Key action | Budget | FTEs |
| 8.1: Develop and maintain a regular Technology and Innovation Radar (TIR) | 120.000 | 1 |
| 8.2: Monitor and analyze emerging trends regarding cybersecurity risks in products with digital elements, and give input to Art 18 report | 150.000 | 3 |
| 8.3: Support MS market surveillance authorities and COM in implementing CRA | 188.000 | 4 |
| **TOTAL** | **458.000** | **8** |

# ACTIVITY 9 SECURE INFRASTRUCTURE

**WHAT WE DO?**

ENISA through Activity 9 will ensure the continuous functionality and durability (incl cybersecurity) of infrastructure and tools, which support operational cybersecurity networks (CSIRTs Network & EU-CyCLONe). The platforms, infrastructure and tools within the scope are: (1) all digital networks, tools and platforms which are directly used by the network members themselves (ex: Mattermost), (2) platforms which enable ENISA to add value in support the networks, both externally facing (EUVDB, CRA SRP, CIRAS) and internally facing (URSA) and (3) any operational infrastructure/tool the Agency is running apart from its internal IT (EUDIR, ENISA website).

In addition the activity supports the development, administration and running of the EUVD both in terms of the maintenance of the database as well as valorizing and synthesizing the information provided and adding value to the MS in the CVD process and vulnerability management at the EU level. Finally, ENISA through Activity 9 will ensure the timely development of the single reporting platform (SRP) end of 2026 and its maintenance 2027 and onwards.

# ACTIVITY 9 KEY OUTPUTS

| DESCRIPTION | Corporate Objectives / Operational KPIs | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 9.1: Develop and maintain ENISA's core IT infrastructure and capabilities (incl secure data center services) | Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks | Input needed by activity | Satisfaction of the ENISA maintained IT systems and platforms | Annual | Input needed by activity |
| | | Input needed by activity | Level of cybersecurity for the infrastructure and tools | Annual | Input needed by activity |
| | EU Vulnerability Database is operationalized by ENISA and a satisfaction rate (by MS and stakeholders) with ENISA ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats | Input needed by activity | User satisfaction with EUVD | Annual | CNW satisfaction > 4 out of 5 |

| | | | | | |
|---|---|---|---|---|---|
| | Reporting platform under CRA is ~~established within 21 months of the entry into force of the Regulation and~~ successfully operated (after its establishment in Q3 2026) | Input needed by activity | Security of IT systems and platforms comply with EUIBAs cybersecurity regulation and ENISA cybersecurity maturity plan. | Annual | Input needed by activity |
| 9.2: Develop and maintain secure IT systems and platforms for operational activities | Introduce digital solutions that maximize synergies and collaboration within the Agency | MT / ITMC | Critical systems uptime//downtime<br><br>Average time to respond to facilities management requests | Annual | 99 %<br><br><1 to acknowledge and <3 to respond |
| 9.3: Develop and maintain secure IT systems and platforms for corporate activities | Introduce digital solutions that maximize synergies and collaboration within the Agency | MT / ITMC | Average time to respond to facilities management requests | Annual | <1 to acknowledge and <3 to respond |
| 9.4: Develop and maintain secure facilities, conducive and sustainable physical and digital workspaces to support the Agency's operations | Develop efficient framework for continuous governance to safeguard high level of IT and physical security | MT / ITMC | Staff satisfaction with IT resolution | Annual | 85 % |

| ACTIVITY 9 RESOURCE FORECASTS | | |
|---|---|---|
| Key action | Budget | FTEs |
| 9.1: Develop and maintain ENISA's core IT infrastructure and capabilities (incl secure data center services)[21] | 300.000 | 8 |

[21] The budget allocation for (9.1 and 9.2), including the cybersecurity maturity plan in activity 11, is significantly less then what is assessed as needed as of 2028 onwards. Additional funding may be provided where such provision is included in the relevant contribution agreements

| | | |
|---|---|---|
| 9.2: Develop and maintain secure IT systems and platforms for operational activities | 1.795.000 + 4.020.000 contribution agreements[22] | 5 + 10[23] |
| 9.3: Develop and maintain secure IT systems and platforms for corporate activities | 2.074.852 | 3 |
| 9.4: Develop and maintain secure facilities, conducive and sustainable physical and digital workspaces to support the Agency's operations | 1.638.942 | 2 |
| **Total** | **5.808.794 + 4.020.000** | **18 + 10** |

[22] Incident and Vulnerability Response Support and Reporting, support Action plan on the cybersecurity of hospitals and healthcare providers and forecast contribution agreement for EUVD management
[23] Incident and Vulnerability Response Support and Reporting, support Action plan on the cybersecurity of hospitals and healthcare providers and forecast contribution agreement for EUVD management

## ACTIVITY 10 HUMAN CAPABILITIES, SKILLS AND RESOURCE

**WHAT WE DO?**

This activity seeks to meet Art 3(4) of the Cybersecurity Act which calls the Agency to: “develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation”.

ENISA aims to develop its human resources to align with the Agency’s goals and needs, by attracting, retaining, and nurturing talent while enhancing its reputation as an agile, knowledge-driven organization where staff is encouraged to grow, in personal and professional perspective, remain engaged and in a healthy work-life balance. A key priority for the Agency is further digitalisation, becoming more efficient, encourage the competency development for staff, positioning ENISA as an "employer of choice" and a rewarding workplace for all.

The Agency strives to maximize resource efficiency by building a flexible, skilled, and fit-for-purpose workforce through strategic workforce planning. ENISA is committed to maintaining the effective functioning of the Agency and delivering high-quality services across both administrative and operational areas. Additionally, the Agency recognizes that flexible working arrangements support a healthy balance between work and personal life for its staff.

## ACTIVITY 10 KEY OUTPUTS

| DESCRIPTION | Corporate objective | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 10.1: Support the workforce planning and annual reviews and implement relevant actions (contract renewals, recruitment, restructurings) | Effective workforce planning and management | MT | Turnover rates | Annual | <5% |
| | | | Establishment plan posts filled | | >95% |
| | | | Percentage of the implementation of approved Recruitment plan | | >90% |
| | | | Implementation of Strategic Workforce Planning and Review decisions | | Timely |
| 10.2: Support the Agency’s performance and talent management and implement annual CDR and reclassification exercises | Efficient talent acquisition, development and retainment | MT | Percentage of staff satisfaction with talent development | Annual | > 50 % |
| | | | Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time | | <10 |
| | | | Number of implemented competency driven training and development activities | | < 10 |

| | | | | | |
|---|---|---|---|---|---|
| 10.3: Develop and maintain HR-related staff services (incl welfare) and help to support high level of psychological safety at work | Efficient talent acquisition, development and retainment | MT | Staff satisfaction with working environment<br><br>High participation in staff satisfaction survey | Annual | >70%<br><br>75 % participation rate |
| 10.4: Plan and develop efficient HR, tendering, contract- and financial management services in support the Agency's operations | Ensure efficient corporate services | MT | Percentage of the implementation of approved Procurement Plan<br><br>Percentage of budget implementation<br><br>Average time for initiating a transaction (FIA role)<br><br>Average time for verifying a transaction (FVA role) | Annual | >90%<br><br>>95%<br><br><7 days<br><br><3 days |

| **ACTIVITY 10 RESOURCE FORECASTS** | | |
|---|---|---|
| Key action | Budget | FTEs |
| 10.1: Support the workforce planning and annual reviews and implement relevant actions (contract renewals, recruitment, restructurings) | 84.697 | 13.5 |
| 10.2: Support the Agency's performance and talent management and implement annual CDR and reclassification exercises | 460.000 | |
| 10.3: Develop and maintain HR-related staff services (incl welfare) and help to support high level of psychological safety at work | 346.000 + 314.848 contribution agreements[24] | |
| 10.4: Plan and develop efficient HR, tendering, contract- and financial management services in support the Agency's operations | 520.000 | 2 contribution agreements[25] |
| **Total** | **1.410.697 + 314.848** | **13.5 + 2** |
| **Salaries** | | |
| Statutory staff (TA, CA, SNEs) | 15.022.286 | |
| Staff financed by contribution agreements | 3.148.480 | |

[24] Budget forecast for HR related services to staff implementing contribution agreements
[25] Procurement FTEs forecast for implementing contribution agreements

# ACTIVITY 11 CORPORATE GOVERNANCE

## WHAT WE DO?

The activity seeks to achieve requirements under Art 4(1) of the CSA that sets an objective for the Agency to: "be a centre of expertise on cybersecurity by virtue of its **independence**, the scientific and technical **quality of the advice and assistance it delivers**, the information it provides, the **transparency of its operating procedures**, the **methods of operation**, and its **diligence in carrying out its tasks**". This objective requires *inter alia* an efficient performance and risk management framework, and the development of single administrative practices, as well as the promotion of sustainability across all Agency's operations. In addition, in line also with Art 4(2) of the CSA, the activity includes contribution to efficiency gains, e.g. via shared services in the EU Agencies network by relying on the Agency's own expertise (e.g. cybersecurity risk management).

Under this activity ENISA seeks to deliver against key objectives of the Agency's Corporate Strategy (service-centric and sustainable organisation), including by establishing a thorough quality assessment framework, ensuring proper and functioning internal controls and compliance checks, as well as maintaining a high level of cybersecurity across all Agency's corporate and operational activities. Enhancing and maintaining the cybersecurity posture of the Agency requires the execution of a cybersecurity maturity plan in order to reach the maturity level required by the Agency for the legislative tasks assigned to it, such as the EU Vulnerability Database, the CRA and DORA platforms and in line with the Regulation (EU).2023/2841.

In terms of resource management, the Budget Management Committee coordinates the Agency's adherence to financial management principles. In the area of IT systems and services, the IT Management Committee coordinates and monitors the comprehensive application of the Agency's IT strategy and adherence to applicable policies and procedures.

The legal basis for this activity is Art 4(1) and 4(2) of CSA, as well as Art 24-28, Art. 41 and Art 32 - 33 (ENISA financial rules and combatting of fraud).

# ACTIVITY 11 KEY OUTPUTS

| DESCRIPTION | Corporate objectives | Validation | Measurement | Frequency & date source | TARGET 2027 |
|---|---|---|---|---|---|
| 11.1: Ensure efficient and effective operational programming, resource planning and reporting | Developing service propositions with additional external resourcing | MT / BMC | Efficiency and effectiveness of ITMC & BMC (survey) | Annual | >90% |
| 11.2: Ensure that the Agency's rules and practices are fit for purpose, compliant and all risks are managed | Developing service propositions with additional external resourcing | MT | Timely follow-up and resolution of internal and external audits (in particular from IAS and ECA) recommendations and findings<br>Number of identified regulatory breaches<br>Percentage of identified internal controls deficiencies addressed within timelines<br>Number of high risks identified in annual risk assessment | Annual | <180 days<br>0 for critical/major, <=3 for moderate<br>100 % for critical, 80 % for major, 60 % for moderate<br><3<br>30% reduction of high risks identified in previous year |
| 11.3: Maintain and enhance ENISA's security posture and implement the cybersecurity maturity plan | Develop efficient framework for continuous governance to safeguard high level of IT and physical security | MT / ITMC | Cybersecurity measures implemented according to maturity plan and for set timelines<br>Address all potential cybersecurity incidents | Annual | Measures and timelines in accordance with the cybersecurity masterplan<br>All cybersecurity incidents addressed in timely way |

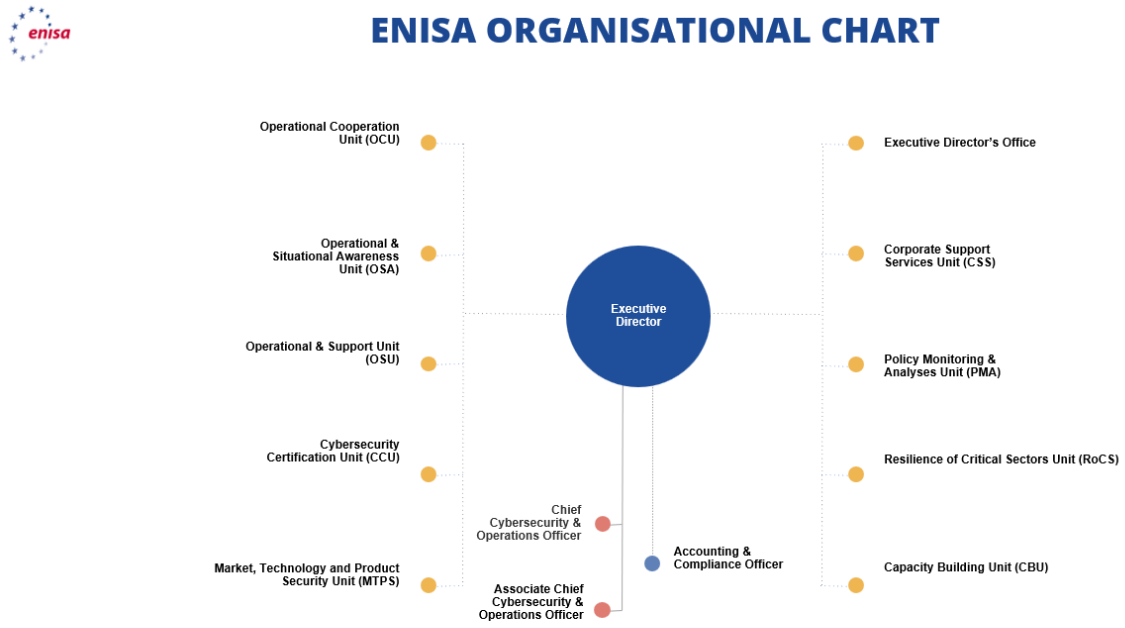
| | | | | | |
|---|---|---|---|---|---|
| | | | Cybersecurity trainings for staff and managers | | >2 training sessions by ISO |
| 11.4: Ensure consistency and synergies across all Agency's IT developments and maximize efficiencies | Develop efficient framework for continuous governance to safeguard high level of IT and physical security | MT / ITMC | Percentage of staff considering that the information they need to do their job is easily available/accessible within ENISA | Annual | 50% |
| 11.5: Ensure support for MB/EB and single administration and administrative services across the Agency | Ensure ENISA is climate neutral by 2030 | MB | Response timeliness to external parties (internal reporting)<br><br>Reduction of CO2 emissions in ENISA HQ<br><br>Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA | Annual | High response rates in accordance with ENISA's code of conduct<br><br>Timely submission of report with actions and recommendations<br><br>>80% |

| ACTIVITY 11 RESOURCE FORECASTS | | |
|---|---|---|
| Key action | Budget | FTEs |
| 11.1: Ensure efficient and effective operational programming, resource planning and reporting | | 4 |
| 11.2: Ensure that the Agency's rules and practices are fit for purpose, compliant and all risks are managed | | |
| 11.3: Maintain and enhance ENISA's security posture and implement the cybersecurity maturity plan[26] | 283.315 | 8 |
| 11.4: Ensure consistency and synergies across all Agency's IT developments and maximize efficiencies | | |
| 11.5: Ensure support for MB/EB and single administration and administrative services across the Agency | 100.000 + 560.000[27] | 1 + 6 contribution agreements[28] |
| **Total** | **383.315 + 560.000** | **13 + 6** |

[26] The budget allocation for the cybersecurity maturity plan in activity 11, is significantly less then what was assessed as needed as of 2028 onwards. Additional funding may be provided where such provision is included in the relevant contribution agreements
[27] Budget forecast for administrative support to implement contribution agreements via external contractor / interim support
[28] Administrative support FTE forecast for implementing contribution agreements

# ANNEX

## I. ORGANISATION CHART AS OF 31.12.2025



# II. RESOURCE ALLOCATION PER ACTIVITY 2027 - 2029

The indicative allocation of the total 2027 financial and human resources following the activities as described in Section III are presented in the table below. The allocation will be done following direct budget and FTEs indicated for each activity with indirect budget being assigned based on causal relationships.

The following assumptions are used in the simplified ABB methodology:

- Budget granted to ENISA through the Contribution Agreements signed in 2023, 2024 and in 2025 is not included in the calculations as activities (as well as budget) defined in the mentioned agreements span through 2024-2028.
- Additional FTEs granted to ENISA through the Contribution Agreements signed in 2023, 2024 and in 2025 are not included in the calculations as their direct and indirect costs should be fully covered by the Contribution Agreement.
- Budget allocation to activity 1-8 includes Direct and Indirect budget attributed to each activity, while activity 9-11 is calculated only on Indirect budget attributed to the activities.
- Direct Budget is the cost estimate of each of the activities as indicated under Section 3.1 of the SPD 2027-2029 (carried out under Articles 5-12) in terms of goods and services to be procured.
- Budget for operational missions and large scale operational events is allocated to activities (Activities 1-8) based on the direct FTEs under each activity.
- Indirect Budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs, attributable to each activity based on the link of the activity to the budget line (as indicated in the Statement of Estimates). The indirect budget is allocated to activities based on different drivers. Main driver for costs allocation was number of foreseen direct FTEs for each activity in 2027.
- In order to estimate full costs of activities (1 to 8), activities (Activities 9 to 11) should be distributed accordingly to all operational activities based on respective drivers.

| ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2027) | Activities as referred to in Section 3 | Direct and Indirect budget allocation (in EUR) | FTE allocation |
|---|---|---|---|
| Policy Monitoring And Analysis | Activity 1 | €1.706.797,00 | 8 |
| Resilience Of Critical Sectors | Activity 2 | €2.205.056,00 | 10 |
| Capacity Building | Activity 3 | €2.432.562,00 | 11 |
| Operational Cooperation & Coordination | Activity 4 | €3.277.467,00 | 12 |
| Operational & Situational Awareness | Activity 5 | €5.146.628,00 | 23 |
| Operational Support | Activity 6 | €662.022,00 | 4 |
| Cybersecurity Certification | Activity 7 | €2.195.056,00 | 10 |
| Market, Technology And Product Security | Activity 8 | €1.782.045,00 | 8 |
| Secure infrastructure | Activity 9 | €3.120.510,00 | 18 |
| Human capabilities, skills and resources | Activity 10 | €2.464.832,00 | 13 |
| Corporate governance | Activity 11 | €2.723.514,00 | 13 |
| **TOTAL** | | 27.716.493 | 130 |

* Activities implementing activities agreed under the Contribution Agreements signed in 2023, 2024 and in 2025 where additional budget has been granted accordingly as well as additional FTEs for implementation of agreed activities during 2024-2028. Further information can be found in Annex XI.

# III. FINANCIAL RESOURCES 2027 - 2029

**TABLE 1:** REVENUE (EXCLUDING ADDITIONAL FINANCING THROUGH CONTRIBUTION AGREEMENTS)

| Revenues | 2026 | 2027 |
|---|---|---|
| **EU contribution** | 26.495.438 | 27.007.607 |
| **forecast other revenue (EFTA)** | 695.364 | 708.886 |
| **Other revenue from other contribution agreements (SLAs, Annex XI)** | p.m. | p.m. |
| **TOTAL** | **27.190.802** | **27.716.493** |

| REVENUES | 2026 budget | VAR 2027 / 2026 | Draft Estimated budget 2027 | Envisaged 2028 | Envisaged 2029 |
|---|---|---|---|---|---|
| 1 REVENUE FROM FEES AND CHARGES | | | | | |
| 2 EU CONTRIBUTION | 26.495.438 | 1,93% | 27.007.607 | 27.547.759 | 28.098.714 |
| *- of which assigned revenues deriving from previous years' surpluses* | *155.877* | | *155.877* | 155.877 | 155.877 |
| 3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries) | 695.364 | 1,94% | *708.886* | 723.145 | 737.690 |
| *- of which EEA/EFTA (excl. Switzerland) ** * | 695.364 | *1,94%* | *708.886* | 723.145 | 737.690 |
| *- of which Candidate Countries* | | | | | |
| 4 OTHER CONTRIBUTIONS *** | p.m. | N/A | p.m. | p.m. | p.m. |
| 5 ADMINISTRATIVE OPERATIONS | | | | | |
| *- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)* | | | | | |
| 6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT **** | p.m. | N/A | p.m. | p.m. | p.m. |
| 7 CORRECTION OF BUDGETARY IMBALANCES | | | | | |
| **TOTAL REVENUES** | **27.190.802** | **1,93%** | **27.716.493** | **28.270.904** | **28.836.404** |

* - after the move to the new building, Hellenic Authorities make rental payments directly to the building owner, therefore no subsidy is paid to ENISA. In 2023 ENISA signed its first Contribution Agreement with DG CONNECT.

** - for the purpose of calculation of EFTA funds for 2027-2029 the surplus of 2024 was used with 2,64% EFTA proportionality factor 2025
*** - 2 new contribution agreements were signed in December 2024: for up to EUR 15 million (prefinancing 80 %) and for up to EUR 400 000 (prefinancing 60%) where the first instalments were received in 2025 12m Support Action, SitCEN and CRA SRP and a new contribution agreement was signed in August 2025 12.233m was received for EU cyber reserve and SitCEN see XI annex
**** - revenue foreseen from the existing SLAs signed with ECCC and eu-LISA, ref. Annex XI
***** budget estimates for 2028 throughout this document are for illustrative purposes only and do not pre-judge the next multiannual financial framework

**Table 2:** Expenditure (C1 funds) (excluding revenue for services rendered and additional financing through contribution agreements)

| EXPENDITURE * ** | 2026 | | 2027 | |
|---|---|---|---|---|
| | Commitment appropriations | Payment appropriations | Commitment appropriations | Payment appropriations |
| **Title 1** | 16.031.333 | 16.031.333 | 16.562.983 | 16.562.984 |
| **Title 2** | 4.290.159 | 4.290.159 | 4.167.109 | 4.167.109 |
| **Title 3** | 6.869.310 | 6.869.310 | 6.986.400 | 6.986.400 |
| **Total expenditure** | **27.190.802** | **27.190.802** | **27.716.492** | **27.716.493** |

| EXPENDITURE (in EUR) | Commitment and Payment appropriations * ** | | | | | |
|---|---|---|---|---|---|---|
| | Amended Budget 2025 | Adopted budget 2026 | Draft budget 2027 | VAR 2027 / 2026 | Envisaged in 2028 | Envisaged in 2029 |
| **Title 1. Staff Expenditure** | **15.555.529** | **16.031.333** | **16.562.983** | **3,3%** | **16.894.325** | **17.232.293** |
| 11 Staff in active employment | 13.840.860 | 14.598.932 | 15.022.286 | 2,9% | 15.322.814 | 15.629.352 |
| 12 Recruitment expenditure | 508.469 | 217.593 | 84.697 | -61,1% | 86.391 | 88.119 |
| 13 Socio-medical services and training | 688.200 | 626.808 | 806.000 | 28,6% | 822.120 | 838.562 |
| 14 Temporary assistance | 518.000 | 588.000 | 650.000 | 10,5% | 663.000 | 676.260 |
| 15 External services on HR matters | N/A | | 0 | | 0 | 0 |
| **Title 2. Building, equipment and miscellaneous expenditure** | **4.159.348** | **4.290.159** | **4.167.109** | **-2,9%** | **4.250.451** | **4.335.460** |
| 20 Building and associated costs | 1.081.300 | 1.061.957 | 1.192.942 | 12,3% | 1.216.801 | 1.241.137 |
| 21 Movable property and associated costs (***) | 0 | | 0 | | 0 | 0 |
| 22 Current corporate expenditure | 687.000 | 336.858 | 316.000 | -6,2% | 322.320 | 328.766 |
| 23 Corporate ICT | 2.391.048 | 2.891.344 | 2.658.167 | -8,1% | 2.711.331 | 2.765.557 |
| **Title 3. Operational expenditure** | **6.999.454** | **6.869.310** | **6.986.400** | **1,7%** | **7.126.128** | **7.268.651** |
| 30 Activities related to meetings and missions | 1.536.000 | 1.290.415 | 1.161.400 | -10,0% | 1.184.628 | 1.208.321 |
| 36/37 Core operational activities | 5.463.454 | 5.578.895 | 5.825.000 | 4,4% | 5.941.500 | 6.060.330 |
| **TOTAL EXPENDITURE** | **26.714.331** | **27.190.802** | **27.716.492** | **1,9%** | **28.270.904** | **28.836.404** |

*(*) Does not include EUR 174 604 for possible revenue under SLAs with ECCC and EU-LISA, ref. Annex XI*

*(**) Does not include amounts granted under the Contribution Agreements, see annex XI*

*(***) As from 2023, "Movable property and associated costs" have been included in Chapter 21 and 22 for streamlining purpose*

**Additional EU funding: contribution and service-level agreements applicable to ENISA**

In addition to the EU contribution, over the period 2024-2026 ENISA will execute an additional funding amounting to EUR 20 million stemming from the Contribution Agreement signed in December 2023;

In December 2024, two additional Contribution Agreements were signed, resulting in a total increase of EUR 15,4 million in funding. Of this amount, EUR 400.000 were allocated to a feasibility study on single reporting platform under the Cyber Resilience Act while the agency was funded by EUR 15 million for the implementation of the 'Incident and Vulnerability Response Support and Reporting' action under the Digital Europe Programme ("DEP")

In July 2025 ENISA received another EUR 36,67 million to finance the implementation of the action EU Cybersecurity Reserve as well as the Cyber Situation and Analysis Center.

In addition, two contribution agreements are expected to be signed in Q1 2026 – Contribution Agreement to support the implementation of the Action plan on the cybersecurity of hospitals and healthcare providers for 6m euros and support to Western Balkans 4m euros. Activity resource forecasts include additional financing for the maintenance and management of EUVD for 4m euros.

Please refer to Annex XI for details of all Contribution Agreements.

**Table 3:** Budget outturn and cancellation of appropriations (unaudited)

| Budget outturn | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|
| **Revenue actually received (+)** | 39.227.392 | 25.293.935 | 42.473.035 | 54.955.252 |
| **Payments made (-)** | -20.396.780 | -21.118.392 | -25.690.066 | -28.674.472 |
| **Carry-over of appropriations (-)** | -18.836.095 | -4.228.452 | -16.945.798 | -38.608.031 |
| **Cancellation of appropriations carried over (+)** | 248.745 | 149.739 | 154.797 | 110.160 |
| **Adjustment for carry-over of assigned revenue appropriations carried over (+)** | 33.743 | 53.469 | 163.909 | 12.337.349 |
| **Exchange rate difference (+/-)** | -18 | 0 | 0 | 0 |
| **Total** | **276.988** | **150.299** | **155.877** | **120.258** |

ENISA's preliminary budgetary outturn amounts to 120 kEUR (unaudited) mainly explained by the cancelled C8 funds for 110 kEUR and the unused C1 funds for 10 kEUR in the 2025 financial year.

With a steady EU budget increase over the last years up to EUR 27,71 million in 2025 a commitment rate of 100% (100% in 2024 and 100% in 2023) of appropriations of the year (C1 funds stemming from the annual EU contribution) at year end has been reached which shows the already proven capacity of the Agency to fully implement its annual appropriations. A very minor amount of EUR 9 748 has not been committed from C1 funds.

Other income, EUR 28,24 million in 2025, are mainly stemming from the various Contribution Agreements signed with the European Commission and from other service level agreements signed with ither EU Bodies.

The payment rate on the committed amounts stemming from the annual European contribution (C1 funds) is 85% (83% in 2024) and the resulting amount carried forward to 2026 is EUR 4,09 million.

The payment appropriations of 2024 carried over to 2025 (C Funds) were utilized at a rate of 97,6% (automatic carry-overs) which indicates a proven capability of estimation of needs (in 2024 – 96,2%). From the total amount of EUR 4,6 million carried forward, the amount of EUR 110 160 was cancelled (or 2,4%).

## IV. HUMAN RESOURCES - QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2027 - 2029

**Table 1:** Staff population and its evolution; Overview of all categories of staff

**Statutory staff and SNE**

| STAFF | 2025 | | | 2026 | 2027 | 2028 | 2029 |
|---|---|---|---|---|---|---|---|
| **ESTABLISHMENT PLAN POSTS** | **Authorised Budget** | **Actually filled as of 31/12/2025** | **Occupancy rate %** | **Envisaged staff** | **Envisaged staff** | **Envisaged staff** | **Envisaged staff** |
| **Administrators (AD)** | 64 | 64 | 100% | 65 | 65 | 65 | 65 |
| **Assistants (AST)** | 19 | 19 | 100% | 18 | 18 | 18 | 18 |
| **Assistants/Secretaries (AST/SC)** | | | | | | | |
| **TOTAL ESTABLISHMENT PLAN POSTS** | **83** | **83** | **100%** | **83** | **83** | **83** | **83** |
| **EXTERNAL STAFF** | **FTE corresponding to the authorised budget 2024** | **Executed FTE as of 31/12/2024** | **Execution rate %** | **Envisaged FTE** | **Envisaged FTE** | **Envisaged FTE** | **Envisaged FTE** |
| **Contract Agents (CA)**[29] | 32 | 30 | 95% | 32 | 32 | 32 | 32 |
| **Contract Agents (stemming from contribution agreements)** | | | | 41 CA contribution agreement | 41* CA contribution agreement | 41* CA contribution agreement | +p.m. |
| **Seconded National Experts (SNE)** | 15 | 13 | 87% | 15 | 15 | 15 | 15 |
| | | | | | | | |
| **TOTAL STAFF**[30] | **130** | **125** | **95%** | **171** | **171** | **171** | **130** |

*Additional external staff expected to be financed from grant, contribution or service-level agreements*

| Human Resources | 2025 | 2026 | 2027 | 2028 | 2029 |
|---|---|---|---|---|---|
| | **Envisaged FTE** | **Envisaged FTE** | **Envisaged FTE** | **Envisaged FTE** | **Envisaged FTE** |
| **Contract Agents (CA)** | 16 | 18[31]* | 18* | p.m. | p.m. |
| **Seconded National Experts (SNE)** | n/a | n/a | n/a | n/a | n/a |
| **TOTAL** | 16* | 18* | 18* | p.m. | p.m. |

[29] Article 38.2 of the ENISA Financial Rules allows the opportunity to "offset the effects of part-time work". ENISA will explore this option in 2025 and may use this option in the future to offset long-term absences and part-time work with short term contracts of CA.
[30] Refers to TAs, CAs and SNEs figures
[31] Please see annex XI for additional information

Other Human Resources

- Structural service providers

| | Actually in place as of 31/12/2024 | Actually in place as of 31/12/2025 |
|---|---|---|
| Security | 7 | 7 |
| IT | 8 | 8 |
| Facilities management | 4 | 4 |

- Interim workers

| | Actually in place as of 31/12/2024 | Actually in place as of 31/12/2025 |
|---|---|---|
| Number | 10 | 12 |

**Table 2:** Multi-annual staff policy plan Years 2025-2029

| Function group and grade | 2025 | | | | 2026 | | 2027 | | 2028 | 2029 |
|---|---|---|---|---|---|---|---|---|---|---|
| | Authorised budget | | Actually filled as of 31/12/2025 | | draft EU budget 2026 | | Envisaged[32] | | Envisaged | Envisaged |
| | Perm. Posts | Temp. posts | Perm. Posts | Temp posts | Perm. posts | Temp. posts | Perm. posts | Temp. posts | Temp. posts | Temp. posts |
| AD 16 | | | | | | | | | | |
| AD 15 | | 1 | | 1 | | 1 | | 1 | 1 | 1 |
| AD 14 | | | | | | | | | | |
| AD 13 | | 2 | | 1 | | 2 | | 2 | 2 | 2 |
| AD 12 | | 4 | | 4 | | 4 | | 4 | 4 | 4 |
| AD 11 | | 3 | | 3 | | 3 | | 3 | 3 | 3 |
| AD 10 | | 4 | | 4 | | 7 | | 7 | 7 | 7 |
| AD 9 | | 14 | | 13 | | 15 | | 15 | 15 | 15 |
| AD8 | | 16 | | 13 | | 14 | | 14 | 14 | 14 |
| AD 7 | | 13 | | 12 | | 12 | | 13 | 13 | 13 |
| AD 6 | | 7 | | 14 | | 6 | | 6 | 6 | 6 |
| AD 5 | | | | | | | | | | |
| AD TOTAL | | 64 | | 65 | | 64 | | 65 | 65 | 65 |
| AST 11 | | | | | | | | | | |
| AST 10 | | | | | | | | | | |
| AST 9 | | 1 | | 2 | | 2 | | 2 | 2 | 2 |
| AST 8 | | 3 | | | | 1 | | 1 | 1 | 1 |
| AST 7 | | 3 | | 1 | | 4 | | 3 | 3 | 3 |
| AST 6 | | 6 | | 7 | | 7 | | 7 | 7 | 7 |
| AST 5 | | 4 | | 4 | | 4 | | 4 | 4 | 4 |
| AST 4 | | 2 | | 2 | | 1 | | 1 | 1 | 1 |
| AST 3 | | | | 1 | | | | | | |
| AST 2 | | | | 1 | | | | | | |
| AST 1 | | | | | | | | | | |
| AST TOTAL | | 19 | | 18 | | 19 | | 18 | 18 | 18 |
| AST/SC 6 | | | | | | | | | | |
| AST/SC 5 | | | | | | | | | | |
| AST/SC 4 | | | | | | | | | | |
| AST/SC 3 | | | | | | | | | | |
| AST/SC 2 | | | | | | | | | | |
| AST/SC 1 | | | | | | | | | | |
| AST/SC TOTAL | | | | | | | | | | |
| TOTAL | | 83 | | 83 | | 83 | | 83 | 83 | 83 |

[32] Envisaged reflects future reclassification exercises

| Function group and grade | 2025 | | | | 2026 | | 2027 | | 2028 | 2029 |
|---|---|---|---|---|---|---|---|---|---|---|
| | Authorised budget | | Actually filled as of 31/12/2025 | | draft EU budget 2026 | | Envisaged[32] | | Envisaged | Envisaged |
| | Perm. Posts | Temp. posts | Perm. Posts | Temp posts | Perm. posts | Temp. posts | Perm. posts | Temp. posts | Temp. posts | Temp. posts |
| GRAND TOTAL | 83 | | 83 | | 83 | | 83 | | 83 | 83 |

**External personnel**

*Contract Agents*

| Contract agents | FTE corresponding to the authorised budget 2025 | Executed FTE as of 31/12/2025 | FTE corresponding to the envisaged budget 2026 | FTE corresponding to the envisaged budget 2027 | FTE corresponding to the envisaged budget 2028 | FTE corresponding to the envisaged budget 2029 |
|---|---|---|---|---|---|---|
| Function Group IV | 30 | 26 + 12 contribution agreement | 30 + 18 contribution agreement | 30 + 39 contribution agreement | 30 + 39 contribution agreement | 30 + pm |
| Function Group III | 2 | 2 | 2 | 2 | 2 | 2 |
| Function Group II | 0 | 0 | 0 | 0 | 0 | 0 |
| Function Group I | 0 | 0 | 0 | 0 | 0 | 0 |
| TOTAL | 32 | 40 | 50 | 71 | 71 | 32 |

*Seconded National Experts*

| Seconded National Experts | FTE corresponding to the authorised budget 2024 | Executed FTE as of 31/12/2025 | FTE corresponding to the authorised budget 2025 | FTE corresponding to the envisaged budget 2026 | FTE corresponding to the envisaged budget 2027 | FTE corresponding to the envisaged budget 2028 | FTE corresponding to the envisaged budget 2029 |
|---|---|---|---|---|---|---|---|
| TOTAL | 15 | 11 | 15 | 15 | 15 | 15 | 15 |

**Table 3**: Recruitment forecasts 2027 following retirement / mobility or new requested posts

| JOB TITLE IN THE AGENCY | TYPE OF CONTRACT (OFFICIAL, TA OR CA) | | TA/OFFICIAL | | CA |
|---|---|---|---|---|---|
| | | | Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication * | | |
| | Due to foreseen retirement/ mobility | New post requested due to additional tasks[33] | Internal (brackets) | External (brackets) | Recruitment Function Group (I, II, III and IV) |

[33] Posts stemming from the required resources for 2026 work programme (12 FTEs)

| | | | | | |
|---|---|---|---|---|---|
| **Expert** | n/a | n/a | n/a | n/a | n/a |
| **Officer** | n/a | n/a | n/a | n/a | |
| **Assistant** | n/a | n/a | n/a | n/a | n/a |

# V. HUMAN RESOURCES - QUALITATIVE

## A. Recruitment policy

Implementing rules in place:

| | | YES | NO | IF NO, WHICH OTHER IMPLEMENTING RULES ARE IN PLACE |
|---|---|---|---|---|
| **Engagement of CA** | Model Decision C(2019)3016 | x | | |
| **Engagement of TA** | Model Decision C(2015)1509 | x | | |
| **Middle management** | Model decision C(2018)2542 | x | | |
| **Type of posts** | Model Decision C(2018)8800 | | x | C(2013) 8979 |

## B. Appraisal and reclassification/promotions

Implementing rules in place:

| | | YES | NO | IF NO, WHICH OTHER IMPLEMENTING RULES ARE IN PLACE |
|---|---|---|---|---|
| **Reclassification of TA** | Model Decision C(2015)9560 | x | | |
| **Reclassification of CA** | Model Decision C(2015)9561 | x | | |
| **Appraisal of TA** | Model Decision C(2015) 1513 | x | | |
| **Appraisal of CA** | Model Decision C(2015) 1456 | x | | |

Table 1: **Reclassification of TA/promotion of official**

| | | AVERAGE SENIORITY IN THE GRADE AMONG RECLASSIFIED STAFF | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Grades** | | **Year 2020** | **Year 2021** | **Year 2022** | **Year 2023** | **Year 2024** | **Year 2025** | **Actual average over 5 years** | **Average over 5 years (According to decision C(2015)9563)** |
| **AD05** | | - | - | - | - | | - | - | 2.8 |
| **AD06** | | - | 1 | 1 | 1 | 2 | 2 | 4,02 | 2.8 |
| **AD07** | | 1 | - | 2 | 1 | 3 | 2 | 4,26 | 2.8 |
| **AD08** | | 2 | 1 | 3 | 1 | 2 | 1 | 3,71 | 3 |
| **AD09** | | - | - | - | 2 | | 2 | 3,13 | 4 |
| **AD10** | | - | - | 2 | - | | 1 | 7,83 | 4 |
| **AD11** | | - | - | - | - | | - | - | 4 |
| **AD12** | | - | 1 | - | - | | - | 10 | 6.7 |
| **AD13** | | - | - | - | - | | - | - | 6.7 |
| **AST1** | | - | - | - | - | | - | - | 3 |
| **AST2** | | - | - | - | - | | - | - | 3 |
| **AST3** | | - | - | 1 | - | | -- | 8,5 | 3 |
| **AST4** | | 1 | - | - | 1 | 1 | - | 5,65 | 3 |
| **AST5** | | - | 1 | - | 1 | - | 1 | 3,47 | 4 |
| **AST6** | | 1 | 1 | - | - | - | 1 | 4 | 4 |
| **AST7** | | - | 1 | 1 | 1 | - | - | 3,97 | 4 |
| **AST8** | | - | - | - | - | 2 | - | 3,5 | 4 |
| **AST9** | | - | - | - | - | | - | - | N/A |
| **AST10 (Senior assistant)** | | - | - | - | - | | - | - | 5 |
| | | **There are no AST/SCs at ENISA: n/a** | | | | | | | |
| **AST/SC1** | | | | | | | | | 4 |
| **AST/SC2** | | | | | | | | | 5 |
| **AST/SC3** | | | | | | | | | 5.9 |
| **AST/SC4** | | | | | | | | | 6.7 |
| **AST/SC5** | | | | | | | | | 8.3 |

**Table 2:** Reclassification of contract staff

| FUNCTION GROUP | GRADE | STAFF IN ACTIVITY AT 31.12.2025 | HOW MANY STAFF MEMBERS WERE RECLASSIFIED IN YEAR 2025 | AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS | AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS ACCORDING TO DECISION C(2015)9561 |
|---|---|---|---|---|---|
| CA IV | 18 | 1 | | 7,8 | - |
| | 17 | - | 1 | 7,8 | Between 6 and 10 years |
| | 16 | 15 | - | - | Between 5 and 7 years |
| | 15 | 4 | 1 | 2,6 | Between 4 and 6 years |
| | 14 | 13 | 2 | 3,5 | Between 3 and 5 years |
| | 13 | 5 | - | 4,15 | Between 3 and 5 years |
| CA III | 12 | 3 | - | - | - |
| | 11 | 1 | - | 2 | Between 6 and 10 years |
| | 10 | 2 | - | 3 | Between 5 and 7 years |
| | 9 | - | - | 4,9 | Between 4 and 6 years |
| | 8 | 0 | - | 4,8 | Between 3 and 5 years |
| CA II | 6 | - | - | - | Between 6 and 10 years |
| | 5 | - | - | - | Between 5 and 7 years |
| | 4 | - | - | - | Between 3 and 5 years |
| CA I | 3 | 1 | - | - | n/a |
| | 2 | - | - | - | Between 6 and 10 years |
| | 1 | - | - | - | Between 3 and 5 years |

## C. Gender representation

**Table 1:** Data on 31.12.2025 statutory staff (only temporary agents and contract agents)

| | | OFFICIAL | | TEMPORARY | | CONTRACT AGENTS | | GRAND TOTAL | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Staff** | **%** | **Staff** | **%** | **Staff** | **%** | **Staff** | **%** |
| **Female** | Administrator level | - | - | 24 | 29,3% | 16 | 35,6% | 40 | 31,5% |
| | Assistant level (AST & AST/SC) | - | - | 13 | 15,9% | 4 | 8,9% | 17 | 13,4% |
| | Total | - | - | **37** | **45,1%** | **20** | **44,4%** | **57** | **44,9%** |
| **Male** | Administrator level | - | - | 40 | 48,8% | 22 | 48,9% | 62 | 48,8% |
| | Assistant level (AST & AST/SC) | - | - | 5 | 6,1% | 3 | 6,7% | 8 | 6,3% |
| | Total | - | - | **45** | **54,9%** | **25** | **55,6%** | **70** | **55,1%** |
| **Grand Total** | | - | - | **82** | **100,0%** | **45** | **100,0%** | **127** | **100,0%** |

| TABLE 2: **DATA REGARDING GENDER EVOLUTION OVER 5 YEARS OF THE MIDDLE AND SENIOR MANAGEMENT (31.12.2025)** | **2020** | | **31.12.2025** | |
|---|---|---|---|---|
| | **Number** | **%** | **Number** | **%** |
| **Female Managers** | 2 | 25% | 3[34] | 30% |
| **Male Managers** | 6 | 75% | 7[35] | 70% |

The focus of the Agency being cybersecurity hints at the reason for a certain gender imbalance. Nevertheless, an improvement has been noted during the past five years. Continuous efforts to encourage female involvement in this domain have borne fruit, however, further efforts should be envisaged in order to achieve a higher percentage of female middle and senior managers at ENISA in the upcoming years.

[34] This category comprises the ED and Heads of Unit level
[35] This category comprises the ED and Heads of Unit level

## D. Geographical Balance

**Table 1:** Data on 31.12.2025 - statutory staff only

| Nationality | AD + CA FG IV | | AST/SC- AST + CA FGI/CA FGII/CA FGIII | | TOTAL | |
|---|---|---|---|---|---|---|
| | Number | % of total staff members in AD and FG IV categories | Number | % of total staff members in AST SC/AST and FG I, II and III categories | Number | % of total staff |
| **BE** | 4 | 3,9% | 2 | 8,0% | 6 | 4,7% |
| **BG** | 2 | 2,0% | | 0,0% | 2 | 1,6% |
| **CY** | 2 | 2,0% | 2 | 8,0% | 4 | 3,1% |
| **CZ** | 1 | 1,0% | | 0,0% | 1 | 0,8% |
| **DE** | 1 | 1,0% | | 0,0% | 1 | 0,8% |
| **Double *80** | 5 | 4,9% | 2 | 8,0% | 7 | 5,5% |
| **EE** | 2 | 2,0% | | 0,0% | 2 | 1,6% |
| **EL** | 45 | 44,1% | 13 | 52,0% | 58 | 45,7% |
| **ES** | 3 | 2,9% | | 0,0% | 3 | 2,4% |
| **FR** | 6 | 5,9% | 1 | 4,0% | 7 | 5,5% |
| **HU** | 1 | 1,0% | | 0,0% | 1 | 0,8% |
| **IT** | 10 | 9,8% | | 0,0% | 10 | 7,9% |
| **LT** | 2 | 2,0% | 1 | 4,0% | 3 | 2,4% |
| **LV** | 2 | 2,0% | | 0,0% | 2 | 1,6% |
| **MT** | 1 | 1,0% | | 0,0% | 1 | 0,8% |
| **NL** | 4 | 3,9% | | 0,0% | 4 | 3,1% |
| **PL** | 3 | 2,9% | 1 | 4,0% | 4 | 3,1% |
| **PT** | 2 | 2,0% | 1 | 4,0% | 3 | 2,4% |
| **RO** | 5 | 4,9% | 1 | 4,0% | 6 | 4,7% |
| **SE** | 1 | 1,0% | | 0,0% | 1 | 0,8% |
| **SK** | | 0,0% | 1 | 4,0% | 1 | 0,8% |
| **TOTAL** | **102** | **100%** | **25** | **100%** | **127** | **100%** |

**Table 2:** Evolution over 5 years of the most represented nationality in the Agency

| MOST REPRESENTED NATIONALITY | 2021 | | 31.12.2025 | |
|---|---|---|---|---|
| | Number | % | Number | % |
| Greek | 29 (out of 74) | 39,2 | 58 (out of 129) | 45 |

### E. Schooling

| Agreement in place with the European School of Heraklion | |
|---|---|
| **Contribution agreements signed with the EC on type I European schools** | **No** |
| **Contribution agreements signed with the EC on type II European schools** | **Yes** |

## VI. ENVIRONMENT MANAGEMENT

To be updated during the course of 2026

## VII. BUILDING POLICY

| Building Name and type | Location | Location SURFACE AREA(in m²) | | | RENTAL CONTRACT | | | Host country (grant or support) | Building present value(€) |
|---|---|---|---|---|---|---|---|---|---|
| | | Office space (m2) | non-office (m2) | Total (m2) | Rent (euro per year) | Duration | Type | | |
| **Athens Office** | Chalandri | 4498 | 2617 | 7115 | | 01/01/2021 to 28/02/2030; | Lease | Rent is fully covered by Hellenic Authorities | N/A |
| **Brussels office** | Brussel centre | 98 | | 98 | 56.496 | N/A | SLA with OIB | | N/A |

**Brussels office**

The office is being used on a daily basis by Brussels based staff, which is a significant benefit for the operational activities of the Agency as they are able to communicate readily with the CERT EU Team situated on the same floor.

| Resources (indicative) | 2027 | 2028 | 2029 |
|---|---|---|---|
| Head count (FTEs) | **13-14** | **13-14** | **13-14** |
| Budget (rent & maintenance costs) | **130.000** | **130.000** | **130.000** |

## VIII. PRIVILEGES AND IMMUNITIES

| Agency privileges | Privileges granted to staff | |
|---|---|---|
| | **Protocol of privileges and immunities / diplomatic status** | **Education / day care** |
| In accordance with Art. 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff.<br>The Greek Government and ENISA signed a Seat Agreement the 13 November 2018, which was ratified by Greek Law 4627/2019 on the 25 September 2019 and entered in to force on the 04 October 2019 and is applicable to ENISA and its staff. | In accordance with Article 35 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff.<br>The Greek Government and ENISA signed a Seat Agreement the 13 November 2018, which was ratified by Greek Law 4627/2019 on the 25 September 2019 and entered in to force on the 04 October 2019 and is applicable to ENISA and its staff. | A public School of European Education, Type 2, was founded in 2005 by the Greek government in Heraklion – Crete for the children of the staff of ENISA.<br>There is no European School operating in Athens. |

## IX. EVALUATIONS

The Agency will conduct its third biennial stakeholder satisfaction survey for the work programming period 2025 to 2026 in 2027. Below are the results of the last biennial stakeholder satisfaction survey concluded in 2025.

The results of the second stakeholder satisfaction survey concluded in 2025 sheds much important light on how stakeholders perceive the added value of ENISA's work.

The evaluation concluded that ENISA is providing significant added value and that the outcome of its work is taken up by stakeholders in the immediate to medium term. The survey also sought to assess the satisfaction levels of stakeholders in relation to the way the agency implements its projects, specifically how work is organised and managed its work. The results of which demonstrate that the agency values the input received by validators and that it supports community building.

The mandate of the agency requires that the tasks that it carries out do not duplicate MS activities. Therefore, the fact that 89% of stakeholders surveyed considered that ENISA deliverables do not duplicate or only somewhat duplicate MS activities is justification of ENISA's actions to involve stakeholders in all stages of its work and ensure that the outcomes/ results are fit for purpose. An improvement of 6% from the previous survey conducted in 2023 for the work programme years 2021 and 2022.

Aggregate results:

- Aggregate results for added value 88% (down 4%) and take up 82% (down 3%) were slightly lower in 2023-2024 than the resounding results of 2021-2022.

- Aggregate results for non-duplication with MS activities 89% (up 6%) improved in 2023-24 compared to 2021-2022.

- Aggregate results for how ENISA operates with stakeholders improved in the area of taking onboard stakeholder feedback 94% (up 2%) and facilitating community interaction 96% (up 1%) however how ENISA organized its work and processes 89% (down 6%) compared to 2021-2022.

• Finally trust in ENISA's ability to achieve its mandate increased by 1% to 96% in 2023-2024 compared to 2021-2022.

The survey received strong engagement, with over 186 respondents—an increase of 15% compared to the previous survey—and generated more than 250 comments.

# X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The Agency's strategy for effective internal controls is based on international practices (COSO Framework's international Standards), as well the relevant internal control framework of the European Commission. It comprises of the following key components:

- The Control Environment is the set of standards of conduct, processes and structures that provide the basis for carrying out internal control across ENISA. The Management Team sets the tone at the top with respect to the importance of the internal controls, including expected standards of conduct.

- Risk assessment is the Agency's dynamic and iterative process for identifying and assessing risks which could affect the achievement of objectives, and for determining how such risks should be managed.

- The Control Activities ensure the mitigation of risks related to the achievement of policy, operational and internal control objectives. They are performed at all levels of the organisation, at various stages of business processes, and across the technology environment. They may be preventive or detective and encompass a range of manual and automated activities as well as segregation of duties.
- Information is necessary for the Agency to carry out internal controls and to support the achievement of objectives. In this respect, it is needed to consider both external and internal communication. External communication provides the Agency's stakeholders and globally the EU citizens with information on ENISA's policy, objectives, actions and achievements. Internal communication provides ENISA staff with the information required to support the achievement of objectives and the awareness for day-to-day controls.

- Continuous and specific assessments are used to ascertain whether each of the five components of internal controls is present and functioning. Continuous assessments, built into business processes at different levels of the organisation, provide timely information on any deficiencies. Findings are assessed and deficiencies are communicated and corrected in a timely manner, with serious matters reported as appropriate.

Following relevant guidance and best practices developed within the EU Agencies network, ENISA conducted in 2022 a thorough review of its internal control framework indicators and the overall internal control strategy. The review consolidated input from different sources and integrated the results of various risk assessments within a single internal control assessment process. The revised ENISA's internal control framework has been in use since 2023 for the assessment of internal controls, together with a comprehensive methodology for enterprise risk assessment across the Agency.

Moreover, in 2025 ENISA revised its Anti-Fraud strategy that had been in place since 2021. The revised Anti-Fraud Strategy (AFS) for the period of 2025-2027 has been adopted by means of the Management Board Decision 2025/03 and builds on the outcomes and lessons learned of the previous period. It this context, the Agency puts special focus on the monitoring of conflicts of interest at different levels (e.g. contractors of the Agency, recruitment procedures, members of ENISA statutory bodies or external experts).

In particular, the Agency applies declarations of conflict of interest and confidentiality declarations for members of Ad hoc working groups and by parties contracted through a procurement procedure. Similar declarations are submitted by members of ENISA's evaluation boards. Annual declarations of interest are submitted by members of the Management Board and their alternates, members of the National Liaison Officers' network, and members of the Advisory Group. Additionally, at the start of each meeting the members, observers and any experts participating in the meeting of an Ad Hoc Working Group should declare any interests which could be considered to be prejudicial to their independence with respect to any of the points on the agenda.

Declarations of conflict of interest are also signed by the candidates taking part in recruitment procedures with a view to assess whether a potential or actual conflict of interest exists which could impair the impartiality and the independence of the candidate regarding his/her future responsibilities in relation to the specific position on-offer. Similar procedure applies for the Selection Board members.

# XI. PLAN FOR GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENTS

| | SLA | Date of signature | Total amount forecast | Duration | Counterpart | Short description |
|---|---|---|---|---|---|---|
| **1** | SLA with ECCC (Activity 9) | 20/12/22 | 44672.05 | Renewal on annual basis automatically | ECCC | The scope of this Service Level Agreement covers support services offered by ENISA to ECCC: data protection officer, accounting officer |
| | | | | | | |
| **2** | SLA with eu-LISA M-CBU-24-C35 (Activity 3) | 08/05/2024 | 112195.07 | 31/12/2025 (with option to renew) | Eu-LISA | The scope of this Service Level Agreement covers support services offered by ENISA to eu-LISA on the planning, execution and evaluation of upcoming annual Security and Business Continuity Exercises |
| **Contribution agreements** | | | | | | |
| **1** | Preparedness and Incident Response Support for Key Sectors | 21/12/2023 | Up to EUR 20 mil (prefinancing rate 80%) | up to 31/12/26 | DG CNECT | The action is developed through the "ENISA Cybersecurity Support Action Programme" which is composed of three: 1) EU-level cyber reserve with services from trusted private providers for incident response; 2) penetration tests in key sectors and 3) the Party's contribution to the Cyber Analysis and Situation Centre. |
| **2** | Incident and Vulnerability Response Support and Reporting<br>HAS assessment / EUCC pilots (Addendum I - LC-03708221) | 19/12/2024 | Up to. EUR 15,25 mil (prefinancing rate 80%)<br>(+250k following the amendment) | 2025 to 2027 | DG CNECT | 1) the following activities Gradual set-up and operation of an EU-level cyber reserve with services from trusted private providers to provide relevant services to mitigate the impact of serious incidents; 2) Contribution to the Cyber Analysis and Situation Centre; and 3) The establishment, management, and maintenance of day-to-day of the Cyber Resilience Act single reporting platform<br>2) Additional actions following the amendement: Actions in support of the implementation of the Cyber Resilience Act, notably actions related to development and assessment of technical |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | specifications and standards, and interplay with the European Cybersecurity Certification schemes. |
| **3** | CRA single reporting platform (feasibility study) | 09/12/2024 | Up to 400.000 (prefinancing rate 60%) | up to 31/07/26 | DG CNECT | The purpose of this Agreement is to provide the Organisation with financial contribution to conduct a feasibility study on single reporting platform under the Cyber Resilience Act that will inform the future steps of the platform development. |
| **4** | EU Cybersecurity Reserve & Cyber Situation and Analysis Center | | Up to 36.670.000,00 (pre financing rate 100% for the first contribution 12months) | 2025 to 2028 (36 months) | DG CNECT | The purpose of this Agreement is to provide a financial contribution to finance the implementation of the action “EU Cybersecurity Reserve”, and of the action “Cyber Situation and Analysis Centre”. |

Detailed breakdown of contribution agreements planned resource consumption

| Contribution agreement | Implementation period | Start date | CA total budget | Remaining Amount to be received from 2026 onwards | 2024 Installments | 2025 Installments | 2026 Installments | 2026 forecast of commitment appropriations | 2027 forecast of commitment appropriations | 2028 forecast of commitment appropriations | 2029 forecast of commitment appropriations | Related Activities |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Preparedness and Incident Response Support for Key Sectors (Support Action & Situational Analysis Center) | until 31/12/2026 | 21/12/23 | 20.000.000 | 4.000.000 | 16.000.000 | 0 | | 4.000.000 | 0 | 0 | 0 | Act.6, |
| Incident and Vulnerability Response Support and Reporting (Support Action, CRA SPR and SitCEN) | until 31/12/2027 | 19/12/24 | 15.000.000 | 3.000.000 | 0 | 12.000.000 | | 1.500.000 | 1.500.000 | 0 | 0 | Act 5, Act.6, Act.8, Act.9 |
| support of the implementation of the Cyber Resilience Act, notably actions related to development and assessment of technical specifications and standards and interplay with European Cybersecurity Certification schemes [36] | until 31/12/2027 | 3/7/25 | 250.000 | 250.000 | 0 | 0 | | 125.000 | 125.000 | 0 | 0 | Part of the above CA, ref. Act.7 & Act.8 |
| CRA single reporting platform (feasibility study) | until 31/07/2026 | 9/12/24 | 400.000 | 160.000 | 0 | 240.000 | | 160.000 | 0 | 0 | 0 | Act.9 |

[36] (Amendment n.1 to the 2024 Contribution Agreement on the Implementation of the "Incident and Vulnerability Response Support and Reporting" Action)

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| EU Cybersecurity Reserve &Cyber Situation and Analysis Centre | 36 months | 31/7/25 | 36.670.000 | 24.446.666,67 | 0 | 12.223.333,33 | | 12.223.333,33 | 12.223.333,34 | 0 | 0 | Act.5 Act.6 Act.9 |
| Contribution Agreement to support the implementation of the Action plan on the cybersecurity of hospitals and healthcare providers | 36 months | December 2025 | 6.000.000 | | | | TBC | TBC | TBC | TBC | TBC | Act.2 Act.3 Act.5 Act.9 |
| Western Balkans (PENDING) | 36 months | January 2026 | 4.000.000 | | | | TBC | TBC | TBC | TBC | TBC | Act.4 |
| EU Digital Wallet (PENDING) | 24 months | January 2026 | **8.000.000** | | | | TBC | TBC | TBC | TBC | TBC | Act.7 |
| Total Budget | | | **72.320.000** | **31.856.667** | **16.000.000** | **24.463.333,33** | | **18.008.333** | **13.848.333,34** | **0** | **0** | |

| Contribution agreement | 2027 forecast of Contract Agents | 2028 forecast Contract Agents | 2029 forecast Contract Agents | Related Activities |
|---|---|---|---|---|
| **Preparedness and Incident Response Support for Key Sectors (Support Action & Situational Analysis Center)** | **3** | **3** | **0** | **Act.6, Act.5** |
| **Incident and Vulnerability Response Support and Reporting (Support Action, CRA SRP and SitCEN)** | **2.5** | **2.5** | **0** | **Act.5, Act.2, Act.7, Act.8** |
| **HAS Amendment n.1 to the 2024 Contribution Agreement on the Implementation of the "Incident and Vulnerability Response Support and Reporting" Action** | **3.5** | **3.5** | **0** | **Part of the above CA, ref. Act.7 & Act.8** |
| **CRA single reporting platform** | **6** | **6** | **0** | **Act.9** |
| **EU Cybersecurity Reserve & Cyber Situation and Analysis Centre** | **9** | **9** | **0** | **Act.6, Act.5, Act.2** |
| Contribution Agreement to support the implementation of the Action plan on the cybersecurity of hospitals and healthcare providers | **5** | **5** | **0** | **Act.2 Act.3 Act.5** |
| **Western Balkans (PENDING)** | **6** | **6** | **0** | **Act.4** |
| **EU Digital Wallet (PENDING)** | **2** | **2** | **0** | **Act.7** |

| | | | | |
|---|---|---|---|---|
| **EUVD management (Forecast)** | **4** | **4** | **0** | **Act.9** |
| **Total** | **41** | **41** | **0** | |

## XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

The Agency's international strategy[37] was adopted by the MB in 2021. It confirmed the Agency's mandate in terms of its focus on the EU and EU actors. At the same time, it foresaw engagement with international partners in line with the strategic objectives outlined in the ENISA Strategy for a Trusted and Cyber Secure Europe of July 2020 and in support of the EU's international priorities, adopting so-called *limited, assisting* and *outreach* approaches to its international engagements. A new international strategy was presented to the MB and adopted in Q4 2025.

Article 12 of the Cybersecurity Act (CSA) states that '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' in various ways, including facilitating the exchange of best practices and providing expertise, at the request of the Commission.

Article 42 "Cooperation with third countries and international organisations" states the following

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

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

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

There are furthermore specific examples in EU legislation where an international role of ENISA is also referred to, including in the areas of certification under the Cybersecurity Act (CSA Art. 54 (t)) and in the implementation of the EU Cybersecurity Reserve under the Cyber Solidarity Act (CSoA Art. 19 (2), (11)).

## XIII. ANNUAL COOPERATION PLAN 2027

To be updated in the course of 2026

## XIV. PROCUREMENT PLAN 2027

To be updated in the course of 2026

## XV. ENISA STATUTORY OPERATIONAL TASKS FROM EU LEGISLATION 2025

The following list of EU legislations will be mapped to activities during the course of 2026

[37] https://www.enisa.europa.eu/publications/corporate-documents/enisa-international-strategy

| EU legislation | Article | Legal provisions | Under review |
|---|---|---|---|
| AIA | Art 67(5) | {Advisory forum} The Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) shall be permanent members of the advisory forum. | |
| CRA | Art 10 | {Enhancing skills in a cyber resilient digital environment} For the purposes of this Regulation and in order to respond to the needs of professionals in support of the implementation of this Regulation, Member States with, where appropriate, the support of the Commission, the European Cybersecurity Competence Centre and ENISA, while fully respecting the responsibility of the Member States in the education field, shall promote measures and strategies … | |
| CRA | Art 16(4) | ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single reporting platform and the information submitted or disseminated via the single reporting platform. It shall notify without undue delay any security incident affecting the single reporting platform to the CSIRTs network as well as to the Commission. | |
| CRA | Art 14(1) | {Reporting obligations of manufacturers} A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA /…/ | |
| CRA | Art 14(3) | {Reporting obligations of manufacturers} A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA /…/ | |
| CRA | Art 14(7) | {Reporting obligations of manufacturers} The notifications referred to in paragraphs 1 and 3 of this Article shall be submitted via the single reporting platform referred to in Article 16 using one of the electronic notification end-points referred to in Article 16(1). The notification shall be submitted using the electronic notification end-point of the CSIRT designated as coordinator of the Member State where the manufacturers have their main establishment in the Union and shall be simultaneously accessible to ENISA. | |
| CRA | Art 14(9) | {Reporting obligations of manufacturers} By... [12 months from the date of entry into force of this Regulation], the Commission shall adopt a delegated act in accordance with Article 61 to supplement this Regulation by specifying the terms and conditions for applying the cybersecurity related grounds in relation to delaying the dissemination of notifications as referred to in Article 16(2). The Commission shall cooperate with the CSIRTs network as established pursuant to Article 15 of Directive (EU) 2022/2555 and ENISA in preparing the draft delegated act. | |
| CRA | Art 14(10) | {Reporting obligations of manufacturers} The Commission may, by means of implementing acts, specify further the format and procedures of the notifications referred to in this Article as well as in Articles 15 and 16. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). The Commission shall cooperate with the CSIRTs network and ENISA in preparing those draft implementing acts. | |
| CRA | Art 15(1) | {Voluntary reporting} Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA. | |
| CRA | Art 15(2) | {Voluntary reporting} Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA. | |
| CRA | Art 15(3) | {Voluntary reporting} The CSIRT designated as coordinator or ENISA shall process the notifications referred to in paragraphs 1 and 2 of this Article in accordance with the procedure laid down in Article 16. /…/ | |

| | | | |
|---|---|---|---|
| CRA | Art 15(5) | {Voluntary reporting} The CSIRTs designated as coordinators as well as ENISA shall ensure the confidentiality and appropriate protection of the information provided by a notifying natural or legal person. | |
| CRA | Art 16(1) | {Establishment of a single reporting platform} For the purposes of the notifications referred to in Article 14(1) and (3) and Article 15(1) and (2) and in order to simplify the reporting obligations of manufacturers, a single reporting platform shall be established by ENISA. The day-to-day operations of that single reporting platform shall be managed and maintained by ENISA. The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification end-points. | |
| CRA | Art 16(2) | {Establishment of a single reporting platform} /…/ Where a CSIRT decides to withhold a notification, it shall immediately inform ENISA about the decision and provide both a justification for withholding the notification as well as an indication of when it will disseminate the notification in accordance with the dissemination procedure laid down in this paragraph. ENISA may support the CSIRT on the application of cybersecurity related grounds in relation to delaying the dissemination of the notification /…/ Only the information that a notification was made by the manufacturer, the general information about the product, the information on the general nature of the exploit and the information that security related grounds were raised are made available simultaneously to ENISA until the full notification is disseminated to the CSIRTs concerned and ENISA. Where, based on that information, ENISA considers that there is a systemic risk affecting security in the internal market, it shall recommend to the recipient CSIRT that it disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself. | |
| CRA | Art 16(5) | {Establishment of a single reporting platform} ENISA, in cooperation with the CSIRTs network, shall provide and implement specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single reporting platform referred to in paragraph 1, including at least the security arrangements related to the establishment, operation and maintenance of the single reporting platform, as well as the electronic notification end-points set up by the CSIRTs designated as coordinators at national level and ENISA at Union level, including procedural aspects to ensure that, where a notified vulnerability has no corrective or mitigating measures available, information about that vulnerability is shared in line with strict security protocols and on a need-to-know basis. | |
| CRA | Art 17(1) | {Other provisions related to reporting} ENISA may submit to the European cyber crisis liaison organisation network (EUCyCLONe) established under Article 16 of Directive (EU) 2022/2555 information notified pursuant to Article 14(1) and (3) and Article 15(1) and (2) if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level. For the purpose of determining such relevance, ENISA may consider technical analyses performed by the CSIRTs network, where available | |
| CRA | Art 17(2) | {Other provisions related to reporting} Where public awareness is necessary to prevent or mitigate a severe incident having an impact on the security of the product with digital elements or to handle an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the CSIRT designated as coordinator of the relevant Member State, may, after consulting the manufacturer concerned and, where appropriate, in cooperation with ENISA, inform the public about the incident or require the manufacturer to do so. | |
| CRA | Art 17(3)* | ENISA, on the basis of the notifications received pursuant to Article 14(1) and (3) and Article 15(1) and (2), shall prepare, every 24 months, a technical report […] | |
| CRA | Art 17(5) | After a security update or another form of corrective or mitigating measure is available, ENISA shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified pursuant to Article 14(1) or Article 15(1) of this Regulation to the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555 | |
| CRA | Art 70(2) | {Evaluation and review} By... [45 months from the date of entry into force of this Regulation], the Commission shall, after consulting ENISA and the CSIRTs network, submit a report to the European Parliament and to the Council, assessing the effectiveness of the single reporting platform set out in Article 16, as well as the impact of the application of the cybersecurity related grounds referred to Article 16(2) by the CSIRTs designated as coordinators on the effectiveness of the single | |

| | | | |
|---|---|---|---|
| | | reporting platform as regards the timely dissemination of received notifications to other relevant CSIRTs | |
| CRA | Art 17(3)* | ENISA, on the basis of the notifications received pursuant to Article 14(1) and (3) and Article 15(1) and (2), shall prepare, every 24 months, a technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555. The first such report shall be submitted within 24 months after the obligations laid down in Article 14(1) and (3) start applying. ENISA shall include relevant information from its technical reports in its report on the state of cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555. | |
| CRA | Art 17(3)* | {emerging trends regarding cybersecurity risks in products with digital elements} […] ENISA shall include relevant information from its technical reports in its report on the state of cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555. | |
| CRA | Art 33(2) | {Support measures for microenterprises and small and medium-sized enterprises, including start-ups} Member States may, where appropriate, establish cyber resilience regulatory sandboxes. Such regulatory sandboxes shall provide for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with this Regulation for a limited period of time before the placing on the market. The Commission and, where appropriate, ENISA, may provide technical support, advice and tools for the establishment and operation of regulatory sandboxes. /…/ | |
| CRA | Art 52(4) | {Market surveillance and control of products with digital elements in the Union market} Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated pursuant to Article 58 of Regulation (EU) 2019/881 and exchange information on a regular basis. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 14 of this Regulation, the designated market surveillance authorities shall cooperate and exchange information on a regular basis with the CSIRTs designated as coordinators and ENISA. | |
| CRA | Art 52(5) | {Market surveillance and control of products with digital elements in the Union market} The market surveillance authorities may request a CSIRT designated as coordinator or ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 54, market surveillance authorities may request the CSIRT designated as coordinator or ENISA to provide an analysis to support evaluations of compliance of products with digital elements. | |
| CRA | Art 52(10) | {Market surveillance and control of products with digital elements in the Union market} Market surveillance authorities may provide guidance and advice to economic operators on the implementation of this Regulation, with the support of the Commission and, where appropriate, CSIRTs and ENISA. | |
| CRA | Art 52(14) | {Market surveillance and control of products with digital elements in the Union market} For products with digital elements that fall within the scope of this Regulation which are classified as high-risk AI systems pursuant to [Article 6] of Regulation... [the AI Regulation], the market surveillance authorities designated for the purposes of Regulation... [the AI Regulation] shall be the authorities responsible for market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to Regulation... [the AI Regulation] shall cooperate, as appropriate, with the market surveillance authorities designated pursuant to this Regulation and, with respect to the supervision of the implementation of the reporting obligations pursuant to Article 14 of this Regulation, with the CSIRTs designated as coordinators and ENISA. /…/ | |
| CRA | Art 56(1) | {Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk} Where the Commission has sufficient reason to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk does not comply with the requirements laid down in this Regulation, it shall inform the relevant market surveillance authorities. | |

| | | | |
|---|---|---|---|
| CRA | Art 56(2) | {Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk} Where the Commission has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of non-technical risk factors, it shall inform the relevant market surveillance authorities and, where appropriate, the competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary. The Commission shall also consider the relevance of the identified risks for that product with digital elements in view of its tasks regarding the Union level coordinated security risk assessments of critical supply chains provided for in Article 22 of Directive (EU) 2022/2555, and consult as necessary the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and ENISA. | |
| CRA | Art 56(3) | {Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk} In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the product with digital elements referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission shall carry out an evaluation of compliance and may request ENISA to provide an analysis to support it. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA. | |
| CRA | Art 57(6) | {Compliant products with digital elements which present a significant cybersecurity risk} Where the Commission has sufficient reason to consider, including based on information provided by ENISA, that a product with digital elements, although compliant with this Regulation, presents the risks referred to in paragraph 1 of this Article, it shall inform and may request the relevant market surveillance authority or authorities to carry out an evaluation and follow the procedures referred to in Article 54 and paragraphs 1, 2 and 3 of this Article. | |
| CRA | Art 57(7) | {Compliant products with digital elements which present a significant cybersecurity risk} In circumstances which justify an immediate intervention to preserve the properfunctioning of the internal market and where the Commission has sufficient reason to consider that the product with digital elements referred to in paragraph 6 continues to present the risks referred to in paragraph 1, and no effective measures have been taken by the relevant national market surveillance authorities, the Commission shallcarry out an evaluation of the risks presented by that product with digital elements and may request ENISA to provide an analysis to support that evaluation and shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA | |
| CRA | Art 59(2) | {Joint activities of market surveillance authorities} The Commission or ENISA shall propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products with digital elements that fall within the scope of this Regulation with the requirements laid down in this Regulation. | |
| CRA | Art 60(3) | {Sweeps} Where, in the performance of its tasks, including based on the notifications received pursuant to Article 14(1) and (3), ENISA identifies categories of products with digital elements for which sweeps may be organised, it shall submit a proposal for a sweep to the coordinator referred to in paragraph 2 of this Article for the consideration of the market surveillance authorities. | |
| CSA | Art 5(1) | assisting and advising on the development and review of Union policy and law in the field of cybersecurity and on sector-specific policy and law initiatives where matters related to cybersecurity are involved, in particular by providing its independent opinion and analysis as well as carrying out preparatory work | |
| CSA | Art 6(1)f | [assisting] Union institutions in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation | |
| CSA | Art 6(1)e** | [assisting] Member States in developing national strategies on the security of network and information systems, where requested pursuant to Article 7(2) of Directive (EU) 2016/1148, and promote the dissemination of those strategies and | |

| | | | |
|---|---|---|---|
| | | note the progress in their implementation across the Union in order to promote best practices | |
| CSA | Art 6(1)e** | [assisting] Member States in developing national strategies on the security of network and information systems, where requested pursuant to Article 7(2) of Directive (EU) 2016/1148, and promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices | |
| CSA | Art 5(2) | assisting Member States to implement the Union policy and law regarding cybersecurity consistently, in particular in relation to Directive (EU) 2016/1148, including by means of issuing opinions, guidelines, providing advice and best practices on topics such as risk management, incident reporting and information sharing, as well as by facilitating the exchange of best practices between competent authorities in that regard; | |
| CSA | Art 5(3) | assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet; | |
| CSA | Art 5(4) | contributing to the work of the Cooperation Group pursuant to Article 11 of Directive (EU) 2016/1148, by providing its expertise and assistance; | |
| CSA | Art 5(5)b | [supporting] the promotion of an enhanced level of security of electronic communications, including by providing advice and expertise, as well as by facilitating the exchange of best practices between competent authorities | |
| CSA | Art 6(1)j | [assist] the Cooperation Group, in the exchange of best practices, in particular with regard to the identification by Member States of operators of essential services, pursuant to point (l) of Article 11(3) of Directive (EU) 2016/1148, including in relation to cross-border dependencies, regarding risks and incidents | |
| CSA | Art 6(2) | ENISA shall support information sharing in and between sectors, in particular in the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available tools, procedures, as well as on how to address regulatory issues related to information-sharing | |
| CSA | Art 9(c) | [ENISA shall] in cooperation with experts from Member States authorities and relevant stakeholders, provide advice, guidance and best practices for the security of network and information systems, in particular for the security of the infrastructures supporting the sectors listed in Annex II to Directive (EU) 2016/1148 and those used by the providers of the digital services listed in Annex III to that Directive; | |
| CSA | Art 6(1)h | [assist] Member States by regularly organising the cybersecurity exercises at Union level referred to in Article 7(5) on at least a biennial basis and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them | |
| CSA | Art 6(1)i | [assist] relevant public bodies by offering trainings regarding cybersecurity, where appropriate in cooperation with stakeholders | |
| CSA | Art 6(1)c* | [assist] Union institutions, bodies, offices and agencies […] to improve their capabilities to respond to such cyber threats and incidents, in particular through appropriate support for the CERT-EU | |
| CSA | Art 6(1)c* | [assist] Union institutions, bodies, offices and agencies in their efforts to improve the prevention, detection and analysis of cyber threats and incidents […], in particular through appropriate support for the CERT-EU | |
| CSA | Art 7(5) | ENISA shall regularly organise cybersecurity exercises at Union level, and shall support Member States and Union institutions, bodies, offices and agencies in organising cybersecurity exercises following their requests. Such cybersecurity exercises at Union level may include technical, operational or strategic elements. On a biennial basis, ENISA shall organise a large-scale comprehensive exercise. Where appropriate, ENISA shall also contribute to and help organise sectoral cybersecurity exercises together with relevant organisations that also participate in cybersecurity exercises at Union level | |

| | | | |
|---|---|---|---|
| CSA | Art 10(a) | [ENISA shall] raise public awareness of cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens, organisations and businesses, including cyber-hygiene and cyber-literacy | |
| CSA | Art 10(d) | [ENISA shall] support closer coordination and exchange of best practices among Member States on cybersecurity awareness and education. | |
| CSA | Art 10(b) | [ENISA shall] in cooperation with the Member States, Union institutions, bodies, offices and agencies and industry, organise regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate; | |
| CSA | Art 10(c) | [ENISA shall] assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education; | |
| CSA | Art 12(a) | [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] 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 | |
| CSA | Art 12(b) | [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] at the request of the Commission, facilitating the exchange of best practices | |
| CSA | Art 12(c) | [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] at the request of the Commission, providing it with expertise | |
| CSA | Art 12(d) | [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] providing advice and support to the Commission on matters concerning agreements for the mutual recognition of cybersecurity certificates with third countries, in collaboration with the ECCG established under Article 62 | |
| CSA | Art 6(1)b | [assist] Member States and Union institutions, bodies, offices and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis | |
| CSA | Art 7(1) | ENISA shall support operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders | |
| CSA | Art 7(2)a | ENISA shall cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies, including the CERT-EU, with the services dealing with cybercrime and with supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern.. | |
| CSA | Art 7(4)b* | [ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by] assisting, at the request of one or more Member States, [...] through the provision of expertise […] in particular by supporting the voluntary sharing of relevant information and technical solutions between Member States | |
| CSA | Art 7(3) | ENISA shall provide the secretariat of the CSIRTs network pursuant to Article 12(2) of Directive (EU) 2016/1148, and in that capacity shall actively support the information sharing and the cooperation among its members. | |
| CSA | Art 7(4) | ENISA and CERT-EU shall engage in structured cooperation to benefit from synergies and to avoid the duplication of activities [In performing tasks enlisted under Art 7(4) points a-d] | |
| CSA | Art 7(4)a* | [ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by] advising on how to improve their capabilities to prevent, detect and respond to incidents […]; | |

| | | | |
|---|---|---|---|
| CSA | Art 7(7)b | [ENISA shall contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity, mainly by] ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level | |
| CSA | Art 7(7)d | [ENISA shall contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity, mainly by] supporting Union institutions, bodies, offices and agencies and, at their request, Member States, in the public communication relating to such incidents or crises; | |
| CSA | Art 7(7)e | [ENISA shall contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity, mainly by] testing the cooperation plans for responding to such incidents or crises at Union level and, at their request, supporting Member States in testing such plans at national level | |
| CSA | Art 6(1)d | [assist] Member States in developing national CSIRTs, where requested pursuant to Article 9(5) of Directive (EU) 2016/1148 | |
| CSA | Art 6(1)g | [assist] national and Union CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices | |
| CSA | Art 5(6)a | [supporting the regular review of Union policy activities by preparing an annual report on the state of the implementation of the respective legal framework regarding] information on Member States' incident notifications provided by the single points of contact to the Cooperation Group pursuant to Article 10(3) of Directive (EU) 2016/1148 | |
| CSA | Art 5(6)b | [supporting the regular review of Union policy activities by preparing an annual report on the state of the implementation of the respective legal framework regarding] summaries of notifications of breach of security or loss of integrity received from trust service providers provided by the supervisory bodies to ENISA, pursuant to Article 19(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council | |
| CSA | Art 5(6)c | [supporting the regular review of Union policy activities by preparing an annual report on the state of the implementation of the respective legal framework regarding] notifications of security incidents transmitted by the providers of public electronic communications networks or of publicly available electronic communications services, provided by the competent authorities to ENISA, pursuant to Article 40 of Directive (EU) 2018/1972 | |
| CSA | Art 6(1)a | [assist] 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 | |
| CSA | Art 7(4)a* | [ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by] […], at the request of one or more Member States, providing advice in relation to a specific cyber threat | |
| CSA | Art 7(4)b* | [ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by] assisting, at the request of one or more Member States, in the assessment of incidents having a significant or substantial impact […] | |
| CSA | Art 7(4)c | [ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by] analyzing vulnerabilities and incidents on the basis of publicly available information or information provided voluntarily by Member States for that purpose | |
| CSA | Art 7(4)d | [ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by] at the request of one or more Member States, providing support in relation to ex-post technical inquiries regarding incidents having a significant or substantial impact within the meaning of Directive (EU) 2016/1148. | |
| CSA | Art 7(6) | ENISA, in close cooperation with the Member States, shall prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats based on | |

| | | | |
|---|---|---|---|
| | | publicly available information, its own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2016/1148, both on a voluntary basis, EC3 and CERT-EU. | |
| CSA | Art 7(7)a | [ENISA shall contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity, mainly by] aggregating and analysing reports from national sources that are in the public domain or shared on a voluntary basis with a view to contributing to the establishment of common situational awareness | |
| CSA | Art 9(b) | [ENISA shall] perform long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents | |
| CSA | Art 9(e) | [ENISA shall] collect and analyse publicly available information regarding significant incidents and compile reports with a view to providing guidance to citizens, organisations and businesses across the Union | |
| CSA | Art 7(4)b* | [ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by] […] assisting, at the request of one or more Member States, in […] facilitating the technical handling of such incidents | |
| CSA | Art 7(7)c | [ENISA shall contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity, mainly by] upon request, facilitating the technical handling of such incidents or crises, including, in particular, by supporting the voluntary sharing of technical solutions between Member State | |
| CSA | Art 8(1)a | [ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by] monitoring developments, on an ongoing basis, in related areas of standardisation and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to point (c) of Article 54(1) where standards are not available; | |
| CSA | Art 8(1)b | [ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by] preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services and ICT processes in accordance with Article 49; | |
| CSA | Art 8(1)c | [ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by] evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8); | |
| CSA | Art 8(1)d | [ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by] participating in peer reviews pursuant to Article 59(4); | |
| CSA | Art 8(1)e | [ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes, as established in Title III of this Regulation, by] assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5). | |
| CSA | Art 8(2) | ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group pursuant to Article 22(4). | |
| CSA | Art 8(3) | ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services and ICT processes, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way | |
| CSA | Art 8(4) | ENISA shall contribute to capacity-building related to evaluation and certification processes by compiling and issuing guidelines as well as by providing support to Member States at their request | |

| | | | |
|---|---|---|---|
| CSA | Art 48 | {Request for a European cybersecurity certification scheme} The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme. (2) In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. The Union rolling work programme shall be updated accordingly | |
| CSA | Art 49 | {Preparation, adoption and review of a European cybersecurity certification scheme} | |
| CSA | Art 49(1) | {Preparation, adoption and review of a European cybersecurity certification scheme} Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54. | |
| CSA | Art 49(2) | {Preparation, adoption and review of a European cybersecurity certification scheme} Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board. | |
| CSA | Art 49(3) | {Preparation, adoption and review of a European cybersecurity certification scheme} When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process. | |
| CSA | Art 49(4) | {Preparation, adoption and review of a European cybersecurity certification scheme} For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise. | |
| CSA | Art 49(5) | {Preparation, adoption and review of a European cybersecurity certification 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 shall adopt an opinion on the candidate scheme. | |
| CSA | Art 49(6) | {Preparation, adoption and review of a European cybersecurity certification scheme} ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme prepared in accordance with paragraphs 3, 4 and 5 to the Commission. The opinion of the ECCG shall not bind ENISA, nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission. | |
| CSA | Art 49(7) | {Preparation, adoption and review of a European cybersecurity certification scheme} The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes which meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2). | |
| CSA | Art 49(8) | {Preparation, adoption and review of a European cybersecurity certification scheme} At least every five years, ENISA shall evaluate each adopted European cybersecurity certification scheme, taking into account the feedback received from interested parties. If necessary, the Commission or the ECCG may request ENISA to start the process of developing a revised candidate scheme in accordance with Article 48 and this Article. | |
| CSA | Art 50 (1) | {Website on European cybersecurity certification schemes} ENISA shall maintain a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information provided in accordance with Article 55. | |
| CSA | Art 53(3) | {Conformity self-assessment} A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA. | |
| CSA | Art 58(7)g | {National cybersecurity certification authorities} [National cybersecurity certification authorities shall]: /…/ provide an annual summary report on the activities conducted under points (b), (c) and (d) of this paragraph or under paragraph 8 to ENISA and the ECCG; | |
| CSA | Art 59(4) | {Peer review} Peer review shall be carried out by at least two national cybersecurity certification authorities of other Member States and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review. | |

| | | | |
|---|---|---|---|
| CSA | Art 62(5) | {European Cybersecurity Certification Group} With the assistance of ENISA, the Commission shall chair the ECCG, and the Commission shall provide the ECCG with a secretariat in accordance with point (e) of Article 8(1) | |
| CSA | Art 5(5)a | [supporting] the development and implementation of Union policy in the field of electronic identity and trust services, in particular by providing advice and issuing technical guidelines, as well as by facilitating the exchange of best practices between competent authorities; | |
| CSA | Art 5(5)c | [supporting] Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy, including by providing advice to the European Data Protection Board upon request; | |
| CSA | Art 8(5) | ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services and ICT processes. | |
| CSA | Art 8(6)** | ENISA shall draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148 | |
| CSA | Art 8(6)** | ENISA shall draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148 | |
| CSA | Art 8(7) | ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union | |
| CSA | Art 9(a) | [ENISA shall] perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity | |
| CSA | Art 11(a) | [ENISA shall] advise the Union institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of cybersecurity, with a view to enabling effective responses to current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies, and with a view to using risk-prevention technologies effectively | |
| CSA | Art 11(b) | [ENISA shall] where the Commission has conferred the relevant powers on it, participate in the implementation phase of research and innovation funding programmes or as a beneficiary | |
| CSA | Art 11(c) | [ENISA shall] contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity | |
| CSA | Art 9(d) | [ENISA shall] through a dedicated portal, pool, organise and make available to the public information on cybersecurity provided by the Union institutions, bodies, offices and agencies and information on cybersecurity provided on a voluntary basis by Member States and private and public stakeholders; | |
| CSOA | Art 12(4) | {Coordinated preparedness testing of entities} For the purpose of supporting the coordinated preparedness testing of entities referred to in Article 11, point (a)(i), of this Regulation across the Union, the Commission shall, after consulting the NIS Cooperation Group, EU-CyCLONe and ENISA, identify the sectors or sub-sectors concerned from the sectors of high criticality listed in Annex I to Directive (EU) 2022/2555 for which a call for proposals to award grants may be issued. The participation of Member States in those calls for proposals is voluntary. | |
| CSOA | Art 12(6) | {Coordinated preparedness testing of entities} The NIS Cooperation Group in cooperation with the Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and ENISA, and, within the remit of its mandate, EU-CyCLONe, shall develop common risk scenarios and methodologies for the coordinated preparedness testing referred to in Article 11, point (a)(i), and, where appropriate, for other preparedness actions referred to in point (a)(ii) of that Article. | |

| | | | |
|---|---|---|---|
| CSOA | Art 6(4) | {Cooperation and information sharing within and between Cross-Border Cyber Hubs} Information sharing as referred to in paragraph 1 between Cross-Border Cyber Hubs shall be ensured by a high level of interoperability. To support such interoperability, ENISA shall, in close consultation with the Commission, without undue delay and in any event by 5 February 2026, issue interoperability guidelines specifying in particular information-sharing formats and protocols, taking into account international standards and best practices, as well as the functioning of any established Cross-Border Cyber Hubs. Interoperability requirements provided for in the cooperation agreements of Cross-Border Cyber Hubs shall be based on the guidelines issued by ENISA. | |
| CSOA | Art 9(4) | {Funding of the European Cybersecurity Alert System} The ECCC shall prepare, at least every 2 years, a mapping of the tools, infrastructure or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, and their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. When preparing the mapping, the ECCC shall consult the CSIRTs network, any existing Cross-Border Cyber Hubs, ENISA and the Commission | |
| CSOA | Art 12(6) | {Coordinated preparedness testing of entities} The NIS Cooperation Group in cooperation with the Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and ENISA, and, within the remit of its mandate, EU-CyCLONe, shall develop common risk scenarios and methodologies for the coordinated preparedness testing referred to in Article 11, point (a)(i), and, where appropriate, for other preparedness actions referred to in point (a)(ii) of that Article. | |
| CSOA | Art 21(1) | {European Cybersecurity Incident Review Mechanism} At the request of the Commission or EU-CyCLONe, ENISA shall, with the support of the CSIRTs network and with the approval of the Member States concerned, review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident and with the aim of drawing lessons learned to avoid or mitigate future incidents, ENISA shall deliver an incident review report to EU-CyCLONe, the CSIRTs network, the Member States concerned and the Commission to support them in carrying out their tasks, in particular the tasks set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where an incident has an impact on a DEP-associated third country, ENISA shall provide the report to the Council. In such cases, the Commission shall provide the report to the High Representative | |
| CSOA | Art 21(2) | {European Cybersecurity Incident Review Mechanism} To prepare the incident review report referred to in paragraph 1 of this Article, ENISA shall cooperate with and gather feedback from all relevant stakeholders, including representatives of Member States, the Commission, other relevant Union institutions, bodies, offices and agencies, industry, including managed security services providers, and users of cybersecurity services. Where appropriate, ENISA shall, in cooperation with CSIRTs and, where relevant, the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555, also cooperate with entities affected by significant cybersecurity incidents or large-scale cybersecurity incidents. Consulted representatives shall disclose any potential conflict of interest. | |
| CSOA | Art 21(3) | {European Cybersecurity Incident Review Mechanism} The incident review report referred to in paragraph 1 of this Article shall cover a review and analysis of the specific significant cybersecurity incident or large-scale cybersecurity incident, including the main causes, known exploitable vulnerabilities and lessons learned. ENISA shall ensure that the report complies with Union or national law concerning the protection of sensitive or classified information. If the relevant Member States or other users referred to in Article 14(3) that are affected by the incident so request, the data and information contained in the report shall be anonymised. It shall not include any details about actively exploited vulnerabilities that remain unpatched. | |
| CSOA | Art 21(4) | {European Cybersecurity Incident Review Mechanism} Where appropriate, the incident review report shall draw recommendations to improve the Union's cyber | |

| | | | |
|---|---|---|---|
| | | posture and may include best practices and lessons learned from relevant stakeholders. | |
| CSOA | Art 21(5) | {European Cybersecurity Incident Review Mechanism} ENISA may issue a publicly available version of the incident review report. That version of the report shall include only reliable public information, or other reliable information with the consent of the Member States concerned and, as regards information relating to a user as referred to in Article 14(3), point (b) or (c), with the consent of that user. | |
| CSOA | Art 10(4) | {Establishment of the Cybersecurity Emergency Mechanism} The actions under the Cybersecurity Emergency Mechanism shall be implemented primarily through the ECCC in accordance with Regulation (EU) 2021/887. However, actions implementing the EU Cybersecurity Reserve as referred to in Article 11, point (b), of this Regulation shall be implemented by the Commission and ENISA | |
| CSOA | Art 14(5) | {Establishment of the EU Cybersecurity Reserve} Without prejudice to the Commission's overall responsibility for the implementation of the EU Cybersecurity Reserve referred to in paragraph 4 of this Article and subject to a contribution agreement as defined in Article 2, point (19), of Regulation (EU, Euratom) 2024/2509, the Commission shall entrust the operation and administration of the EU Cybersecurity Reserve, in full or in part, to ENISA. Aspects not entrusted to ENISA shall remain subject to direct management by the Commission | |
| CSOA | Art 14(6) | {Establishment of the EU Cybersecurity Reserve} ENISA shall prepare, at least every 2 years, a mapping of the services needed by the users referred to in paragraph 3, points (a) and (b), of this Article. The mapping shall also include the availability of such services, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. In mapping that availability, ENISA shall assess the skills and capacity of the Union cybersecurity workforce relevant to the objectives of the EU Cybersecurity Reserve. When preparing the mapping, ENISA shall consult the NIS Cooperation Group, EU-CyCLONe, the Commission and, where applicable, the Interinstitutional Cybersecurity Board established pursuant to Article 10 of Regulation (EU, Euratom) 2023/2841 (IICB). In mapping the availability of services, ENISA shall also consult relevant cybersecurity industry stakeholders, including managed security service providers. ENISA shall prepare a similar mapping, after informing the Council and after consulting EU-CyCLONe, the Commission and, where relevant, the High Representative, to identify the needs of users referred to in paragraph 3, point (c), of this Article | |
| CSOA | Art 14(7) | {Establishment of the EU Cybersecurity Reserve} The Commission is empowered to adopt delegated acts in accordance with Article 23 to supplement this Regulation by specifying the types and the number of response services required for the EU Cybersecurity Reserve. When preparing those delegated acts, the Commission shall take into account the mapping referred to in paragraph 6 of this Article and may exchange advice and cooperate with the NIS Cooperation Group and ENISA. | |
| CSOA | Art 15(6) | {Requests for support from the EU Cybersecurity Reserve} ENISA, in cooperation with the Commission and EU-CyCLONe, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve. | |
| CSOA | Art 16(4) | {Implementation of the support from the EU Cybersecurity Reserve} To prioritise requests, in the case of concurrent requests from users referred to in Article 14(3), the criteria referred to in paragraph 3 of this Article shall be taken into account, where relevant, without prejudice to the principle of sincere cooperation between Member States and Union institutions, bodies, offices and agencies. Where two or more requests are assessed as equal under those criteria, higher priority shall be given to requests from Member State users. Where the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA pursuant to Article 14(5), ENISA and the Commission shall closely cooperate to prioritise requests in accordance with this paragraph | |
| CSOA | Art 16(6) | {Implementation of the support from the EU Cybersecurity Reserve} The agreements referred to in paragraph 5 shall be based on templates prepared by ENISA, after consulting Member States and, where appropriate, other users of the EU Cybersecurity Reserve. | |

| | | | |
|---|---|---|---|
| CSOA | Art 16(7) | {Implementation of the support from the EU Cybersecurity Reserve} The Commission, ENISA and the users of the EU Cybersecurity Reserve shall bear no contractual liability for damage caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve. | |
| CSOA | Art 16(9)a | {Implementation of the support from the EU Cybersecurity Reserve} Within 2 months of the end of a support, users that have received support shall provide a summary report about the service provided, the results achieved and the lessons learned, to: (a) the Commission, ENISA, the CSIRTs network and EU-CyCLONe in the case of users referred to in Article 14(3), point (a); | |
| CSOA | Art 16(9)b | {Implementation of the support from the EU Cybersecurity Reserve} Within 2 months of the end of a support, users that have received support shall provide a summary report about the service provided, the results achieved and the lessons learned, to: (b) the Commission, ENISA and the IICB in the case of the user referred to in Article 14(3), point (b); [ | |
| CSOA | Art 16(9)c | {Implementation of the support from the EU Cybersecurity Reserve} Within 2 months of the end of a support, users that have received support shall provide a summary report about the service provided, the results achieved and the lessons learned, to: (c) the Commission in the case of users referred to in Article 14(3), point (c). | |
| CSOA | Art 16(10) | {Implementation of the support from the EU Cybersecurity Reserve} Where the operation and administration of the EU Cybersecurity Reserve has been entrusted, in full or in part, to ENISA pursuant to Article 14(5) of this Regulation, ENISA shall report to and consult the Commission on a regular basis in that respect. In that context, ENISA shall immediately send to the Commission any requests it receives from users referred to in Article 14(3), point (c), of this Regulation and, where required for the purposes of prioritisation under this Article, any requests it has received from users referred to in Article 14(3), point (a) or (b), of this Regulation. The obligations in this paragraph shall be without prejudice to Article 14 of Regulation (EU) 2019/881 | |
| CSOA | Art 19(2) | {Support to DEP-associated third countries} Within 3 months of the conclusion of the agreement referred to in paragraph 1 and in any event prior to receiving any support from the EU Cybersecurity Reserve, the DEP-associated third country shall provide to the Commission information about its cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant cybersecurity incidents or large-scale-equivalent cybersecurity incidents, as well as information on responsible national entities, including computer security incident response teams or equivalent entities, their capabilities and the resources allocated to them. The DEP-associated third country shall provide updates of that information on a regular basis and at least once a year. The Commission shall provide the High Representative and ENISA with that information for the purposes of facilitating the application of paragraph 11. | |
| CSOA | Art 19(11) | {Support to DEP-associated third countries} Upon receipt of a request for support under this Article, the Commission shall immediately inform the Council. The Commission shall keep the Council informed of the assessment of the request. The Commission shall also cooperate with the High Representative about the requests received and the implementation of the support granted to DEP-associated third countries from the EU Cybersecurity Reserve. Additionally, the Commission shall also take into account any views provided by ENISA in respect of those requests. | |
| CSOA | Art 22(1)b | {Amendments to Regulation (EU) 2021/694} The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council. However, the EU Cybersecurity Reserve shall be implemented by the Commission and, in accordance with Article 14(6) of Regulation (EU) 2025/38, by ENISA. | |
| CSOA | Art 22(4) | {Amendments to Regulation (EU) 2021/694} /…/ When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in accordance with Article 10 of this Regulation. The Commission and ENISA may also act as wholesaler, by buying, stocking | |

| | | | |
|---|---|---|---|
| | | and reselling or donating supplies and services, including rentals, to those third countries. By way of derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council (*5), the request from a single third country shall be sufficient to mandate the Commission or ENISA to act.<br><br>When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies, offices or agencies. The Commission and ENISA may also act as a wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies, offices or agencies. By way of derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509, a request from a single Union institution, body, office or agency shall be sufficient to mandate the Commission or ENISA to act. | |
| CSOA | Art 19 | {Amendments to Regulation (EU) 2021/694} With regard to actions supporting mutual assistance provided for in Article 18 of Regulation (EU) 2025/38, the ECCC shall inform the Commission and ENISA about Member States' requests for direct grants without a call for proposals. | |
| DEP | Art 6(2) | The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, technology and research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council with the exception of actions implementing the EU Cybersecurity Reserve, which shall be implemented by the Commission and, in accordance with Article 12(6) of Regulation (EU) .../... [insert reference to Cybersolidarity Act], by ENISA.' | |
| DEP | Art 14(2) | When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) .../... [Cyber Solidarity Act], the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in line with Article 10. The Commission and ENISA may also act as wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By derogation from Article 169(3) of Regulation (EU) .../... [FR Recast], the request from a single third country is sufficient to mandate the Commission or ENISA to act. | |
| DEP | Art 19 | [...] For actions specified in Article 10(1), point (c) of Regulation (EU) .../... [Cyber Solidarity Act], the ECCC shall inform the Commission and ENISA about Member States' requests for direct grants without a call for proposals. | |
| DGA | Art 29(1) | {European Data Innovation Board} The Commission shall establish a European Data Innovation Board in the form of an expert group, consisting of representatives of the competent authorities for data intermediation services and the competent authorities for the registration of data altruism organisations of all Member States, the EDPB, the EDPS, ENISA, the Commission, the EU SME Envoy or a representative appointed by the network of SME envoys, and other representatives of relevant bodies in specific sectors as well as bodies with specific expertise. [..] | |
| DORA | Art 15 | {Further harmonisation of ICT risk management tools, methods, processes and policies} The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards/.../ | |
| DORA | Art 16(3) | {Simplified ICT risk management framework} The ESAs shall, through the Joint Committee, in consultation with the ENISA, develop common draft regulatory technical standards /.../ | |
| DORA | Art 32(4)c | {Structure of the Oversight Framework} The Oversight Forum shall be composed of: /.../ the Executive Directors of each ESA and one representative from the Commission, from the ESRB, from ECB and from ENISA as observers | |
| DORA | Art 49(1) | {Financial cross-sector exercises, communication and cooperation} The ESAs, through the Joint Committee and in collaboration with competent authorities, resolution authorities as referred to in Article 3 of Directive 2014/59/EU, the ECB, the Single Resolution Board as regards information relating to entities falling under the scope of Regulation (EU) No 806/2014, the ESRB and ENISA, as appropriate, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across sectors. | |

| | | | |
|---|---|---|---|
| DORA | Art 18(4) | {Classification of ICT-related incidents and cyber threats} When developing the common draft regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2), as well as international standards, guidance and specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors. For the purposes of applying the criteria set out in Article 4(2), the ESAs shall duly consider the need for microenterprises and small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly. | |
| DORA | Art 18(3) | {Classification of ICT-related incidents and cyber threats} The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft regulatory technical standards | |
| DORA | Art 19(7) | {Reporting of major ICT-related incidents and voluntary notification of significant cyber threats} Following receipt of information in accordance with paragraph 6, EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority, shall assess whether the major ICT-related incident is relevant for competent authorities in other Member States. Following that assessment, EBA, ESMA or EIOPA shall, as soon as possible, notify relevant competent authorities in other Member States accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system. | |
| DORA | Art 20 | {Harmonisation of reporting content and templates} The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop: (a) common draft regulatory technical standards in order to: (i) establish the content of the reports for major ICT-related incidents in order to reflect the criteria laid down in Article 18(1) and incorporate further elements, such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident or not; (ii) determine the time limits for the initial notification and for each report referred to in Article 19(4); (iii) establish the content of the notification for significant cyber threats.When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, specificities of financial sectors, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to this Regulation and to Directive (EU) 2022/2555. The ESAs shall, as applicable, provide justification when deviating from the approaches taken in the context of that Directive; (b) common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat. | |
| DORA | Art 21(1) | {Centralisation of reporting of major ICT-related incidents} The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities | |
| DORA | Art 34(3) | {Operational coordination between Lead Overseers} […] The Lead Overseers may, on an ad-hoc basis, call on the ECB and ENISA to provide technical advice, share hands-on experience or join specific coordination meetings of the JON. | |
| ECCC | Art 3(2) | {Mission of the Competence Centre and the Network} The Competence Centre and the Network shall undertake their tasks in collaboration with ENISA and the Community, as appropriate. | |
| ECCC | Art 5(2)b&c | {Tasks of the Competence Centre} Through the Agenda and the multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and the Digital Europe Programme /…/ ensuring synergies between and cooperation with relevant Union institutions, bodies, offices and agencies, in particular ENISA, while avoiding any duplication of activities with those Union institutions, bodies, offices and agencies; | |

| | | | |
|---|---|---|---|
| ECCC | Art 7(1)g | {Tasks of the national coordination centres} without prejudice to the competences of Member States for education and taking into account the relevant tasks of ENISA, engaging with national authorities regarding possible contributions to promoting and disseminating cybersecurity educational programmes; | |
| ECCC | Art 8 | {The Cybersecurity Competence Community} The Community shall consist of industry, including SMEs, academic and research organisations, other relevant civil society associations as well as, as appropriate, relevant European Standardisation Organisations, public entities and other entities dealing with cybersecurity operational and technical matters and, where relevant, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges. The Community shall bring together the main stakeholders with regard to cybersecurity technological, industrial, academic and research capacities in the Union. It shall involve national coordination centres, European Digital Innovation Hubs, where relevant, as well as Union institutions, bodies, offices and agencies with relevant expertise, such as ENISA. | |
| ECCC | Art 10(1) | {Cooperation of the Competence Centre with other Union institutions, bodies, offices and agencies and international organisations} To ensure consistency and complementarity while avoiding any duplication of effort, the Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies, including ENISA, the European External Action Service, the Directorate-General Joint Research Centre of the Commission, the European Research Executive Agency, the European Research Council Executive Agency and the European Health and Digital Executive Agency established by Commission Implementing Decision (EU) 2021/173 (13), relevant European Digital Innovation Hubs, the European Cybercrime Centre at the European Union Agency for Law Enforcement Cooperation established by Regulation (EU) 2016/794 of the European Parliament and of the Council (14), the European Defence Agency in relation to the tasks set out in Article 5 of this Regulation and other relevant Union entities. | |
| ECCC | Art 13(4) | {Tasks of the Governing Board} Regarding the decisions set out in points (a), (b) and (c) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, in accordance with the rules of procedure of the Governing Board | |
| ECCC | Art 18(5) | {Strategic Advisory Group} Representatives of the Commission and of other Union institutions, bodies, offices and agencies, in particular ENISA, may be invited by the Strategic Advisory Group to participate in and support its work. | |
| ECCC | Art 12(7) | {Composition of the Governing Board} A representative from ENISA shall be a permanent observer in the Governing Board. The Governing Board may invite a representative from the Strategic Advisory Group to attend its meetings | |
| eIDAS2 | Art 46(c)(2) | {Single points of contact} Each single point of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other competent authorities within its Member State. | |
| eIDAS2 | Art 46(e)(4) | {The European Digital Identity Cooperation Group} ENISA shall be invited to participate as observer in the workings of the Cooperation Group when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity certificates or standards are addressed. | |
| eIDAS2 | Art 47(e)(5)(c)(iv) | {The European Digital Identity Cooperation Group} [...] with the support of ENISA, exchange views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services; | |
| NCSS | Art 4(2) | {Competent authority} Member States shall, without delay, notify the Commission, ACER, ENISA, the NIS Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and the Electricity Coordination Group set up under Article 1 of Commission Decision of 15 November 2012 ( 17) and communicate to them the name and the contact details of their competent authority designated pursuant to paragraph 1 of this article and any subsequent changes thereto. | |

| | | | |
|---|---|---|---|
| NCSS | Art 4(3) | {Competent authority} [..] The competent authority shall communicate the name, contact details, assigned tasks and any subsequent changes thereto of the authorities to whom a task has been delegated to the Commission, to ACER, to the Electricity Coordination Group, to ENISA and to the NIS Cooperation Group. | |
| NCSS | Art 8(3) | {Terms and conditions or methodologies or plans} ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 6(2). | |
| NCSS | Art 9 (1) | {Consultation} TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall consult stakeholders, including ACER, ENISA and the competent authority of each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 6(2) and for plans referred to in Article 6(3). The consultation shall last for a period of not less than one month. | |
| NCSS | Art 12 (1) | {Monitoring} [...] In carrying out this monitoring, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group and the NIS Cooperation Group on the implementation of this Regulation. | |
| NCSS | Art 12 (3) | {Monitoring} By 13 June 2025, ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for the monitoring purposes as well as the process and frequency for the collection, based on the performance indicators defined in accordance with paragraph 5. | |
| NCSS | Art 12 (5) | {Monitoring} ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are related to cybersecurity aspects of cross-border electricity flows. | |
| NCSS | Art 13 (1) | {Benchmarking} By 13 June 2025, ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. […] | |
| NCSS | Art 13 (5) | {Benchmarking} Without prejudice to the confidentiality requirements in Article 47 and to the need to protect the security of entities subject to the provisions of this Regulation, the benchmarking analysis referred in paragraphs 2 and 3 of this Article shall be shared with all NRAs, all competent authorities, ACER, ENISA and the Commission. | |
| NCSS | Art 16 (1) n | {Cooperation between the ENTSO for Electricity and the EU DSO Entity} development of guidelines for the implementation of this Regulation in consultation with ACER and ENISA. | |
| NCSS | Art 16 (3) | {Cooperation between the ENTSO for Electricity and the EU DSO Entity} The ENTSO for Electricity and the EU DSO entity shall regularly inform ACER, ENISA, the NIS Cooperation Group and the Electricity Coordination Group on the progress in implementing the Union-wide and regional cybersecurity risk assessments pursuant to Article 19 and Article 21. | |
| NCSS | Art 17 (2) | {Cooperation between ACER and the competent authorities} The cooperation between ACER, ENISA and each competent authority may take the form of a cybersecurity risk monitoring body. | |
| NCSS | Art 19 (5) | {Union-wide cybersecurity risk assessment} Within three months after receipt of ACER's opinion, the ENTSO for Electricity, in cooperation with the EU DSO entity shall notify the final Union-wide cybersecurity risk assessment report to ACER, the Commission, ENISA and the competent authorities. | |
| NCSS | Art 34(1) | {Mapping matrix for electricity cybersecurity controls against standards} Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity and in consultation with ENISA, shall develop a proposal for a matrix to map the controls set out in Article 28(1), points (a) and (b) against selected European and international standards as well as relevant technical specifications ('the mapping matrix'). | |

| | | | |
|---|---|---|---|
| NCSS | Art 34(3) | {Mapping matrix for electricity cybersecurity controls against standards} Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity and in consultation with ENISA, shall propose an amendment to the competent authority for mapping matrix. | |
| NCSS | Art 36(2) | {Guidance on use of European cybersecurity certification schemes for procurement of ICT products, ICT services and ICT processes} The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall closely cooperate with ENISA in providing the sector-specific guidance included in non-binding cybersecurity procurement recommendations pursuant to paragraph 1. | |
| NCSS | Art 38(2) | {Each high-impact and critical-impact entity shall:establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), CSOC capabilities…} ENISA may issue non-binding guidance on establishing such capabilities or subcontracting the service to MSSPs, as part of the task defined in Article 6(2) of Regulation (EU) 2019/881. | |
| NCSS | Art 41(1) | {Cybersecurity crisis management and response plans} Within 24 months after the notification to ACER of the Union-wide risk assessment report, ACER shall in close cooperation with ENISA, the ENTSO for Electricity, the EU DSO entity, CS-NCAs, competent authorities, RP-NCAs, the NRAs and the NIS national cyber crisis management authorities, develop a Union-level cybersecurity crisis management and response plan for the electricity sector. | |
| NCSS | Art 42(1) | {Cybersecurity early alert capabilities for the electricity sector} The competent authorities shall cooperate with ENISA to develop Electricity Cybersecurity Early Alert Capabilities (ECEAC) as part as the assistance to Member States pursuant to Articles 6(2) and (7) of Regulation (EU) 2019/881. | |
| NCSS | Art 42(2) c | {Cybersecurity early alert capabilities for the electricity sector} […] assess the information ENISA has access to for identifying cyber risk conditions and relevant indicators for aspects of cross-border electricity flows | |
| NCSS | Art 47(7) | {Confidentiality of information} ACER, after consulting ENISA, all competent authorities, ENTSO for Electricity and the EU-DSO Entity, shall by 13 June 2025issue guidelines addressing mechanisms for all entities listed in Article 2(1) to exchange information, and in particular envisaged communication flows, and methods to anonymise and to aggregate information for the purpose of implementation of this Article. | |
| NCSS | Art 43(5) | {Cybersecurity exercises at entity and Member State levels} By 31 December 2026, and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall make available an exercise scenario template to perform the cybersecurity exercises at entity and Member State level referred to in paragraphs 1. This template shall take into account the results of the most recently performed cybersecurity risk assessment at entity and Member State levels and shall include key success criteria. The ENTSO for Electricity and the EU DSO entity shall involve ACER and ENISA in the development of such template. | |
| NCSS | Art 44(2) | {Regional or cross regional cybersecurity exercises} ENISA shall support the ENTSO for Electricity and the EU DSO entity in the preparation and organisation of the cybersecurity exercise at regional or at cross-regional level. | |
| NCSS | Art 44(6) | {Regional or cross regional cybersecurity exercises} The ENTSO for Electricity shall consult the Commission and may seek advice from ACER, ENISA and the Joint Research Centre on the organisation and execution of the regional and cross regional cybersecurity exercises. | |
| NCSS | Art 45(2) | {Outcome of cybersecurity exercises at entity, Member State, regional or cross regional levels} The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1), with the advice of ENISA if requested by them and pursuant to Article 7(5) of Regulation (EU) 2019/881, shall analyse and finalise the relevant cybersecurity exercise through a report summarising the lessons, addressed to all participants. | |

| | | | |
|---|---|---|---|
| NCSS | Art 42(3) | {Cybersecurity early alert capabilities for the electricity sector} The CSIRTs shall disseminate the information received from ENISA to the entities concerned without delay, within their tasks defined in Article 11(3), point (b) of Directive (EU) 2022/2555. | |
| NCSS | Art 42(4) | {Cybersecurity early alert capabilities for the electricity sector} ACER shall monitor the effectiveness of the ECEAC. ENISA shall assist ACER by providing all necessary information, pursuant to Articles 6(2) and 7(1) of Regulation (EU) 2019/881. | |
| NCSS | Art 37(1)(g) | {Rules on information sharing} If a competent authority receives information related to a reportable cyber-attack, that competent authority: /…/ shall share with ENISA a summary report, after anonymisation and removal of business secrets, with the information of the cyber-attack. | |
| NCSS | Art 37(2)(a) | {Rules on information sharing} If a CSIRT becomes aware of an unpatched actively exploited vulnerability, it shall:<br>(a) share it with ENISA via an appropriate secure information exchange channel without delay, unless otherwise specified in other Union law; | |
| NCSS | Art 37(8) | {Rules on information sharing} The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall develop a cyber-attack classification scale methodology by 13 June 2025. The TSOs, with the assistance of the ENTSO for Electricity and the EU DSO entity may request the competent authorities to consult ENISA and their competent authorities responsible for cybersecurity for assistance in the development of such classification scale. | |
| NCSS | Art 37(11) (a) | {Feasibility study to assess the possibility and the financial costs necessary to develop a common tool enabling all entities to share information with relevant national authorities} The ENTSO for Electricity, in cooperation with the EU DSO entity, shall: /.../ consult ENISA and the NIS Cooperation Group, the national single points of contact and the representatives of main stakeholders when assessing the feasibility; | |
| NIS2 | Art 7(4) | {National cybersecurity strategy} Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive | |
| NIS2 | Art 18(1)* | {Report on the state of cybersecurity in the Union} ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine readable data […] | |
| NIS2 | Art 18(1)d* | {Report on the state of cybersecurity in the Union} […] [The report shall, inter alia […] include] an aggregated assessment of the outcome of the peer reviews referred to in Article 19 | |
| NIS2 | Art 18(1)e* | {Report on the state of cybersecurity in the Union} […] [The report shall, inter alia […] include] an aggregated assessment […] as of the extent to which the Member States' national cybersecurity strategies are aligned | |
| NIS2 | Art 18(2)* | {Report on the state of cybersecurity in the Union} The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union […] | |
| NIS2 | Art 18(3) | {Report on the state of cybersecurity in the Union} ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e). | |
| NIS2 | Art 19(1) | {Peer reviews} The Cooperation Group shall, by 17 January 2025, establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level | |

| | | | |
|---|---|---|---|
| | | of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. | |
| NIS2 | Art 19(2) | {Peer reviews} /…/ The Commission and ENISA shall participate as observers in the peer reviews. | |
| NIS2 | Art 19(5) | {Peer reviews: self assessment} /…/ The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for the Member States' self-assessment. | |
| NIS2 | Art 19(6) | {Peer reviews: designated cybersecurity experts} /…/ The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts. | |
| NIS2 | Art 14(4)q | {Cooperation Group} to establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1), as well as to lay down the self-assessment methodology for Member States in accordance with Article 19(5), with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts in accordance with Article 19(6); | |
| NIS2 | Art 19(8) | {Peer reviews} Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State. | |
| NIS2 | Art 3(4) | {Essential and important entities} The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall without undue delay provide guidelines and templates regarding the obligations laid down in this paragraph. | |
| NIS2 | Art 8(4) | {Competent authorities and single points of contact} Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State. | |
| NIS2 | Art 18(1)e* | {Report on the state of cybersecurity in the Union} […] [The report shall, inter alia […] include] an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level […] | |
| NIS2 | Art 21(5) | {Cybersecurity risk-management measures} The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e) | |
| NIS2 | Art 22(1)** | {Union level coordinated security risk assessments of critical supply chains} The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors | |
| NIS2 | Art 22(2)** | {Union level coordinated security risk assessments of critical supply chains} The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1. | |
| NIS2 | Art 27(1) | {Registry of entities} ENISA shall create and maintain a registry of 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, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable. | |
| NIS2 | Art 27(4) | {Registry of entities} Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA. | |

| | | | |
|---|---|---|---|
| NIS2 | Art 29(5) | {Cybersecurity information-sharing arrangements} ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance. | |
| NIS2 | Art 18(1)b* | {Report on the state of cybersecurity in the Union} […] [The report shall, inter alia […] include] an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union | |
| NIS2 | Art 18(1)c* | {Report on the state of cybersecurity in the Union} […] [The report shall, inter alia […] include] an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises | |
| NIS2 | Art 10(10) | {Computer security incident response teams (CSIRTs)} Member States may request the assistance of ENISA in developing their CSIRTs. | |
| NIS2 | Art 12(2) | {Coordinated vulnerability disclosure and a European vulnerability database} ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include: … | |
| NIS2 | Art 15(2) | {CSIRTs network} ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs | |
| NIS2 | Art 16(2) | {European cyber crisis liaison organisation network (EU-CyCLONe)} ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information | |
| NIS2 | Art 14(3) | {Cooperation Group} The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. | |
| NIS2 | Art 18(1)a* | {Report on the state of cybersecurity in the Union} […] [The report shall, inter alia […] include] a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape; | |
| NIS2 | Art 18(2)* | {Report on the state of cybersecurity in the Union} The report shall include […] a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881 | |
| NIS2 | Art 23(6) | {Reporting obligations} Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident /…/ | |
| NIS2 | Art 23(9) | {Reporting obligations} The single point of contact shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received every six months. | |
| NIS2 | Art 37(1) | {Mutual assistance} [..]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 and ENISA. | |
| NIS2 | Art 24(3) | {Use of European cybersecurity certification schemes} Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881. | |

| | | | |
|---|---|---|---|
| NIS2 | Art 22(1)** | {Union level coordinated security risk assessments of critical supply chains} The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors | |
| NIS2 | Art 22(2)** | {Union level coordinated security risk assessments of critical supply chains} The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1. | |
| NIS2 | Art 25(2) | {Standardisation: technical specifications relevant to the security of network and information systems} ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered. | |
| REU | Art 21(8)* | {Reporting obligations} […] The summary report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555. | |
| REU | Art 13(7) | {CERT-EU mission and tasks} CERT-EU shall organise and may participate in cybersecurity exercises or recommend participation in existing exercises, where applicable in close cooperation with ENISA, to test the level of cybersecurity of the Union entities. | |
| REU | Art 13(5) | {CERT-EU mission and tasks} Within its competence, CERT-EU shall engage in structured cooperation with ENISA on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881 | |
| REU | Art 22(2) | {Incident response coordination and cooperation} CERT-EU, where relevant in close cooperation with ENISA, shall facilitate coordination among Union entities on incident response /…/ | |
| REU | Art 23(1) | {Management of major incidents} In order to support at operational level the coordinated management of major incidents affecting Union entities and to contribute to the regular exchange of relevant information among Union entities and with Member States, the IICB shall, pursuant to Article 11, point (q), establish a cyber crisis management plan based on the activities referred to in Article 22(2), in close cooperation with CERT-EU and ENISA. | |
| REU | Art 13(3)e | {CERT-EU mission and tasks} CERT-EU shall carry out the following tasks to assist the Union entities:: /…/ contribute to the Union cyber situational awareness in close cooperation with ENISA; | |
| REU | Art 21(8)* | {Reporting obligations} CERT-EU shall submit to the IICB, ENISA, the EU INTCEN and the CSIRTs network, every three months, a summary report including anonymised and aggregated data on significant incidents, incidents, cyber threats, near misses and vulnerabilities pursuant to Article 20 and significant incidents notified pursuant to paragraph 2 of this Article […] | |
| REU | Art 22 | {Incident response coordination and cooperation} CERT-EU, in close cooperation with ENISA, shall support Union entities regarding situational awareness of incidents, cyber threats, vulnerabilities and near misses as well as sharing relevant developments in the field of cybersecurity. | |
| REU | Art 5(1) | {Implementation of measures} By 8 September 2024, the Interinstitutional Cybersecurity Board established pursuant to Article 10 shall, after consulting the European Union Agency for Cybersecurity (ENISA) and after receiving guidance from CERT-EU, issue guidelines to Union entities for the purpose of carrying out an initial cybersecurity review and establishing an internal cybersecurity risk-management, governance and control framework pursuant to Article 6, carrying out cybersecurity maturity assessments pursuant to Article 7, taking cybersecurity risk-management measures pursuant to Article 8, and adopting the cybersecurity plan pursuant to Article 9 | |

| | | | |
|---|---|---|---|
| REU | Art 11(o) | {Tasks of the IICB} When exercising its responsibilities, the IICB shall, in particular: /…/ facilitate the establishment of an informal group of local cybersecurity officers of Union entities, supported by ENISA, with the aim of exchanging best practices and information in relation to the implementation of this Regulation; | |
| Blueprint | Art 14 | EU-CyCLONe, with the support of ENISA as its secretariat, should maintain an up-to-date list of national cyber crisis management authorities with contact details of EU-CyCLONe officers and executives, and make it available to EU-CyCLONe members. | |
| Blueprint | Art 18 | ENISA is the Union agency carrying out the tasks assigned under Regulation (EU) 2019/881 of the European Parliament and of the Council (11) for the purposes of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States and Union institutions, bodies and agencies. ENISA provides, among others, the secretariat for the CSIRTs network and EU-CyCLONe, situational awareness services, and assists Member States by regularly organising cybersecurity exercises at Union level. In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2024/2847 of the European Parliament and of the Council (12), ENISA receives information about significant cross-border incidents and actively exploited vulnerabilities and incidents affecting digital products. | |
| Blueprint | Art 25 | In order to enhance shared situational awareness and to facilitate assessment of the EU impact, EU-CyCLONe and the CSIRTs network with support of ENISA should use internally agreed reporting mechanism to produce an EU overview of technical and operational activities based on the information gathered at the national level | |
| Blueprint | Art 26 | EU-CyCLONe and the CSIRTs network should:<br>(a)cooperate to improve information sharing between the technical and operational level and situational awareness as a whole;<br>(b)continue to build a climate of trust between their members and between the networks;<br>(c)make full use of the available tools for information sharing, with support of ENISA, reflect on how to improve these tools and ensure interoperability between the networks. | |
| Blueprint | Art 28 | ENISA, as the secretariat for the CSIRTs network and EU-CyCLONe, has a central role in supporting Member States and Union institutions, bodies and agencies to achieve a common EU situational awareness on the technical and operational level to support preparing for large-scale cybersecurity incidents and crises. | |
| Blueprint | Art 29 | In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2019/881, Member States and relevant Union entities should coordinate with the private sector, including open-source communities and manufacturers, to improve information sharing. In particular ENISA should utilise its partnership programme in this regard. Additionally, Member States and relevant Union entities could also build on existing Information Sharing and Analysis Centres ('ISACs') at EU and national levels, to enhance cybersecurity capacity and to respond to cybersecurity incidents, including through joint meetings of the private sector with EU-CyCLONe or the CSIRTs network. | |
| Blueprint | Art 30 | To enhance information sharing within and between the networks, and to clarify mutual expectations for such sharing, EU-CyCLONe should, with the support of ENISA as secretariat and after consulting the CSIRTs network and the NIS Cooperation Group, within 24 months from adoption of this Recommendation, agree on a common aligned taxonomy of incident severity levels. This taxonomy should enable a comparison of the severity of incidents across Member States by considering the impact on service delivery, the number of affected entities and their respective relevance, the impact on other services and infrastructure, as well as the monetary, reputational and political damage inflicted. It should build on relevant existing scales or taxonomies, such as Reference Incident Classification Taxonomy. | |
| Blueprint | Art 36 | In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2024/2847, ENISA receives information about significant cross-border incidents and actively exploited vulnerabilities and incidents affecting digital products. ENISA acting as the secretariat should advise the CSIRTs network and EU-CyCLONe with the objective of supporting the networks in determining whether further actions should be taken and to contribute to the shared situational awareness. | |
| Blueprint | Art 40 | The Commission, in coordination with the High Representative, supported by ENISA, after consulting EU-CyCLONe and the CSIRTs network, should compile an efficient annual rolling programme of cyber exercises to prepare for cyber crises and to | |

| | | | |
|---|---|---|---|
| | | enhance organisational efficiency. The rolling programme of cyber exercises should take account of exercises of the UCPM and other Union-level crisis response mechanisms exercises, including the exercise outlined in the EU Critical Infrastructure Blueprint. The first rolling programme should be developed within 12 months after the adoption of the Cyber Blueprint, with subsequent programmes to be completed by 31 March of each year. The rolling programme should be submitted to the Council for information. | |
| Blueprint | Art 42 | ENISA, in its role of secretariat of the CSIRTs network and EU-CyCLONe, should ensure the systematic collection of lessons learnt from exercises, as well as the identification and proposing ways of implementation of resulting actions, to guarantee their effective execution and positive impact on the EU common resilience, including respective SOPs. | |
| Blueprint | Art 44 | The NIS Cooperation Group should invite the CSIRTs network, EU-CyCLONe and ENISA to present lessons learnt from the exercises, as well as the identification and proposed way of implementation of resulting actions. | |
| Blueprint | Art 45 | The Council may invite the chairs of the CSIRTs network, EU-CyCLONe, the NIS Cooperation Group and ENISA, to present how lessons learnt from the exercises were implemented. | |
| Blueprint | Art 46 | ENISA, in cooperation with the Commission and the High Representative, is invited to organise an exercise to test Cyber Blueprint during the next Cyber Europe exercise. The exercise should involve all relevant actors, including the political level. ENISA is invited to coordinate with the Presidency of the Council of the European Union the involvement of the political level. The exercise may also include the private sector and NATO. | |
| Blueprint | Art 55 | In the event of a large-scale cybersecurity incident or a cyber crisis, all actors and networks should respond in close coordination as follows:<br>(a)at the technical level:<br>i.The affected Member States and their CSIRTs should cooperate with the affected entities to respond to incidents and provide assistance, where applicable;<br>ii.The CSIRTs should cooperate through the CSIRTs network to share relevant technical information about the incident; the CSIRTs cooperate in their efforts to analyse the available technical artefacts and other technical information related to the incident with a view of determining the cause and possible technical mitigation measures;<br>iii.When a CSIRT or a Member State's cyber crisis management authority becomes aware of a significant incident, they are encouraged to share within the CSIRTs network or EU-CyCLONe.<br>iv.The CSIRTs network, with the support of ENISA, should prepare an aggregation of national reports provided by CSIRTs, which should be presented to EU-CyCLONe; | |
| Blueprint | Art 60 | For the purposes of preparing for large-scale cybersecurity incidents and cyber crises, Member States and, as appropriate, the Commission and CERT-EU, are invited to exchange on their communication efforts within EU-CyCLONe and the CSIRTs network, including best practices, such as advisories or awareness raising campaigns. ENISA should provide tools supporting such an exchange and ensuring an easy access | |
| Blueprint | Art 74 | A comprehensive list of lessons learnt from cyber crises or managed cybersecurity incidents in the past and best practices should be provided by EU-CyCLONe to the CSIRTs network, the NIS Cooperation Group, and the Council. ENISA should ensure that these lessons learnt are properly reflected in future preparedness activities and when considering the planning of future exercises. | |
| Blueprint | Art 80 | EU-CyCLONe, in cooperation with the CSIRT network and other main actors in the EU Cyber Crisis Management Ecosystem, supported by ENISA, should develop, within one year following the publication of the Recommendation, detailed process flow diagrams outlining the information flows between relevant actors, decision-making processes and reports developed during the management of large-scale cybersecurity incident or cyber crisis as described in this Recommendation. The flow diagrams should cover different cooperation modes and layers. They should be updated when necessary. | |

**CSA**: Cybersecurity Act - REGULATION (EU) 2019/881 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881)

**NIS2**: Directive on measures for a high common level of cybersecurity across the Union - DIRECTIVE (EU) 2022/2555 (https://eur-lex.europa.eu/eli/dir/2022/2555)

**CRA**: Cyber Resilience Act - 2024/2847 20.11.2024 REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847

**CSOA**: Cybersolidarity Act - 2025/38 15.1.2025 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) DEP: Digital Europe Programme - Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847

**ECCC**: Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres - REGULATION (EU) 2021/887 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0887)

**REU**: Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union - REGULATION (EU, Euratom) 2023/2841 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302841)

**AIA**: AI Act - Regulation laying down harmonised rules on artifitial intelligence and amending certain union legislative acts - REGULATION (EU) 2024/XXXX (https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf) NB! NOT OFFICIAL JOURNAL VERSION!

**DORA**: Regulation on digital operational resilience for the financial sector - REGULATION (EU) 2022/2554 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554)

**NCSS**: Commission Delegated Regulation (EU) 2024/1366 - Electricity Network Code (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401366)

**eIDAS 2**: Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183)

**DGA**: Data Governance Act: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 ( https://eur-lex.europa.eu/eli/reg/2022/868/oj) electricity flows

**Blueprint** - C/2025/3445 20.6.2025 COUNCIL RECOMMENDATION 6 June 2025 on an EU blueprint for cyber crisis management (C/2025/3445) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202503445#enc_1

* - denotes responsible for only part of a legal provision

** - denotes shared responsibility of a same legal provision

XX-00-00-000-XX-X

## ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

**ENISA**
European Union Agency for Cybersecurity

**Athens Office**
Agamemnonos 14, Chalandri 15231, Attiki, Greece

**Heraklion Office**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000

# Draft Statement of Estimates 2027 (Budget 2027)

*European Union Agency for Cybersecurity*

**CONTENTS**



**1. GENERAL INTRODUCTION**

**Explanatory statement**

**Legal Basis:**

1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity)

**Reference acts**

1. Impact assesment submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', as part of the draft 'Cybersecurity Act' (COM(2017) 477 final)
2. ENISA Financial Rules adopted by the Management Board on 15 October 2019

**2. JUSTIFICATION OF MAIN HEADINGS**

**2.1 Revenue in 2027**

The 2027 total revenue amounts to € 27716493 and consists of a subsidy of € 27007607 from the General Budget of the European Union and EFTA countries' contributions € 708886
Subsidy from the Greek Government for the rent of the offices of ENISA in Greece is no longer available as rent is directly covered by Greece
On 21 December 2023 the Contribution Agreement between DG CONNECT and ENISA was signed with the purpose to provide ENISA with financial contribution to implement the 'Preparedness and Incident Response Support for Key Sectors' action under the Digital Europe Programme (DEP) which grants ENISA a total of € 20.000.000 for implementation of agreed actions during the period 2024-2026. Amount of € 16.000.000 has been received in February 2024 as the first instalment.
On 9 December 2024 the Contribution Agreement between DG CONNECT and ENISA was signed with the purpose to provide ENISA with financial contribution to conduct a feasibility study on single reporting platform under the Cyber Resilience Act that will inform the future steps of the platform development which grants ENISA a total of € 400.000 for implementation of agreed actions up to 31/07/2026. Amount of € 240.000 has been received in March 2025 as the first instalment.
On 19 December 2024 the Contribution Agreement between DG CONNECT and ENISA was signed with the purpose to provide ENISA with financial contribution to implement the 'Incident and Vulnerability Response Support and Reporting' action under the Digital Europe Programme (DEP) which grants ENISA a total of € 15.000.000 for implementation of agreed actions during the period 2025-2027. Amount of € 12.000.000 was received in May 2025 as the first instalment. On 3 July 2025 the 1st Addendum I-LC-03708221 was signed with the purpose to provide ENISA support on the implementation of the Cyber Resilience Act, notably actions related to the development and assessment of technical specifications and standards, and interplay with the European Cybersecurity Certification schemes, which grants ENISA an additional amount of € 250.000.

On 31 July 2025 the Contribution Agreement between DG CONNECT and ENISA was signed with the purpose to provide ENISA with financial contribution to implement the action "EU Cybersecurity Reserve" and the action "Cyber Situation and Analysis Centre" which grants ENISA a total of € 36.670.000 for the implementation of agreed actions during the period 2025-2028. Amount of € 12.223.333,33 has been received in September 2025 as the first installment.
On 8 December 2025 the Contribution Agreement between DG CONNECT and ENISA was signed with the purpose to provide ENISA with financial contribution to implement the action "European Cybersecurity Support Centre for hospitals and healthcare providers" which grants ENISA a total of € 6.000.000 for the implementation of the agreed actions over the period of 36 months. Amount of € 3.600.000 has been received in December 2025 as the first intallment.
ENISA has signed a few SLAs with other EU Agencies for provision of services where revenue is expected to reach € 170.000,00

**2.2 Expenditure in 2027**

The total forecasted expenditure is in balance with the total forecasted revenue.

**Title 1 - Staff**

The estimate of Title 1 costs is based on the Establishment Plan for 2027, which contains 83 Temporary Agent posts.
Total expenditure under Title 1 amounts to € 16.562.984

**Title 2 - Buildings, equipment and miscellaneous operating expenditure**

| | | |
|---|---|---|
| Total expenditure under Title 2 amounts to | € | 4.167.109 |

**Title 3 - Operational expenditure**

| | | |
|---|---|---|
| Operational expenditure is mainly related to the implementation of Work Programme 2027 and amounts to | € | 6.986.400 |

**Title 4 - Externally funded activities**

| | | |
|---|---|---|
| Expenditure under Title 4 amounts to | | p.m. |

# 3. STATEMENT OF REVENUE 2027

| Title | Heading | Voted Appropriations 2025 € | Amended Budget 2025 € | Voted Appropriations 2026 € | Draft Appropriations 2027 € | Remarks - budget 2027 |
|---|---|---|---|---|---|---|
| 1 | EUROPEAN COMMUNITIES SUBSIDY | 25.716.933 | 25.993.311 | 26.495.438 | 27.007.607 | Total subsidy of the European Communities |
| 2 | THIRD COUNTRIES CONTRIBUTION | 713.309 | 721.020 | 695.364 | 708.886 | Contributions from Third Countries. |
| 3 | OTHER CONTRIBUTIONS | p.m. | 28.063.333 | p.m. | p.m. | *Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA under the Digital Europe Programme (DEP), EUR 16.000.000 *Contribution Agreement of 09/12/2024 between DG CONNECT and ENISA for CRA single reporting platform, EUR 240.000. *Contribution Agreement of 19/12/2024 between DG CONNECT and ENISA under the Digital Europe Programme (DEP) on "Incident and Vulnerability Response Support and Reporting" and HAS assessment EUCC pilots, EUR 12.000.000 *Contribution Agreement of 31/07/2025 between DG CONNECT and ENISA on "EU Cybersecurity Reserve"and on "Cyber Situation and Analysis Centre", EUR 12.223.333,33 *Contribution agreement of 08/12/2025 on European Cybersecurity Support Center for hospitals and healthcare providers, EUR 3.600.000 *Other contribution agreements are at draft stage. |
| 4 | ADMINISTRATIVE OPERATIONS | p.m. | 60.000 | p.m. | p.m. | Other expected income from other operations including under SLAs with other EU Agencies. |
| | **GRAND TOTAL** | **26.430.242** | **54.837.664** | **27.190.802** | **27.716.493** | |

| Article Item | Heading | Voted Appropriations 2025 € | Amended Appropriations 2025 € | Voted Appropriations 2026 € | Draft Appropriations 2027 € | Remarks - budget 2027 |
|---|---|---|---|---|---|---|
| 1 | EUROPEAN COMMUNITIES SUBSIDY | | | | | |
| 10 | EUROPEAN COMMUNITIES SUBSIDY | | | | | |
| *100* | *European Communities subsidy* | 25.716.933 | 25.993.311 | 26.495.438 | 27.007.607 | Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security. |
| *100* | *European Communities subsidy - Expansion of Activities 3, 4, 5* | n/a | n/a | n/a | n/a | |
| | CHAPTER 10 | 25.716.933 | 25.993.311 | 26.495.438 | 27.007.607 | |
| | **TITLE 1** | **25.716.933** | **25.993.311** | **26.495.438** | **27.007.607** | |
| 2 | THIRD COUNTRIES CONTRIBUTION | | | | | |
| 20 | THIRD COUNTRIES CONTRIBUTION | | | | | |
| *200* | *Third Countries contribution* | 713.309 | 721.020 | 695.364 | 708.886 | Contributions from Associated Countries. |
| | CHAPTER 2 0 | 713.309 | 721.020 | 695.364 | 708.886 | |
| | **TITLE 2** | **713.309** | **721.020** | **695.364** | **708.886** | |
| 3 | OTHER CONTRIBUTIONS | | | | | |
| 30 | OTHER CONTRIBUTIONS | | | | | |
| *300* | *External funding under Contribution Agreement* | p.m. | 28.063.333 | p.m. | p.m. | *Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA under the Digital Europe Programme (DEP), EUR 16.000.000 *Contribution Agreement of 09/12/2024 between DG CONNECT and ENISA for CRA single reporting platform, EUR 240.000. *Contribution Agreement of 19/12/2024 between DG CONNECT and ENISA under the Digital Europe Programme (DEP) on "Incident and Vulnerability Response Support and Reporting" and HAS assessment EUCC pilots, EUR 12.000.000 *Contribution Agreement of 31/07/2025 between DG CONNECT and ENISA on "EU Cybersecurity Reserve"and on "Cyber Situation and Analysis Centre", EUR 12.223.333,33 *Contribution agreement of 08/12/2025 on European Cybersecurity Support Center for hospitals and healthcare providers, EUR 3.600.000 *Other contribution agreements are at draft stage. |
| | CHAPTER 30 | p.m. | 28.063.333 | p.m. | p.m. | |
| | **TITLE 3** | **p.m.** | **28.063.333** | **p.m.** | **p.m.** | |
| 4 | ADMINISTRATIVE OPERATIONS | | | | | |
| 40 | ADMINISTRATIVE OPERATIONS | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***400*** | ***Administrative Operations*** | | **p.m.** | **60.000** | **p.m.** | **p.m.** | Revenue from administrative operations including SLAs with other EU Agencies. Estimated amount for the year shall be € 174604 |
| | | **CHAPTER 40** | **p.m.** | **60.000** | **p.m.** | **p.m.** | * Assigned revenue may be included in the estimate of revenue and expenditure only for the amounts that are certain at the date of the establishment of the estimate (Art. 20(7) of the FFR) |
| | | **TITLE 4** | **p.m.** | **60.000** | **p.m.** | **p.m.** | |
| | | **GRAND TOTAL** | **26.430.242** | **54.837.664** | **27.190.802** | **27.716.493** | |

# 4. STATEMENT OF EXPENDITURE 2027

| Title | Heading | | Voted Appropriations 2025 € | Amended Appropriations 2025 € | Voted Appropriations 2026 € | Draft Appropriations 2027 € | Remarks - budget 2027 |
|---|---|---|---|---|---|---|---|
| **1** | **STAFF** | | **15.271.440** | **15.555.529** | **16.031.333** | **16.562.984** | Total funding for covering personnel costs. |
| **2** | **BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE** | | **4.159.348** | **4.159.348** | **4.290.159** | **4.167.109** | Total funding for covering general administrative costs. |
| **3** | **OPERATIONAL EXPENDITURE** | | **6.999.454** | **6.999.454** | **6.869.310** | **6.986.400** | Total funding for operational expenditures. |
| **4** | **EXTERNALLY FUNDED ACTIVITIES** | | **p.m.** | **28.123.333** | **p.m.** | **p.m.** | Total external funding such as contribution agreements and SLAs. |
| | | **GRAND TOTAL** | **26.430.242** | **54.837.664** | **27.190.802** | **27.716.493** | |
| **1** | **STAFF** | | | | | | |
| **11** | **STAFF IN ACTIVE EMPLOYMENT** | | | | | | |
| ***110*** | ***Staff holding a post provided for in the establishment plan*** | | | | | | |
| 1100 | Basic salaries | | 10.314.300 | 10.598.389 | 11.110.332 | 11.145.393 | Staff Regulations applicable to officials of the European Communities and in particular Articles 62 and 66 thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of permanent officials and Temporary Agents (TA). |
| | | Article 1 1 0 | 10.314.300 | 10.598.389 | 11.110.332 | 11.145.393 | |
| ***111*** | ***Other staff*** | | | | | | |
| 1110 | Contract Agents | | 2.428.441 | 2.428.441 | 2.615.195 | 2.968.130 | Conditions of employment of other servants of the European Communities and in particular Article 3 and Title III thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of Contract Agents (CA). |
| 1113 | Seconded National Experts (SNEs) | | 814.031 | 814.031 | 873.405 | 908.764 | This appropriation is intended to cover basic salaries and all benefits of SNEs. |
| | | Article 1 1 1 | 3.242.472 | 3.242.472 | 3.488.600 | 3.876.894 | |
| | | **CHAPTER 11** | **13.556.771** | **13.840.860** | **14.598.932** | **15.022.287** | |
| **12** | **RECRUITMENT/DEPARTURE EXPENDITURE** | | | | | | |
| ***120*** | ***Expenditure related to recruitment*** | | | | | | |
| 1201 | Recruitment and Departure expenditure | | 508.469 | 508.469 | 217.593 | 84.697 | This appropriation is intended to cover the travel expenses of staff (including members of their families), the installation allowances for staff obliged to change residence after taking up their duty, the removal costs of staff obliged to change residence after taking up duty, the costs of daily subsistance allowances as per Staff Regulations applicable to officials of the European Communities (SR) and in particular Articles 20 and 71 thereof and Articles 5, 6, 7, 9, 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants.<br>This appropriation is intended to cover expenditure related to recruitment, e.g. incurred for interviewing candidates, external selection committee members, screening applications and other related costs. |
| | | Article 1 2 0 | 508.469 | 508.469 | 217.593 | 84.697 | |
| | | **CHAPTER 1 2** | **508.469** | **508.469** | **217.593** | **84.697** | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **13** | **SOCIO-MEDICAL SERVICES AND TRAINING** | | | | | | |
| ***132*** | ***Staff Development*** | | | | | | |
| 1320 | Staff Development | | 450.000 | 450.000 | 343.000 | 460.000 | This appropriation is intended to cover the costs of language and other training needs as well as teambuilding and other staff development activities. |
| | | Article 1 3 2 | 450.000 | 450.000 | 343.000 | 460.000 | |
| ***133*** | ***Staff Welfare*** | | | | | | |
| 1332 | Staff Welfare | | 238.200 | 238.200 | 283.808 | 346.000 | This appropriation is intended to cover staff welfare measures such as the subsidy for the functioning of the School of European Education of Heraklion and other expenditure relevant to schooling & education of children of the Agency staff, health related activities to promote well-being of staff, other activities related to internal events, other welfare measures.<br>This appropriation is also intended to cover the costs of annual medical visits and inspections, occupational doctor services as well as pre-recruitment medical costs and other costs related to medical services. |
| | | Article 1 3 3 | 238.200 | 238.200 | 283.808 | 346.000 | |
| | | **CHAPTER 1 3** | **688.200** | **688.200** | **626.808** | **806.000** | |
| **14** | **TEMPORARY ASSISTANCE** | | | | | | |
| ***142*** | ***Temporary Assistance*** | | | | | | |
| 1420 | External Temporary Staffing | | 518.000 | 518.000 | 588.000 | 650.000 | This appropriation is intended to cover the costs of temporary assistance (trainees and interim services). |
| | | Article 1 4 2 | 518.000 | 518.000 | 588.000 | 650.000 | |
| | | **CHAPTER 1 4** | **518.000** | **518.000** | **588.000** | **650.000** | |
| | | **Total Title 1** | **15.271.440** | **15.555.529** | **16.031.333** | **16.562.984** | |
| **2** | **BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE** | | | | | | |
| **20** | **BUILDINGS AND ASSOCIATED COSTS** | | | | | | |
| ***200*** | **Buildings and associated costs** | | | | | | |
| 2001 | Building costs | | 1.081.300 | 1.081.300 | 1.061.957 | 1.192.942 | This appropriation is intended to cover various building related costs including the payment of rent for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces, utilities and insurance of the premises of the Agency, cleaning and maintenance of the premises used by the Agency, fitting-out of the premises and repairs in the buildings, costs of building surveillance as well as purchases and maintenance cost of equipment related to security and safety of the building and the staff, expenditure of acquiring technical equipment, as well as maintenance and services related to it, and other costs such as for example market survey costs for rent of buildings, costs of moving to and/or establishing new premises of the Agency and other handling costs. |
| | | Article 2 0 0 | 1.081.300 | 1.081.300 | 1.061.957 | 1.192.942 | |
| | | **CHAPTER 2 0** | **1.081.300** | **1.081.300** | **1.061.957** | **1.192.942** | |
| **22** | **CURRENT CORPORATE AND ADMINISTRATIVE EXPENDITURE** | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ***222*** | ***Consultancy and other outsourced services*** | | | | | | |
| 2220 | Consultancy and other outsourced services (incl. legal services) | | 612.000 | 612.000 | 317.258 | 290.000 | This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. financial, HR related, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy, etc. |
| | | Article 2 2 2 | 612.000 | 612.000 | 317.258 | 290.000 | |
| ***223*** | ***Corporate and Administrative Expenditures*** | | | | | | |
| 2230 | Corporate and Administrative Expenditures | | 75.000 | 75.000 | 19.600 | 26.000 | This appropriation is intended to cover corporate and administrative expenditure such as the costs of purchasing, leasing, and repairs of furniture, the costs of maintenance and repairs of transport equipment as well as insurance and fuel, the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions, the costs of office stationery and the purchase of office kitchen consumables, post office and special courrier costs, bank charges, interest paid and other financial and banking costs and other costs of corporate administrative nature. |
| | | Article 2 2 3 | 75.000 | 75.000 | 19.600 | 26.000 | |
| | | **CHAPTER 2 2** | **687.000** | **687.000** | **336.858** | **316.000** | |
| **23** | **ICT** | | | | | | |
| ***231*** | ***Core and Corporate ICT expenditure*** | | | | | | |
| 2312 | Core and corporate ICT costs | | 2.391.048 | 2.391.048 | 2.891.344 | 2.658.167 | This appropriation is intended to cover core and corporate ICT costs including recurrent corporate ICT costs (including support and consulting services) as well as new investments and one-off projects for hardware, software, services and maintenance as well as ENISA website and portals support and corporate cybersecurity aspects. |
| | | Article 2 3 1 | 2.391.048 | 2.391.048 | 2.891.344 | 2.658.167 | |
| | | **CHAPTER 2 3** | **2.391.048** | **2.391.048** | **2.891.344** | **2.658.167** | |
| | | **Total Title 2** | **4.159.348** | **4.159.348** | **4.290.159** | **4.167.109** | |
| **3** | **OPERATIONAL EXPENDITURE** | | | | | | |
| **30** | **ACTIVITIES RELATED TO OUTREACH AND MEETINGS** | | | | | | |
| ***300*** | ***Outreach, meetings and representation expenses*** | | | | | | |
| 3001 | Outreach, meetings, translations and representation expenses | | 768.800 | 768.800 | 643.615 | 619.400 | This appropriation is intended to cover costs of outreach activities (communications, stakeholders' management, publication and translations), meetings of statutory bodies (i.e. MB, AG, NLOs, and meetings with other stakeholders) and other representation costs. It also covers mission costs for the ED, COO, ACOO as well as missions related to the implementation of Activities 9-11 as defined in the SPD 2027-2029 mainly covering horizontal tasks and other administrative services. |
| 3002 | Operational missions | | 512.200 | 512.200 | 382.200 | 318.000 | This appropriation is intended to cover costs of operational missions related to the implementation of Activities 1-8 as defined in the SPD 2025-2027 related to performing operational tasks. |
| 3003 | Large scale operational events | | 255.000 | 255.000 | 264.600 | 224.000 | This appropriation is intended to cover costs of large scale operational events (>50 participants) related to the implementation of Activities 1-8 as defined in the SPD 2027-2029 related to performing operational tasks. |
| | | Article 3 0 0 | 1.536.000 | 1.536.000 | 1.290.415 | 1.161.400 | |
| | | **CHAPTER 3 0** | **1.536.000** | **1.536.000** | **1.290.415** | **1.161.400** | |
| **36** | **CORE OPERATIONAL ACTIVITIES** | | | | | | |
| ***361*** | ***Activity 1*** | | | | | | |
| 3610 | Activity 1 - Support for policy monitoring and development | | 294.037 | 294.037 | 267.295 | 300.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT). |
| | | Article 3 6 1 | 294.037 | 294.037 | 267.295 | 300.000 | |
| ***362*** | ***Activity 2*** | | | | | | |
| 3620 | Activity 2 - Cybersecurity and resilience of critical sectors | | 331.024 | 331.024 | 396.900 | 550.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT). |
| | | Article 3 6 2 | 331.024 | 331.024 | 396.900 | 550.000 | |
| ***363*** | ***Activity 3*** | | | | | | |
| 3630 | Activity 3 - Capacity building | | 691.409 | 691.409 | 541.940 | 612.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs). |
| | | Article 3 6 3 | 691.409 | 691.409 | 541.940 | 612.000 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***364*** | ***Activity 4*** | | | | | |
| 3640 | Activity 4 - Enabling operational cooperation | 1.537.091 | 1.537.091 | 1.888.950 | 2.025.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT). |
| | Article 3 6 4 | 1.537.091 | 1.537.091 | 1.888.950 | 2.025.000 | |
| ***365*** | ***Activity 5*** | | | | | |
| 3650 | Activity 5 - Provide effective operational cooperation through situational awareness | 1.476.118 | 1.476.118 | 1.274.000 | 1.340.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT). |
| | Article 3 6 5 | 1.476.118 | 1.476.118 | 1.274.000 | 1.340.000 | |
| ***366*** | ***Activity 6*** | | | | | |
| 3660 | Activity 6 - Provide services for operational assistance and support | p.m. | p.m. | p.m. | p.m. | This appropriation is intended to cover direct operational costs relevant to the Activity 6 (including operational ICT). |
| | Article 3 6 6 | p.m. | p.m. | p.m. | p.m. | |
| ***367*** | ***Activity 7*** | | | | | |
| 3670 | Activity 7 - Development and maintenance of EU cybersecurity certification framework | 570.089 | 570.089 | 631.610 | 540.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT). |
| | Article 3 6 7 | 570.089 | 570.089 | 631.610 | 540.000 | |
| ***368*** | ***Activity 8*** | | | | | |
| 3680 | Activity 8 - Supporting European cybersecurity market, research & development and industry | 563.687 | 563.687 | 578.200 | 458.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT). |
| | Article 3 6 8 | 563.687 | 563.687 | 578.200 | 458.000 | |
| | **CHAPTER 3 6** | **5.463.454** | **5.463.454** | **5.578.895** | **5.825.000** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **TITLE 3** | **6.999.454** | **6.999.454** | **6.869.310** | **6.986.400** | |
| **4** | **EXTERNALLY FUNDED ACTIVITIES *** | | | | | * The appropriations corresponding to assigned revenue shall be made available automatically, both as commitment appropriations and as payment appropriations, when the revenue has been received by the Union body (Art. 21(2) of the FFR) |
| **40** | **ACTIVITIES RELATED TO EXTERNALLY FUNDED PROJECTS** | | | | | |
| ***400*** | ***Implementation of externally EU funded projects*** | | | | | |
| 4000 | Activities related to the Contribution Agreement under DEP | p.m. | p.m. | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA with the purpose to implement the 'Preparedness and Incident Response Support for Key Sectors' action under the Digital Europe Programme (DEP).<br>This Contribution Agreement covers Support Action ex-ante/ex-post and SitCen (2024-2026). |
| 4001 | Operational activities related to the implementation of SLAs | n/a | 60.000 | p.m. | n/a | This appropriation is intended to cover costs of implementation of operational activities under the SLAs between ENISA and other EU Agencies. |
| 4002 | Administrative activities related to the implementation of SLAs | n/a | p.m. | p.m. | n/a | This appropriation is intended to cover costs of implementation of administrative activities under the SLAs between ENISA and other EU Agencies. |
| 4003 | Activities related to the Contribution Agreement for CRA | p.m. | 240.000 | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement of 09/12/2024 between DG CONNECT and ENISA with the purpose to conduct a feasibility study on single reporting platform under the Cyber Resilience Act with an estimated amount of EUR 400 000 which shall be implemented up to 31/07/2026. |
| 4004 | Activities related to the Contribution Agreement for Support Action, SitCen, and CRA-SRP | p.m. | 12.000.000 | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement of 19/12/2024 between DG CONNECT and ENISA with the purpose to implement the 'Incident and Vulnerability Response Support and Reporting' action under the Digital Europe Programme (DEP).<br>This Contribution Agreement covers Support Action incident response services, CRA SRP establishment and SitCen (2025-2027). |
| 4005 | Activities related to the Contribution Agreement for Cyber Reserve and SitCen | p.m. | 12.223.333 | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement of 31/07/2025 between DG CONNECT and ENISA with the purpose to implement the action "EU Cybersecurity Reserve" and the action "Cyber Situation and Analysis Centre" during the period 2025-2028. |
| 4006 | Activities related to the Contribution Agreement for HAP | p.m. | 3.600.000 | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement of 08/12/2025 between DG CONNECT and ENISA with the purpose to implement the action "European Cybersecurity Support Centre for hospitals and healthcare providers"; implementation period is 36 months. |
| 4007 | Activities related to the Contribution Agreement for Western Balkans | p.m. | p.m. | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for the Western Balkans which is currently in draft stage. |
| 4008 | Activities related to the Contribution Agreement for EUDI Wallet | p.m. | p.m. | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for the EUDI Wallet which is currently in draft stage. |
| 4009 | Activities related to the Contribution Agreement for 2026 CA1 | p.m. | p.m. | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the future Contribution Agreements. |
| 4010 | Activities related to the Contribution Agreement for 2026 CA2 | p.m. | p.m. | p.m. | p.m. | This appropriation is intended to cover costs of implementation of activities under the future Contribution Agreements. |
| | Article 4 0 0 | p.m. | 28.123.333 | p.m. | p.m. | |
| | **CHAPTER 4 0** | **p.m.** | **28.123.333** | **p.m.** | **p.m.** | |
| | **TITLE 4** | **p.m.** | **28.123.333** | **p.m.** | **p.m.** | |
| | **GRAND TOTAL** | **26.430.242** | **54.837.664** | **27.190.802** | **27.716.493** | |

European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

## Establishment Plan 2027

| Category and grade | Establishment plan as part of draft EU Budget 2026[1] | | Draft Establishment Plan 2027[2] | |
|---|---|---|---|---|
| | Off. | TA | Off. | TA |
| AD 16 | | | | |
| AD 15 | | 1 | | 1 |
| AD 14 | | | | |
| AD 13 | | 2 | | 2 |
| AD 12 | | 4 | | 4 |
| AD 11 | | 3 | | 3 |
| AD 10 | | 7 | | 7 |
| AD 9 | | 15 | | 15 |
| AD 8 | | 14 | | 14 |
| AD 7 | | 12 | | 13 |
| AD 6 | | 6 | | 6 |
| AD 5 | | | | |
| **Total AD** | | **64** | | **65** |
| AST 11 | | | | |
| AST 10 | | | | |
| AST 9 | | 2 | | 2 |
| AST 8 | | 1 | | 1 |
| AST 7 | | 4 | | 3 |
| AST 6 | | 7 | | 7 |
| AST 5 | | 4 | | 4 |
| AST 4 | | 1 | | 1 |
| AST 3 | | | | |
| AST 2 | | | | |
| AST 1 | | | | |
| **Total AST** | | **19** | | **18** |
| AST/SC1 | | | | |
| AST/SC2 | | | | |
| AST/SC3 | | | | |
| AST/SC4 | | | | |
| AST/SC5 | | | | |
| AST/SC6 | | | | |
| **Total AST/SC** | | | | |
| **TOTAL** | | **83** | | **83** |

[1] Draft (EU, Euratom) 2025 of the European Union's annual budget for the financial year 2026

[2] draft establishment plan 2027 includes changes foreseen in the MB decision 2025-17 modifying the 2025 establishment plan (A budget neutral change of one post from AST7 to AD7)