

MANAGEMENT BOARD DECISION

DECISION No MB/2025/18

OF THE ENISA MANAGEMENT BOARD

of 20 November 2025,

**on adopting the Single Programming Document (SPD) 2026-2028, the
statement of estimates for 2026 and the establishment plan for 2026**

THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

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., 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
- Commission Opinion No. C(2025) 7139 final on the draft Single Programming Document for 2026 – 2028 of ENISA dated 20 October 2025
- Commission Communication C(2014) 9641 final, on the guidelines for programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies dated 16.12.2014

Whereas

- (1) The Single Programming Document 2026-2028 should be adopted by the Management Board by 30 November 2025.
- (2) The Single Programming Document 2026-2028 was scrutinised by the Executive Board on 24 October 2025.
- (3) The Single Programming Document of the Agency should be forwarded to the Member States, the European Parliament, the Council and the Commission following adoption;

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2026-2028 is adopted as set out in the Annex 1 of this decision.

Article 2

The statement of estimates of revenue and expenditure for the financial year 2026 and the establishment plan 2026 is adopted as set-out in Annex 2 and Annex 3 of this decision. They shall become final following the definitive adoption of the general budget of the Union for the financial year 2026.

Article 3

Where necessary, the Management Board shall adjust ENISA's Single Programming Document 2026-2028 and ENISA's budget and the establishment plan in accordance with the general budget of the Union for the financial year 2026.

Article 4

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

Done in Athens, 20 November 2025

On behalf of the Management Board,

[signed]

Ms Fabienne Tegeler
Chair of the Management Board of ENISA



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2026-2028

Including Multiannual planning,
Work programme 2026 and
Multiannual staff planning

FINAL

TABLE OF CONTENTS

| | |
|---|-----------|
| Vertical objectives: | 7 |
| Strategic Objective: “Support for effective and consistent implementation of EU cybersecurity policies” | 7 |
| SECTION I. GENERAL CONTEXT | 9 |
| SECTION II. MULTI-ANNUAL PROGRAMMING 2026 – 2028 | 11 |
| 1. Multi-annual work programme | 11 |
| 2. HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2026-2028 | 13 |
| 2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION | 13 |
| 2.2 . OUTLOOK FOR THE YEARS 2026-2028 | 16 |
| 2.3 RESOURCE PROGRAMMING FOR THE YEARS 2026-2028 | 17 |
| 2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS | 19 |
| SECTION III. WORK PROGRAMME 2026 | 21 |
| 3.1 OPERATIONAL ACTIVITIES | 25 |
| 3.2 CORPORATE ACTIVITIES | 52 |
| ANNEX64 | |
| I. ORGANISATION CHART AS OF 01.01.2025 | 64 |
| II. RESOURCE ALLOCATION PER ACTIVITY 2026 - 2028 | 65 |
| III. FINANCIAL RESOURCES 2026 - 2028 | 67 |
| IV. HUMAN RESOURCES - QUANTITATIVE | 69 |
| V. HUMAN RESOURCES - QUALITATIVE | 75 |
| VI. ENVIRONMENT MANAGEMENT | 80 |
| VII. BUILDING POLICY | 81 |
| VIII. PRIVILEGES AND IMMUNITIES | 81 |
| IX. EVALUATIONS | 82 |
| X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS | 83 |
| XI. PLAN FOR GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENTS | 85 |
| XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS | 90 |
| XIII. ANNUAL COOPERATION PLAN 2026 | 90 |



| | |
|---|------------|
| XIV. PROCUREMENT PLAN 2026 | 90 |
| XV. ENISA STATUTORY OPERATIONAL TASKS FROM EU LEGISLATION 2024 | 92 |
| XVI. CORPORATE STRATEGY GOALS AND INDICATORS | 115 |

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 | Computer Emergency Response Team for EU institutions, bodies 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 | Cyber Crisis Liaison Organisation Network |
| -Ne | |
| 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

As we embark on the next phase of our journey to enhance the maturity and resilience of cybersecurity in the European Union, I am pleased to introduce the Single Programming Document (SPD) for 2026-2028.

This SPD outlines the steps that the European Union Agency for Cybersecurity (ENISA) will take to support the implementation of key EU cybersecurity policies, including the Cybersecurity Act, the NIS2 Directive, the Cyber Resilience Act, EU Blueprint for Cyber Crisis Management, the Cyber Solidarity Act, the EU Action Plan for the Cybersecurity of Hospitals and Health Providers and the Digital Omnibus. These will shape and inform the actions that will be undertaken in 2026 and beyond.

Firstly, this SPD outlines the commitment to continue our work to support EU Member States in their pursuits to enhance cybersecurity. ENISA will focus its effort on supporting EU Member States to implement key legislation such as NIS2 Directive, the Cyber Resilience Act and policies by serving as a centre of expertise both collecting and providing independent, high quality technical advice and assistance.

Secondly, ENISA will build on our existing capabilities and capacities, leveraging our expertise and partnerships to drive progress in areas where the Agency itself needs to implement key priorities. In cybersecurity certification, vulnerability reporting and management, and crisis management to name but a few. The launch of the Single Reporting Platform in September 2026 will be a significant deliverable of the Agency, a global first for vulnerability management. Moreover, the administration and operation of the EU Cybersecurity Reserve puts ENISA in the limelight as a dependable partner to the cybersecurity community in the EU.

Finally, the Agency welcomes the recently proposed Digital Omnibus and the revision of the Cybersecurity Act and in 2026, the Agency will work with our partners to ensure the final provisions will contribute to a trusted and secure single market.

I am proud of the progress we have made so far, and I am confident that the work outlined in this SPD will help us achieve our goals. I would like to thank our partners, stakeholders, and team members for their hard work and dedication to our mission. Together, we can break new ground towards an even more cyber secure digital single market that meets the challenges of today and tomorrow.

Juhan Lepassaar

Executive Director



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

The Single Programming Document sets out the activities that ENISA will undertake in the years 2026 to 2028 in accordance with the Agency's Regulation (EU) 2019/881 on ENISA (Cybersecurity Act)¹ and takes into account the new ENISA Strategy, the transposition of the NIS2 Directive, the Cyber Resilience Act (CRA), Cyber Solidarity Act (CSoA) among other legislative acts and regulations.

During the course of 2025 the Agency achieved a number of significant milestones that are expected to drive and shape the 2026 work programme, including developments in the cybersecurity landscape.

These include:

Revised Blueprint for Cyber Crisis Management: The Council of the EU adopted a revised Blueprint, which ENISA will support through its expertise and exercises. The revised Blueprint aims to strengthen the response to large-scale cyber incidents and crises in the EU. ENISA will work with the European Commission and Member States to implement the revised Blueprint, providing support and expertise as needed.

European Vulnerability Database: ENISA launched the European Vulnerability Database, providing aggregated and actionable information on cybersecurity vulnerabilities. The database will help to enhance situational awareness and support the identification of potential vulnerabilities. ENISA will continue to develop and improve the database, gathering feedback from users and stakeholders to ensure that it meets their needs.

EU Action Plan for Cybersecurity of Hospitals and Healthcare Providers: ENISA welcomed the proposed Action Plan and is committed to collaborating with the European Commission and Member States to strengthen the sector's digital infrastructure. The Action Plan proposes the establishment of a pan-European Cybersecurity Support Centre for hospitals and healthcare providers. ENISA will work with the European Commission and Member States to implement the Action Plan, providing expertise and support as needed to enhance the cybersecurity of hospitals and healthcare providers as part of ENISA's support for all NIS2 via the Resilience of Critical Sectors Unit (activity 2)

Certification: 2025 marked the full entry into force of the EUCC, the very first European cybersecurity scheme adopted, with the celebration of the first EUCC notified Conformity Assessment Bodies (CABs) and of the first certificates, as well as the adoption of a first amendment of the scheme. This significant landmark in the certification field is paving the way for certified products, and for the maintenance of certification schemes. Also, EUCC certification being a possible option for ensuring conformity of digital products to the CRA, ENISA launched pilots with industry on EUCC-CRA mapping. In the coming year, ENISA will develop the new EUDI wallet and MSS schemes according to received requests, with first versions foreseen to be available from 2026, and will ensure the maintenance of the full certification framework, enlarging where necessary the scope of these schemes. In addition, work is ongoing for the finalisation and delivery of EUCS and EU5G.

EU Cybersecurity Reserve: ENISA signed a contribution agreement with the European Commission to administer and operate the EU Cybersecurity Reserve, in order to provide incident response support services to Member States, Union entities and, conditionally, DEP-associated third countries. The Reserve will provide pre-committed services that can be converted into preparedness services related to incident prevention and response. ENISA will procure services for the Reserve and assess requests from Member States' cyber crisis management authorities and/or CSIRTs. The Reserve is expected to be fully operational by the end of 2025. ENISA will continue to work with the European Commission and Member States to finalize the operational details of the Reserve and ensure its successful launch.

Additional Contribution Agreements: At the end of 2024 the Agency and DG CNECT signed a €15.25 million agreement for the establishment, management of the CRA Single Reporting Platform and the continuation of the Support Action. Moreover, three additional contribution agreements are expected to be signed with the European Commission by the end of 2025. These agreements will provide funding for specific projects and initiatives that support the Agency's mandate. ENISA will finalize the negotiations and sign the agreements, ensuring that the projects and initiatives are properly funded and can be implemented effectively.

Other non-legislative policy developments include Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures for which ENISA is a member of the expert group of national authorities created under the

¹ Regulation (EU) 2019/881

Recommendation and the EU Action Plan on Cable Security and Commission Recommendation on submarine cables that was adopted as a follow-up to the Nevers Call of 9 March 2022. In addition, ENISA continues to support the adoption of the European Cybersecurity Skills Framework and its role in facilitating a European professional attestation scheme.

Advisory Group: ENISA selected 26 experts to form a new Advisory Group, which will advise on the Agency's tasks and provide input on the annual work programme. The Advisory Group will play a crucial role in ensuring that ENISA's work is aligned with the needs of its stakeholders. The Advisory Group will hold its first meeting Q4 2025, where it will discuss its work programme and priorities for the next two and a half years.

Strengthening ENISA IT Infrastructure: The single programming document 2026-2028 takes into account the actions needed to further enhance the Agency's cybersecurity posture, as well as the migration of the ENISA's data centre from Heraklion. The expanded legislative tasks of the Agency, such as the CRA, the EU Vulnerability Database and DORA platforms require that ENISA scales its cybersecurity maturity over the coming years and maintain them to the highest level with regular reassessments as mandated by Regulation (EU) 2023/2841.

The multi-annual (2026-2028) cybersecurity maturity plan that has been endorsed by the ENISA's management team is essential to that end, as it provides a structured, strategic approach to managing cybersecurity risks, ensuring business continuity, regulatory compliance, and alignment with ENISA's strategic objectives. Moreover, as foreseen in Management Board decision 2024/06, the Agency shall close the ENISA office in Heraklion by 30th June 2026 thus requiring the Agency to migrate its data centre. The migration will be combined with efficiency gains and will be strategically aligned with the implementation of the cybersecurity maturity plan. The additional required resources both in terms of budget and FTEs were endorsed by the MB in January's adopted draft and in a second draft submitted to the MB in July 2025. ENISA will start implementing the data centre migration during the course of 2025 and seek to finalise the move from Heraklion premises during the course of 2026. The cybersecurity maturity plan likewise will be initiated in 2025 and actions have been planned throughout 2026.

Resourcing: The Agency submitted two single programming documents to the MB for adoption during the course of 2025, the January draft highlighted the need for an additional 6.2 million EUR for delivering the 2026 work programme and the second adopted draft highlighted the additional resources required for scaling up ENISA cybersecurity maturity and migrating ENISA's data center. The budget that the Agency foresaw that it required for these two projects was an additional 5.65 million EUR. With regards workforce needs the Agency put forward 13 FTEs of which 7 FTEs relate to operational activities for delivering the work programme and the remaining specifically for the cybersecurity maturity plan and data centre migration.

These achievements and milestones among others are expect to inform the 2026 work programme. In addition, the 2026 programme will be implemented during the period of the expected revision of Agency's basic act, which may necessitate adjustments to the work programming during the year.

The full list of statutory tasks that the Agency undertakes from EU legislation is presented in annex XV.

SECTION II. MULTI-ANNUAL PROGRAMMING 2026 – 2028

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA reviewed and updated the Agency’s strategy in 2024, which builds on the Cybersecurity Act (CSA), and outlines how the Agency will strive to meet the expectation of the cybersecurity ecosystem in a medium to long-term perspective, in a manner that is open, innovative, agile as well as being socially and environmentally responsible. The strategy sets out a vision of “A trusted and cyber secure Europe” in which all citizens and organisations of Europe not only benefit but are also key components in the effort to secure Europe. Most importantly, the ENISA strategy outlines three horizontal strategic objectives and four vertical strategic objectives which are derived from the CSA and set the expected medium to long-term goals for the Agency.

1. Multi-annual work programme

The following table maps the strategic objectives stemming from ENISA’s strategy and the associated indicators used to measure progress of the objectives. These strategic indicators are structured to cover several years, supporting continuous assessment and progress 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 | Uptake of ENISA recommendations to support Member States and stakeholders in implementing EU legislation | Use of ENISA’s secure infrastructure and tools and added value of the support to the operational cybersecurity networks | Rate of satisfaction with ENISA’s capacity building activities (e.g. exercises, trainings) | Number of EU certification schemes developed and maintained, number EU regulations making reference to CSA, number of active Member States’ NCCAs (e.g. issuing European certificates) |
| | Foresight on emerging and future cybersecurity opportunities and challenges | Number of identified future and emerging areas reflected in the policy initiatives and interventions | Operationalisation 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 | Number of advise and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC | Rate of satisfaction with ENISA’s support to the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG) |



| | | | | |
|--|--|---|---------------------------------------|---|
| <p>Consolidated and shared cybersecurity information and knowledge support for Europe</p> | <p>Uptake of recommendations stemming from NIS2 Art. 18 report</p> | <p>EU Vulnerability Database is operationalised 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</p> | <p>Percentage of MS that use ECSF</p> | <p>Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and successfully operated</p> |
|--|--|---|---------------------------------------|---|

ENISA Corporate Strategy

The corporate strategy is expected to be assessed for first changes in 2026 with a mid-term review and the Agency is aiming for a total transformation of its corporate strategy by 2029.

ENISA’s corporate vision is to make available a contemporary and attractive workplace for all, based on trust and inclusion, while developing and transforming towards a dynamic, service-oriented organisation, an organisation that continuously improves its operational and administrative efficiency by redesigning its operational and administrative processes, and optimising its structures, services and use of resources. ENISA aims to ensure that it does the right things in terms of actions / activities (effectiveness) in the right way in terms of project and resource management (efficiency) and capitalises efficiency gains before reinforcing any area of work with extra resources. In order to address this vision, the ENISA corporate strategy sets forth objectives with Environment, Social and Governance (ESG) criteria in mind, across three interconnected strategic dimensions, which would drive the Agency and guide the development of its corporate objectives, activities and resource planning: People centric approach, sustainable governance and service delivery.

ENISA’s corporate strategy presents a common vision for a contemporary, flexible and values-driven organisation that empowers staff to deliver outstanding results for people across the EU and beyond. The strategy addresses ENISA’s ambition to perform at the highest level in the interests of Europeans and the needs of its staff members to have an attractive workplace and a fulfilling career where excellence and effort are rewarded. Founded on European Commission strategies and practices, ENISA will strive to maximise the efficiency of its resources by maintaining its focus on developing a flexible, highly skilled and fit-for-purpose workforce that would support ENISA’s goals to enhance its capabilities in future-readiness and continue its path towards an agile, knowledge-based and matrix way of working.

The strategy aims to accelerate the tendency towards flexibility and digitalisation of the workplace into being a front runner in the transition to a green administration, by ensuring that staff work in a green and sustainable work environment. ENISA will continue to enhance its secure operational environment aiming at the highest level compatible with its mission and responsibilities and to strive towards excellence in its infrastructure services based on best practices and frameworks. ENISA will also explore cloud-enabled services that are fit for purpose and provide services in accordance with recognised standards.

The strategy also aims to enhance personal accountability, responsibility and growth, and sets out a common vision in which all staff will work in a trust-based environment through the introduction of new technologies that facilitate modern and flexible work practices. ENISA will strive to promote and foster eco-system solutions, explore opportunities for shared services with other Union Entities, leverage standard technologies where possible and support flexible ways of working.



HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2026-2028

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

Over recent years, the Agency has made persistent and strategic efforts to better manage, prioritize, and balance its resources. These measures aim to address the growing demand for ENISA services from Member States and stakeholders. Actions to ensure the effective and efficient use of resources have included the following:

Structural adjustments: In 2024, the Agency implemented measures to optimize its operational activities and support-structure, focusing on enhancing efficiency, fostering synergies. To ensure the effective execution of its expanding tasks and functions (CRA, CSOA), MB decided to align its operational structure more closely with its work programme. This included the creation of eight dedicated units, each responsible for one of the work programme's eight operational activities. This consolidation not only leverages existing synergies more effectively but also increases both the budget and the median FTE count per activity, rising from just under 8 FTEs in 2024 to nearly 12 FTEs in 2025 and onwards. This higher median FTE count is critical for providing operational activities with greater "operational depth," enabling them to better absorb unforeseen urgent tasks. It also offers increased flexibility, allowing resources to be reallocated within activities as new priorities emerge.

Reallocation of Human Resources: Over recent years, the Agency has introduced various measures to improve the efficiency of its human resources. Although the staff count under the Staff Policy Plan increased by 12 FTEs, from 118 in 2021 to 130² in 2024 to support the Agency in tackling new responsibilities, internal restructuring has remained the primary method for reallocating resources to align with new priorities. A total of 20 posts were restructured and reallocated during this period, highlighting the Agency's agility and ability to adapt effectively to emerging and new service needs. Priority was given to operational units and functions by reallocating posts from corporate functions, many of which have been externalized as much as possible. While this shift has strengthened the human resources supporting the Agency's operational mandate, it has now reached its natural limit. Further internal adjustments at the expense of corporate activities would risk severely compromising essential administrative functions, including IT and physical security, legal compliance, financial and procurement processes, and other critical corporate support services.

According to ENISA's Corporate Strategy adopted by the Management Board in 2023, due to business needs and shortage of resources, ENISA has been using non-statutory staff for demand driven, repetitive and more technical tasks, such as the initiation of financial and operational transactions. Usage of non-statutory staff to initiate financial transactions was exceptionally permitted by internal rules, however this does not comply with EU Financial rules as highlighted by the ECA in their latest audit findings. Should the Commission grant a modification of the EU financial rules the Agency will not be required to rebalance resources by re-allocating posts from operations to corporate.

The Agency assessed its internal workforce needs for 2023-2025 within its previous annual workforce reviews, concluding that the Agency would need an additional 41,5 FTEs in order to address all external as well as internal expectations requisite with the tasks and mandate of the Agency. It also concluded that around 50% of all the needs were critical or highly critical (linked with emerging statutory tasks). Thus, on this basis the Agency took steps in 2023 and 2024 to address the highly-critical and critical internal FTE needs to the extent possible including signing a number of Contribution Agreements with DG CNECT in 2023 and 2024, to be able to engage in total 13 CA agents to meet the specific objectives of the contribution agreements. Also, under the direction of its Management Board the Agency took steps to deprioritise or suppress a number of outputs in previous work programmes and reassign staff to more critical tasks.

Improving Fulfilment of Posts: The Agency significantly increased the implementation of its Establishment Plan, from 87% in 2022 to 98% in 2024. This progress was achieved despite challenges such as heightened competition for cybersecurity talent and the comparatively less competitive salary when benchmarked against the private sector or economically advanced Member States. The Agency nevertheless was able to attract talent mainly due to the flexible teleworking and hybrid-work policy endorsed by the MB, allowing most experts to telework outside their place of assignment for a majority of time as long as they can be at the disposal of the Agency within a reasonable pre-determined time-frame. In 2024, the Agency also established a reserve list of cybersecurity experts. This list allows the Agency to quickly draw on qualified professionals when new positions become available or to address gaps resulting from resignations.

² This figure does not include the posts stemming from the contribution agreements

Maximising Financial Resources: The Agency is committed to optimizing the use of its financial resources by maximizing the utilization of its budgetary allocations. While all Agencies are expected to fully implement their voted budgets, the minimum benchmark is set at 95%. This creates a 5% margin of maneuver, which becomes significant as the Agency's budget grows. Between 2021 and 2024, the Agency has significantly improved its budget implementation rate, ensuring that resources are utilized to their fullest potential.

These improvements are the result of sustained efforts, including measures such as setting financial Key Performance Indicators (KPIs) for all budget managers, enhancing budgetary planning, and improving monitoring processes. As a result, the Agency achieved a 100% budget implementation rate in the past two years. In 2023, for instance, it fully executed the voted budget at a 100% commitment rate. Over the three-year period from 2021 to 2023, these efforts allowed the Agency to commit an additional €1,802,058.78, which would have been forfeited if the implementation rate had remained at the 2020 level of 97%.

The Agency has also prioritized the full utilization of carry-over funds (C8). In 2023, it successfully disbursed the majority of an additional €15 million allocated in late 2022, achieving a final C8 payment rate of 96.14% for the voted budget and 99% for the ENISA Cybersecurity Support Action. This initiative continued into 2023, with the Agency signing a €20 million Contribution Agreement with the Commission for 2024-2026, ensuring the continuation of the Cybersecurity Support Action. The agreement is set for implementation until 31 December 2026.

Another important step taken by the Agency to optimize financial resources is the planned closure of the Heraklion, Crete office by 30 June 2026. Since relocating to the Athens metropolitan area in 2019, the Hellenic authorities has assumed full responsibility for the rent of the headquarters. Maintaining a portion of administrative functions in Heraklion, while the majority of the Agency operates in Athens, incurs not only direct costs but also significant indirect expenses. Closing the Heraklion office will result in additional financial savings, enabling the Agency to redirect these resources toward operational activities.

Finally, the Agency has centralised two important operational budget lines, the operational missions and the operational large-scale events. The centralisation of this budget under the oversight of the COO will improve effectiveness of ENISA actions and increase budget efficiency.

Service Packages: To enhance its service delivery, the Agency introduced service packages in key mandate areas. These packages were designed to integrate ENISA's outputs across various operational activities, creating high-impact, value-added services for its primary beneficiaries—Member States and European Union Institutions, Bodies, and Agencies (Union Entities). This approach also helped streamline resources by avoiding duplication of efforts within ENISA and with external partners.

Partnerships and Synergies: Building on these service packages, the Agency expanded its external partnerships and synergies, ensuring an efficient use of expertise and human resources. Notable examples include:

- **Collaboration with the European Commission:** This includes working with DG CNECT to enhance Member States' critical infrastructure preparedness and provide incident response support when needed. Under the Contribution Agreement signed in Q4 2023, the Agency and the European Commission have secured an additional €20 million for 2024–2026, alongside the possibility of a temporary increase of up to 12 contract agent posts to meet service delivery needs. This is in addition to the €15 million added to ENISA's budget to meet the request from Member States for enhanced cybersecurity support via the "Cybersecurity Support Action" from ENISA in the wake of Russia's invasion of Ukraine. The delivery of support action services has enabled the Agency to implement actions with greater efficiency. This enhanced approach has been recognized and highly valued by Member States, as evidenced by the significant adoption and utilization of these services by them and the feedback received. In the end of 2024, the Agency and DG CNECT have signed yet another Contribution Agreement, which includes €15.25 million for the implementation of the CRA Single Reporting Platform and the continuation of the Support Action, which will be implemented by 31st December 2027. The agreement includes 7% remuneration of the total amount of the action for ENISA for the implementation of the activities. In addition, another contribution agreement was penned with the European Commission in August 2025, through which the Commission entrusts ENISA with the administration and operation of the EU Cybersecurity Reserve with 36 million euros over three years, including 0.67 million for ENISA to support the Cyber Situation and Analysis Centre.
- **Structured Cooperation with CERT-EU:** Joint efforts have supported the development of better situational awareness across the Union, as required by Article 7 of the CSA Regulation. Products such as Joint Rapid Reports and Joint Cyber Assessment Reports, delivered in collaboration with EC3 and EEAS, underscore the importance of this partnership.
- **Support for EU-LISA:** The renewal of annual agreements to plan, execute, and evaluate cybersecurity exercises has bolstering the Agency's capacity-building initiatives and enhanced EU-LISA ability to deal with complex threat landscapes.

- MoUs with EU Entities: Memoranda of Understanding signed with entities such as the European Cybersecurity Competence Centre (ECCC), European Railway Agency (ERA), European Banking Authority (EBA), ESMA, and EIOPA have further enabled the efficient use of the Agency's expertise and human resources while meeting stakeholders' needs. Including long standing MoU with the European Defence Agency (EDA), Europol EC3 and (CERT-EU) to leverage synergies and cooperation between the four EU entities.

The Agency has demonstrated its commitment to maximizing resource efficiency through shared services and strategic partnerships in corporate and administrative areas. For instance, it signed a service-level agreement with the European Cybersecurity Competence Centre (ECCC) to foster corporate synergies in areas such as accounting, data protection, and information security. Additionally, the Agency has been providing legal support services to the European Centre for the Development of Vocational Training (CEDEFOP) under a Memorandum of Understanding (MoU), which also outlines cooperation in joint procurement, shared financial services, human resources, IT solutions, and data protection.

Shared service agreements are also in place with the European Union Intellectual Property Office (EUIPO), and the Agency has continued to enhance its shared services strategy by strengthening partnerships with other EU bodies, including the corporate service centers of the European Commission. Moreover, it has explored new collaborations, such as the joint service center launched in 2024 with the European Institute of Innovation and Technology (EIT) and the European Insurance and Occupational Pensions Authority (EIOPA), providing HR, procurement, and corporate cybersecurity support services.

In the area of cybersecurity, the Agency has supported the implementation of Regulation 2023/2841 on common binding rules for Union entities. This support includes the proposal of a risk management methodology to be used by Union Entities, as well as capacity building activities offered in collaboration with CERT-EU. These collaborative formats can deliver efficiency gains and a coherent approach to cybersecurity across all Union Entities

These efforts underline the Agency's dedication to effective financial management and resource optimization.

2.2. OUTLOOK FOR THE YEARS 2026-2028

The anticipated revision of the cybersecurity act could fundamentally shape the role and responsibilities of the Agency. Without prejudice to the ongoing discussions, the medium-term outlook will be markedly influenced by the revision which could significantly impact the Agency's work programme, due to potential changes to the scope of assigned tasks, and the allocation of resources necessary to fulfil emerging regulatory and operational requirements. In addition the proposed Digital Omnibus package of the European Commission aimed at harmonising incident reporting and clarifying obligation from existing regulations will also shape the Agency's programming of outputs and activities over the coming years.

Looking back the Agency was assigned new tasks following a number of new legislations towards the end of 2024, specifically the Cyber Resilience Act that entered into force on 10 December 2024, Cyber Solidarity Act entered into force on the 4 February 2025, the regulation laying down measures for high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union and the EU Digital Identity Framework Regulation (eIDAS2), in conjunction with existing duties to MS with the transposition of the NIS2 Directive.

The new legislations mentioned above have brought new tasks to the Agency which will require resourcing during the period 2026-2028. Unfortunately, the financial statements accompanying the CRA only allocated 2 additional FTEs (one additional SNE and one additional TA) and the CSoA and eIDAS2 did not allocate any new resources to the Agency. The Agency did put forward its estimations as regards to the resourcing needs which the Agency needs to address the new tasks from CRA and CSoA in previous work programmes in line with the letter of the former Commissioner Breton, which requested the management of ENISA, through the established processes and channels (such as the SPD), to put forward proposals on the "Adequacy of ENISA's programming, organisation and resources."

The allocation of resources to ENISA should take into account the new tasks assigned by new legislations. It is essential to account for the increased legislative duties, policy expectations, and demands, considering also the heightened threat levels highlighted in the ENISA Threat Landscape Report 2024. This report identified a significant escalation in attacks, establishing new benchmarks in terms of both the variety and volume of incidents, as well as their consequences. Ongoing regional conflicts continue to play a major role in shaping the cybersecurity landscape. Additionally, the findings and recommendations from the first State of Cybersecurity in the Union Report should be taken into account.

The Council conclusions³ from the 6 December 2024 acknowledge that the expansion of ENISA's important role is the result of recent legislative initiatives, such as the Cyber Resilience Act (CRA) or the revised network and information systems (NIS 2) directive, which have entrusted the agency with additional tasks. Its key role was also boosted by the growing scale and complexity of the cyber threats and challenges these last years. Therefore, the Council recommends that this increase in tasks should be reflected in adequate resources, without pre-empting the upcoming negotiation of the Multiannual Financial Framework. It is, however, equally important to prioritise actions and to have a sound cooperation with other actors in the cyber domain to avoid duplication of tasks.

The conclusions acknowledge ENISA's support to member states when it comes to policy development and implementation. However, they also call for further improvements and action, notably regarding the development of European cybersecurity certification schemes, as well as the establishment of a single reporting platform.

The text of the conclusions also recognises ENISA's important contribution in enhancing common situational awareness, as well as in developing a common response to large-scale cyber incidents or crises. Further cooperation with the European Commission, the European External Action Service (EEAS), the Computer Security Incident Response Teams (CSIRTs, groups of experts that assess, document, and respond to a cyber incident) network and the European cyber crisis liaison organisation network (EU-CyCLONe, a cooperation network for Member States' national authorities in charge of cybersecurity) is also emphasised in this respect.

³ <https://data.consilium.europa.eu/doc/document/ST-16527-2024-INIT/en/pdf>

Finally, the conclusions highlight the importance of ENISA's cooperation with other actors in the cyber ecosystem, such as the cybersecurity service for EU institutions (CERT-EU), the European Cybersecurity Competence Centre and Europol, but also with international organisations and partners and with the private sector.

It is under this context the Agency put forward additional resource requests for the programming period 2026 – 2028, in the January adopted draft single programming document 2026-2028 and in a second draft adopted in July 2025. The adopted draft single programming document from July highlighted the additional resources required to elevate the cybersecurity posture of the Agency and the migration of the ENISA data centre over the next few years.

2.3 RESOURCE PROGRAMMING FOR THE YEARS 2026-2028

2.3.1. Financial resources

In developing the budgetary estimates of the first and second adopted draft 2026 work programme, the Agency took into account its imperative needs, priorities and objectives as set in the Corporate Strategy and the needs, priorities and objectives of the operational activities.

The current total appropriations in EU Budget for 2026 amount to 26.9 million euros. However, the Agency's draft estimates far exceed this budget envelope, and despite deprioritising a number of statutory tasks in line with the guidelines agreed with the Agency's Executive Board⁴, the Agency needs more resources in 2026 to be able to fulfil its core mandate effectively. The additional required budget that the agency put forward in the second adopted draft of the single programming document 2026-2028 amounted to an additional 11.85 million euros. This amount includes the budget required to scale up ENISA cybersecurity maturity, migrate its data centre from Heraklion, and budget needed to maintain the operational activities in line with the needs of stakeholders and the additional FTEs put forward to accommodate that end. For the years 2027 and 2028 the Agency put forward an additional required budget for the implementation of the cybersecurity maturity plan of 3.5 million euros recurring per year from 2028 onwards and 800 thousand euros from 2028 onwards recurring every year for the data centre migration.

The expanded legislative tasks of the Agency, such as the CRA, the EU Vulnerability Database and DORA platforms require that the Agency scales its cybersecurity maturity over the coming years and maintains them to the highest level with regular reassessments as mandated by Regulation (EU) 2023/2841. The multi-annual cybersecurity maturity plan of the Agency is a complex project with several sub-projects that encompass all ENISA's IT systems. The execution of the cybersecurity maturity plan requires resources from both the operational and corporate units for planning, implementation, as well as monitoring / compliance capabilities.

The decommissioning of the Heraklion data centre by Q2 2026, as foreseen with the Management Board decision 2024/06, requires the necessary resources for migration. The data centre migration is strategically aligned with the cybersecurity maturity plan by increasing resilience while reducing maintenance costs. The decision as to where the data centre will be located has yet to be determined and as such could impact the final required budget.

The additional budget required creates a compounding effect, increasing annually as more projects are deferred to future years. Consequently, the Agency's budgetary needs, based on the development of the draft work programme, significantly exceed its available resources.

⁴ Criteria for prioritising operational activities are based on 1) Legal requirements: legislative mandates obligating the Agency to carry out specific tasks (NIS2, CRA, CSOA etc.) 2) Urgency and deadlines: legal acts requiring the Agency to take action within a specified timeframe or on a recurring basis, often requiring also preparatory steps before legal act is in force. 3) Resources: have new tasks led to additional resource requirements in order to be able to carry out the work

4) Stakeholder feedback: Actions prioritized by Member States (MS) & Commission based on their input and feedback. 5) Added value & impact: Impact & added value of the output for stakeholders as inscribed in the Agency annual activity report.

2.3.2. Human resources

With regards on-going human resource needs, the Agency has started to conduct a thorough analysis of its workforce needs for 2026 to 2028, which it aims to conclude during the course of 2025 in order to recalibrate its needs given the new and / or expanded current legislative tasks (notably stemming from CRA CSoA, targeted amendment of the CSA in 2024 etc), its renewed strategy and the evolving threat landscape.

Though the initial internal workforce needs for 2026-2028 – which were put forward by the activity managers and subsequently assessed and validated by the administration – sum up to a very similar total of 41 FTEs (it was 41,5 FTEs for period 2023-2025) to cover all external expectations and essentially deliver the full plethora of tasks within ENISA mandate, it is important to stress that 64,2% (or fully 27 FTE) of those needs are considered to be not critical. This means that the Agency will be able to mostly use its regular mechanisms via working programme reprioritisation of tasks in the mid-term perspective and reprofiling/restructuring of current functions, to try to address these needs by end of 2028.

However, the remaining 13 FTE needs which are highly critical (plus 2 critical FTE needs), need to be tackled in the short-term perspective. The 2 additional posts allocated to ENISA's 2025 Establishment Plan and Staff Policy Plan through adoption of CRA, have been used to address part of the highly critical needs. Respectively, in activity 5 (1 full FTE post which also addresses a critical need of activity 4) and in activity 8 (1 full FTE post). In addition, the Contribution Agreement which ENISA signed with DG CNCT in December 2024 enables ENISA to address additional highly critical needs in the amount of 3 FTE's which mainly address the short term need to cover the development of CRA single reporting platform. The rest of the 7 highly critical FTE needs, which have to be addressed at latest in 2026 to be able to fulfil the objectives outlined are brought forward under the 2026 additional FTE resource requests for activities 5 "provide effective operational cooperation through situational awareness", activity 7 "supporting development and maintenance of EU cybersecurity certification framework" and activity 8 "supporting market, technology and product-security. In addition, there is 1 FTE additional resource need which is considered critical (but not highly critical) to support activity 2. Thus, the Agency would need to restructure or reprofile in total 7 posts within these activities in the short term, should these additional FTE resources not be granted, and suppress current tasks/functions of these activities in scope requisite with the needs.

The undertaking of the data centre migration and the scaling up of the ENISA cybersecurity maturity plan requires additional resources for both executing the plan and on-going maintenance from the operational and corporate units responsible for platforms, systems and capabilities. The Agency will capitalise on its human resources to undertake a large amount of the tasks in-house, as described in Article 3 paragraph 4 of the CSA, in order to ensure trusted services and business continuity. The Agency put forward an additional 5.5 FTEs required for both the implementation of cybersecurity maturity plan and the data centre migration in its adopted draft V.2 single programming document 2026-2028 of July 2025. For the years 2027 and 2028 the Agency put forward additional required human resources for the implementation of the cybersecurity maturity plan of 6 FTEs and 1.5 FTEs for the data centre migration.

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

Given the current constraints of its resources but also in order to fulfil its strategic and corporate objectives – including setting the pace of its staff development – ENISA will remain committed to the continuous improvement of its efficiency across its operational and corporate tasks. In the period 2026-2028 ENISA will thus further rigorously pursue all the areas which were outlined in section 2.1. and which have already brought tangible benefits. Namely:

- Developing its talent base and thus increasing operational capacities as outlined in its Corporate Strategy and HR strategy;
- Addressing critical HR needs through reprioritisation and externalisation of administrative tasks, including through shared services and partnerships in corporate and administrative areas;
- Utilising internal and external synergies to gain additional resources and use current resources efficiently, in particular through external operational partnerships; and
- Maximising to the outmost the use of existing budgetary resources.
- Further utilising joint corporate services with other Agencies

Within the programming period 2026-2028 ENISA will continue develop and review its operational service packages, to ensure internal alignment and synergies between its structural entities.

Beyond and on top of further elaborating and updating the service packages, ENISA aims to build partnerships with Member States (incl by exploring short- and medium-term secondments and exchanges of staff with relevant national authorities) and strengthen synergies with a number of Union institutions, bodies, offices and agencies. This includes by proposing joint operational objectives and KPIs in the respective work programs, thus further utilising external support and mobilising external resources for the benefit of ENISA operational objectives when those are aligned with the objectives of prospective partners. The main current and possible partnerships and/or prospective cooperation frameworks across its operational activities shall include:

The Agency continues to implement its work programme by systematic use of its statutory bodies (NLO Network, ENISA Advisory Group), as well as other statutory groups such as Stakeholder Cybersecurity Certification Group (SCCG as set out in CSA Art. 22, NISD Cooperation Group and its work-streams, ECATS art.18 group eIDAS regulation, expert groups created under the Union law) and its own ad hoc expert groups. The Agency relies on these groups so as , to avoid duplication of efforts, build synergies, and peer-review the scope and direction of actions undertaken by the Agency to implement its SPD outputs, as well as to validate the results. This way the Agency will fulfil its obligation as outlined in Article 3(3) of the CSA, to avoid the duplication of Member State activities and taking into consideration existing Member State expertise. Hence, all activities enlisted under section 3.1. and 3.2. in this SPD contain an indication of how specific deliverables and other actions undertaken to fulfil the outputs will be validated and peer-reviewed or consulted with relevant external experts.

ENISA also intends to assess and analyse sustainability of existing processes, explore alternative models for providing indirect support and propose actions to ensure operational efficiency without compromising the activities of the operational units. Within the context of its Corporate Strategy, the overall operating business model of the support units would continue to be reviewed in order to ensure that thresholds and requirements of the Corporate Strategy are met. Digitalisation of services, self-service functionalities and service optimisation will be also at the core of the future way of working and ENISA's corporate strategy to build an agile workforce. ENISA will continue to review and explore possibilities to reengineer its processes, with a view to optimising service quality and cost-effectiveness.

Another example of the Agency seeking to achieve efficiency gains is via joint corporate services with other Agencies such as with the shared support services for cybersecurity risk management via the (C)ISO Support Service pilot, developed in close cooperation with CERT-EU and other participating EU entities.

In addition, as part of its strategy to achieve efficiency gains at the IT level, ENISA will focus on enhancing synergies and interoperability between existing and newly developed platforms, particularly in the domain of Cyber Threat Intelligence (CTI). ENISA aims to streamline information sharing and threat detection capabilities across the EU cybersecurity ecosystem. A key component of this strategy involves developing shared CTI platforms that integrate with existing systems, allowing for real-time data exchange. ENISA will also prioritize the creation of interoperable tools

and interfaces, such as CRA, DORA, and EU Vulnerability Database, reducing redundancy and enabling more efficient resource allocation. This approach not only supports operational readiness but also ensures that EU-wide cybersecurity efforts are more cohesive, scalable, and adaptable to emerging threats. The shared platforms will enable ENISA to deliver targeted cybersecurity services to a wider range of stakeholders, enhancing overall resilience while optimizing operational costs.

SECTION III. WORK PROGRAMME 2026

This is the main body of the Work Programme describing, per operational and corporate activity, 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 eight operational activities and three corporate activities have been identified to support the implementation of ENISA's mandate in 2026.

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.

2026 Work Programme Priorities

The agency's work program for 2026 focuses on key priorities that align with the ENISA strategy. These priorities include implementation of the cyber reserve, CRA single reporting platform, the publication of the second state of cybersecurity in the EU report and assisting MS in enhancing cybersecurity maturity. By prioritizing the areas described below, ENISA will ensure effective implementation of our strategic objectives while addressing critical challenges and opportunities.

1. Policy Monitoring & Resilience of Critical Sectors

- State of Cybersecurity in the EU Report (NIS2 Article 18): ENISA will publish the second edition in cooperation with the NIS Cooperation Group and the European Commission, ensuring follow-up on recommendations.
- Critical Sector Resilience: Assist Member States in enhancing cybersecurity maturity through NIS Investments study, NIS360 service catalogue and EU action plan for hospitals and healthcare providers under NIS2.
- Union Risk Assessments: Conduct coordinated resilience stress tests and supply chain risk assessments to evaluate and strengthen critical infrastructure.
- Sectorial & Horizontal Working Groups: Support NIS2 workstreams to refine policies and address emerging threats.

Strategic Alignment: Support for effective and consistent implementation of EU cybersecurity policies

2. Capacity Building

- Cyber Europe 2026: Host the 8th edition of Europe's largest cybersecurity exercise, testing the revised Cyber Crisis Management Blueprint in response to evolving geopolitical threats.
- European Cybersecurity Skills Framework (ECSF): Assist Member States in adopting ECSF to standardize cybersecurity training and workforce development.

Strategic Alignment: Strong cybersecurity capacity within the EU.

3. Operational Cooperation, Support Services & Situational Awareness

- Strengthen CSIRTs Network and EU-CyCLONE cooperation by providing threat assessments, vulnerability analysis, and cross-border incident response.
- Threat Intelligence & Preparedness: Ensure stakeholders are informed about cyber threats, vulnerabilities, and crises to improve EU-wide resilience.
- EU Cybersecurity Reserve (Cyber Solidarity Act): Operationalize the reserve to enhance large-scale incident response capabilities (financed via contribution agreement).
- EU Cybersecurity Networks & Platforms: Develop and upgrade IT systems for operational support, including the EU Vulnerability Database and CRA Single Reporting Platform (financed via contribution agreement).

Strategic Alignment: Effective Union preparedness and response to cyber incidents, threats, and crises.

4. Certification & Market Support

- EU Certification Schemes: Develop candidate schemes for EUMSS & EUDIW in line with EU Cybersecurity Certification Framework.

- Support CRA implementation with technical guidance, market surveillance and analysis, and assessment of harmonized standards and supporting the relevant stakeholders in particularly SMEs.

Strategic Alignment: Building trust in secure digital solutions

In addition, each of the priorities align with the horizontal objectives of empowered communities in an involved and engaged cyber ecosystem, foresight on emerging and future cybersecurity opportunities and challenges and consolidated and shared cybersecurity information and knowledge support for Europe.

5. Strengthening ENISA’s IT infrastructure

ENISA will prioritize IT infrastructure to support its evolving mandate, with two critical initiatives:

- Data Center Migration - Complete the transition of ENISA’s data center from Heraklion by the end of 2026.
- Cybersecurity maturity plan - Implement a comprehensive cybersecurity maturity framework aligned with Regulation (EU) 2023/2841, that supports expanded legislative tasks under CRA, the EU Vulnerability Database and others.

The following graphs provide insights into the resource’s allocation of each of the operational activities for 2026 work programme.

Table 1 presents the budget allocated to each of the ENISA operational activities financed from Title 3 EU subsidy budget. Please note that activity 4 manages the IT platforms and systems on behalf of the all-operational activity business owners. Activity 6 actions are financed via contribution agreements, see table 3 for further information on contribution agreements and annex XI

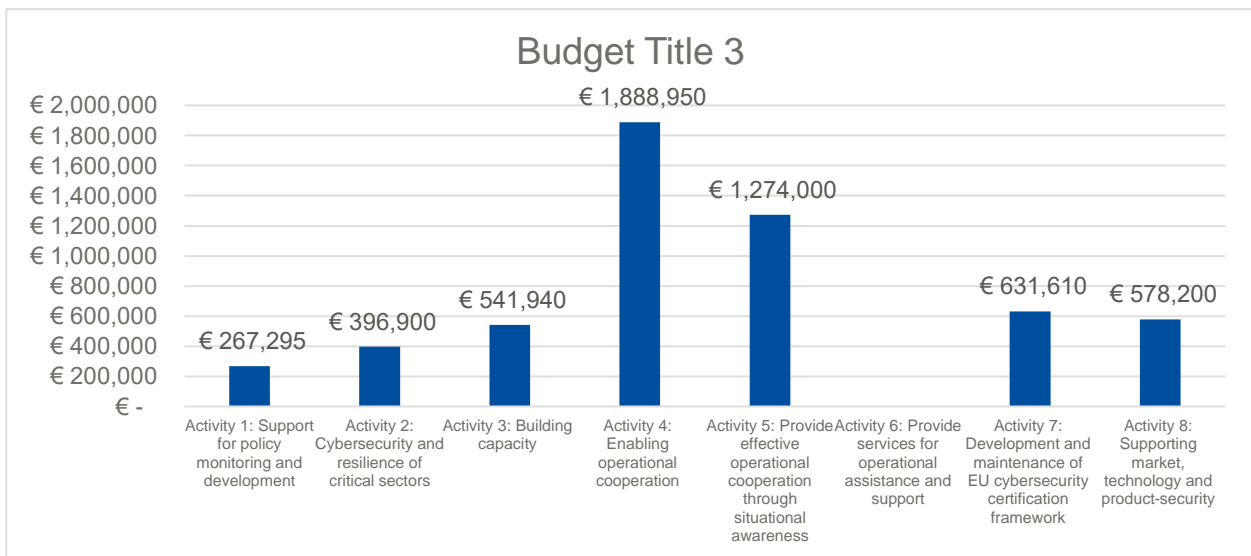


Table 2 presents the allocated number of target FTEs for each of the ENISA operational activities financed from Title 1 EU subsidy budget.



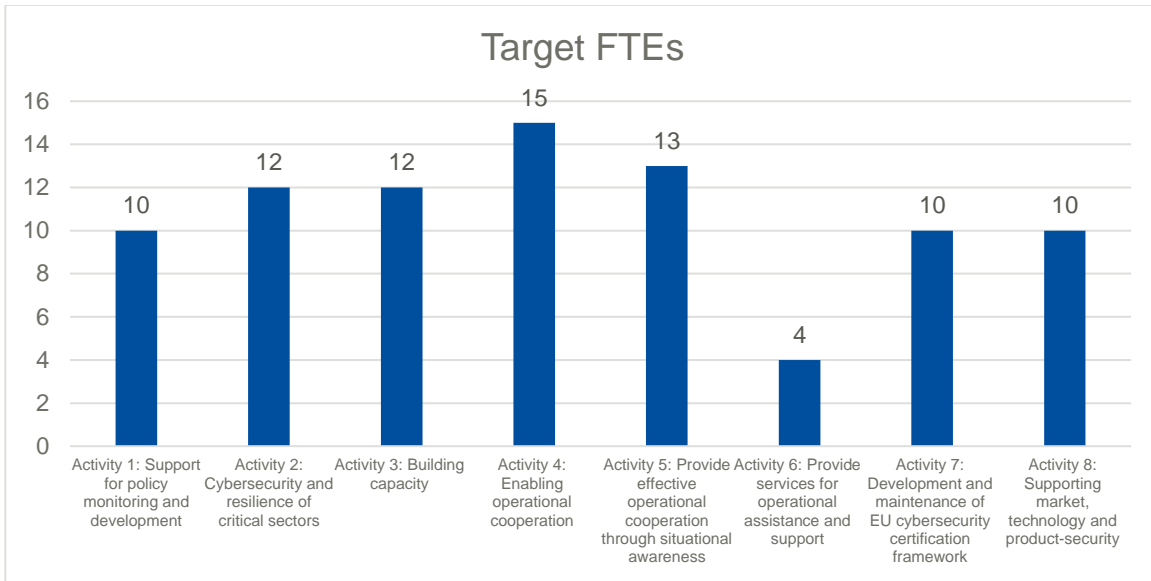


Table 3 presents the 2026 forecast commitment appropriations of the contribution agreements Title 4 budget.

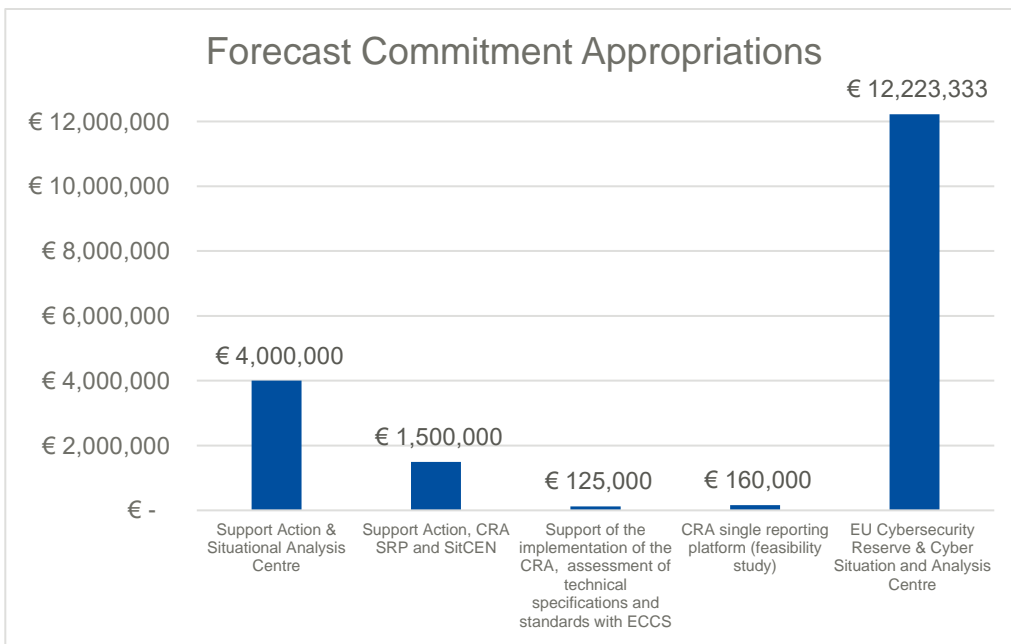
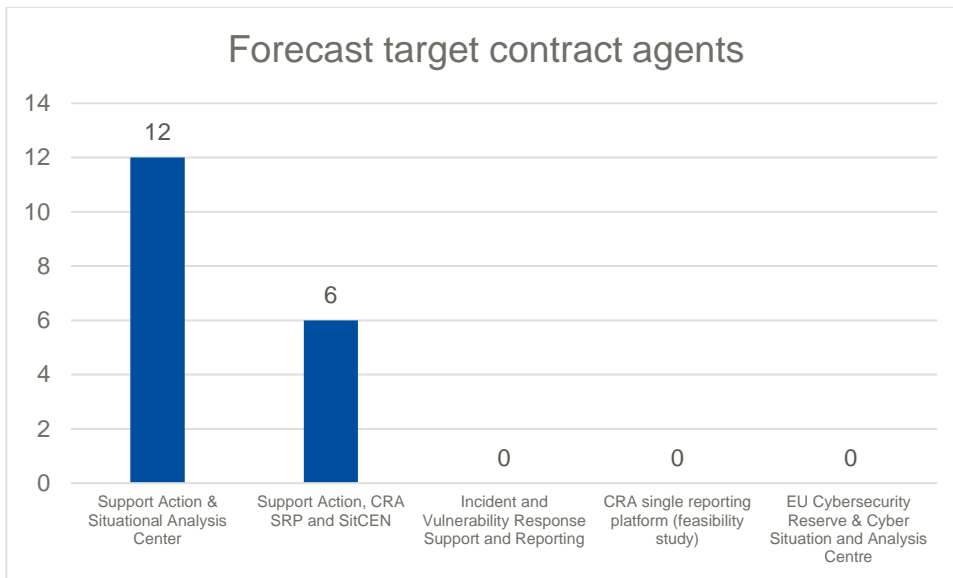


Table 4 presents the forecast number of FTE contract agents financed via the contribution agreements Title 4 budget.

Please note that a number of FTEs from the Support action contribution agreement signed in 2023 will be transposed during the course of 2026 to the Cyber Reserve.





Service packages

In 2022 the Agency introduced the concept of service packages to allow management to focus efforts and resources in a highly structured and more efficient manner for obtaining specific objectives. The ENISA service packages are organised into individual service packages, a service package is a collection of cybersecurity products and services that span across a number of activities and contribute to the objectives of a discrete service package. A service package is a means of centralizing all services that are important to the stakeholders that use it. The Agency will continue to review and prioritize its actions in order to build and make use of internal synergies, and ensure that adequate resources are reserved across the Agency in a transparent manner.

The agency has identified five discrete service packages that make up ENISA’s service catalogue:

- NIS2 led by activity 2 cybersecurity and resilience of critical sectors
- Training and exercises (TREX) led by activity 3 capacity building
- Situational Awareness (SITAW) led by activity 5 provide effective operational cooperation through situation awareness
- Certification (CERTI) led by activity 7 development & maintenance of EU cybersecurity certification
- Cybersecurity index (INDEX) led by activity 1 support for policy monitoring and development

Stakeholders and engagement level

Stakeholder strategy is expected to be reviewed at the later end of 2025 as such this section will be reviewed and updated according to the outcome of the strategy during the drafting of the 2027-2029 work programme.

KPIs / metrics

The work programme for 2026 includes indicators for measuring the new strategic objectives from the updated ENISA strategy, indicators and targets for measuring the activity objectives and indicators at the output level to measure the performance of the outputs. The implementation of Strategic KPIs are expected to be reviewed and the requirements for achieving them to be drawn up during the course of 2026 and will be reflected in the draft work programme 2027-2029.



3.1 OPERATIONAL ACTIVITIES

Activity 1 Support for policy monitoring and development

OVERVIEW OF ACTIVITY

This activity delivers on ENISA's strategic objectives "support for effective and consistent implementation of EU cybersecurity policies" and "consolidated and shared cybersecurity information and knowledge support for Europe". In particular, work under this Activity shall provide strategic long-term analysis, guidance and advice on current policy challenges and opportunities with the aim to support informed decision making. In terms of knowledge management, ENISA will work towards consolidating information on the cybersecurity posture across MS, including via input from National Cybersecurity Strategies in conjunction with the EU cybersecurity index, the peer-reviews, as well as from other ENISA's activities. Efforts in developing and maintaining the EU cybersecurity index and developing and following up on the biennial "Report on the State of Cybersecurity in the Union" mandated by Art.18 of NIS2 will continue. The highlight for 2026 is the biannual report on State of Cybersecurity in the Union (Art 18 of NIS2 directive).

As such, under this Activity ENISA will support the Union institutions and MS on new policy initiatives⁵ through evidence-based inputs into the policy development process. ENISA will also conduct policy monitoring, in coordination with and in support of other EU institutions/bodies and MS. Such monitoring will facilitate the identification of potential areas for policy development or measures for policy implementation.. This will also be supported by the development of in-house capabilities to timely, regularly and consistently be able to provide advice on the effectiveness of the existing Union policy and law, in accordance with the EU's institutional competencies, via the "Implementation Check" model, in particular together with Activities 2 and 8.

This cross cutting activity leads ENISA's efforts towards delivering the cybersecurity index (INDEX) and policy analyses to better map MS needs and requirements, which can be used for programming activities 2 and 3. The added value of this activity is to support the decision makers in evidence-based policy making, in a timely manner and to inform them on developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework, by also utilizing among other sources information from threat landscape, situational awareness, foresight, incident reporting and vulnerabilities disclosure in collaboration with Activities 4, 5 and 8.

Activity 1 leads the Index service package and supports the NIS, TREX and CERTI service packages. The Activity supports COM or EEAS initiatives for Eastern partnership or similar.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV.

| LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY) | INDICATOR FOR STRATEGIC OBJECTIVES |
|--|---|
| Empowered communities in an involved and engaged cyber ecosystem Consolidated and shared cybersecurity information and knowledge support for Europe Effective and consistent EU policies implementation for cyber resilience | Uptake of recommendations stemming from NIS2 Art. 18 report. Number of identified future and emerging areas adopted by policy interventions. |

ACTIVITY 1 OBJECTIVES

| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|--|--|--------------------------------|---|---|
| 1.A By end 2026 implement a policy monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, support and assistance to national and Union policymakers in cybersecurity | Art 5 CSA; Art. 9 CSA | 2026 and continuous afterwards | Assessment of ENISA advice and on EU policy (stakeholder survey, desktop research) | 75% stakeholder satisfaction from ENISA's advice (among EU policy makers) |
| 1.B By Q3 2026 and in collaboration with Activity 2, aim to ensure that 2/3 of policy observations within the first State of Cybersecurity in the Union report have been followed up by MS and COM | Art 18 NIS2 | 2026 and continuous afterwards | Assessment of MS usage of the Art. 18 report (stakeholder survey, desktop research) | 2/3 of MS are using Art.18 report as input for their cybersecurity strategies |
| | | | | All MS use ENISA support and tools for the work on their NIS Strategies |

ACTIVITY 1 OUTPUTS

⁵ Horizontal initiatives on NIS2 sectors and CRAs



| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ⁶ |
|---|---|--|--|--|------------------------|---|
| 1.1 Assist MS to implement, assess, review National Cybersecurity Strategies and policies. Enhance a culture of trust and cooperation among MS, also through peer reviews. | Stakeholders receive technical advice with the evidence needed for policy-making activities and the definition of implementation measures | NIS CG, including relevant work streams; NLOs, including relevant subgroups, Advisory Group | Rate of use by MS of the the National Capabilities assessment framework or the peer review framework, including the code of conduct. | Biennial (Survey), annual dialogues, and annual desktop research | NA | 2/3 of MS are using Art.18 report as input for their cybersecurity strategies and policy making. All MS use ENISA support and tools for the work on their NIS Strategies and policy making |
| 1.2. Collect relevant evidence by maintaining and enhancing the EU cybersecurity index and use such evidence to inform ENISA's support on strategies, as per output 1.1. Present collected knowledge in the Report on the State of Cybersecurity in the Union, further contextualising it with other ENISA sources e.g. the CRA Market Analysis (Activity 8). | | | Rate of contribution of State of the Cybersecurity in the Union Report by CSIRT N and NIS CG. | | Contribution by all MS | 100% |
| 1.3. Maintain analyses on time-sensitive policy observations offering technical advice to policy development and implementation by mapping gaps, challenges and needs in implementing NIS2 and other EU legal acts. | | | Assessment of timeliness, regularity and consistency of advice provided during policy development | | NA | 75% stakeholder satisfaction from ENISA's advice (among EU policy makers) |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: Union institutions such as DG CNECT, other DGs, HWPCI, EP ITRE, MS cybersecurity authorities, NIS Cooperation Group and relevant work streams, ENISA National Liaison Officers and subgroups; Advisory group.

Involve / Engage: Operators of NIS2 and industry associations/representatives

ACTIVITY 1 RESOURCE FORECASTS



| | Budget | FTEs |
|------------------------------------|-------------------|-----------------------|
| Activity resources from EU subsidy | Budget: € 267.295 | FTE ⁷ : 10 |

⁷ Target FTEs

Activity 2 Cybersecurity and resilience of critical sectors⁸

OVERVIEW OF ACTIVITY

The activity supports Member States with increasing cybersecurity maturity in critical sectors, not only through policy implementation but also through measuring the needs of each sector and offer tailor made recommendations. The objectives of this activity are to ensure efficient measurement of the maturity of the sectors (through the NIS Investments study and the NIS360); to promote actions towards increasing the cybersecurity posture also through increased collaboration; to support alignment and integration of the sector specific resilience policies (such as DORA, for resilience in the finance sector; the Network code for cybersecurity of cross-border electricity flows; Part-IS for Aviation etc). This activity includes an annual policy implementation check (through the NIS Investments study and the NIS360), which relies on direct information from companies in the NIS sectors.

Under this activity ENISA provides support to the on sector related and sector focused working groups such as the NIS Cooperation Group workstreams implementing the NIS CG work program. ENISA’s goal here is to monitor the implementation of the adopted horizontal frameworks for risk management, security measures and incident reporting across all policy files, which can also be used beyond the NIS2 (for example, under DORA and the Aviation Part-IS when relevant), creating a common approach. Similarly, other related sector specific files (like the Healthcare Cybersecurity Action Plan or the Electricity Code) will be coordinated under this activity supporting the MS, depending on allocated resources.

Secondly, under this activity, ENISA supports MS and the Commission with addressing specific threats and risk scenarios for the Union related to critical sectors (supply chain), considering technology/ market developments such as O-RAN, and other Union coordinated risk evaluations (such as Nevers in 2024, Cyber risk posture for telecoms and energy in 2024) the Council Cyber Posture⁹, the Union coordinated supply chain risk assessments (under the NIS2), and the Union coordinated preparedness tests (aka resilience stress tests, under the Cyber Solidarity Act). Based on the stress tests methodology developed by ENISA, this activity is supporting the implementation of the cables security¹⁰ toolbox.

In 2026 ENISA will also support the MS and the Commission with carrying out a Union coordinated resilience preparedness tests and a Union coordinated supply chain risk assessments. Resilience stress tests are part of the services catalogue ENISA has developed for the critical sectors to increase their maturity. This activity is tightly linked with Activity 8 on market, technologies and product security.

Thirdly the activity also addresses sector-specific issues, working with sectorial stakeholders in the NIS sectors, providing a service catalogue based on their criticality and maturity posture (NIS360). For each sector, ENISA will support (if created) the NIS Cooperation Group workstream of relevant national authorities, but also engage with the industry, either by supporting EU ISACs, or by co-organising industry events together with Member States or relevant authorities to facilitate public-private dialogue on cybersecurity. This activity provides important sectorial input to other SPD activities, such as cybersecurity posture of the Union (Activity 1), cyber exercises and training (Activity 3) and sectorial situational awareness reports (Activity 5).

Finally, there is a dedicated output for checking the implementation of these policies and the efficiency of the services catalogue in long term, by collecting data from public sector and the industry directly, to ensure that the NIS2, sectorial rules and other lex specialis, do not only remain on paper, but actually improve the level of security of the NIS sectors, producing the annual NIS investments report, the annual NIS 360 and sectorial cyber risk posture briefs, which give an overview of the posture of different NIS sectors. This output provides important sectorial input to the State of Cybersecurity in the Union report (Activity 1).

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV.

| LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY) | INDICATOR FOR STRATEGIC OBJECTIVES |
|--|--|
| Empowered communities in an involved and engaged cyber ecosystem Effective and consistent EU policies implementation for cyber resilience | Uptake of ENISA recommendations to support Member States and stakeholders in implementing EU legislation |

ACTIVITY 2 OBJECTIVES

| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|--|--|-----------------------------|---|---|
| 2.A By [2026] pilot and by [end 2027] implement common frameworks and joint tools for NIS2 in the areas of (a) risk management, (b) security measures and (c) incident reporting for all EU sectors, and in line with industry good practices and international standards. | CSA Article 5, Article 6 and NIS2 | Frameworks pilot by 2026 | Pilot program implementation (# of sectors piloting the frameworks, feedback scores on the usability) | #20MS to adopt/use/endorse the frameworks |
| | | Full implementation by 2027 | | >75% usability score |

⁸ Critical sectors as terminology is used in this context to cover ALL sectors in scope of the NIS2.

⁹ <https://www.consilium.europa.eu/media/56358/st09364-en22.pdf>

¹⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009>



| | | | | |
|---|--------------------------------------|------|---|---|
| 2.B Provide continuous comprehensive support to MS for implementing Union's regulatory cybersecurity requirements and raising resilience across critical sectors. | CSA Article 5, Article 6 and NIS2 | 2027 | Requests received by the NIS CG or MS or other community groups | >80% of requests received have been resolved for a maximum of 20 requests |
| | | | | >75% satisfaction with ENISA support over period |
| 2.C By [end 2027], help to increase [the overall maturity level] of critical sectors under NIS 2 [by 2027]. | CSA Article 5 [possibly NCCS] & NIS2 | 2027 | Maturity assessment based on the updated NIS360 methodology | >2 sectors improving maturity |

ACTIVITY 2 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ¹¹ |
|--|--|---|--|-------------------------|-----------------------|--|
| 2.1 Support Member States with the implementation of policy files (such as NIS2, DORA etc) | NIS2 frameworks for risk management, security measures, and incident reporting | DG CNECT, NIS CG | Framework usage | Annual (Internal count) | n/a | to be mapped against national frameworks from 3 MS |
| | | | EU register for digital entities is used by all MS | Annual (Report) | (2025) 5 MS use EUDIR | at least 10 MS to use EUDIR |
| | | | Coherence in the level of implementation between NIS2 and other frameworks, e.g. DORA, NCCS" | Satisfaction survey | n/a | 60% |
| 2.2 Support Member States with, union coordinated risk evaluations, and union coordinated preparedness tests | Support Union-wide risk evaluations and risk scenarios (health, transport, vehicles) and their follow-up (5G, Nevers) Coordinated risk assessment of critical supply chains | DG CNECT, NIS CG | Stakeholder satisfaction | Biennial (Survey) | 94% | 70% |
| | | | Number of sectorial situational awareness reports | Annual (Internal count) | 6 | 6 |
| | | | Stakeholder satisfaction | Biennial (Survey) | 94% | 70% |
| 2.3 Improve cybersecurity and resilience of the NIS sectors | Stakeholders use the NIS service packages to improve security and resilience of the sectors | DG CNECT, NIS CG, Sectorial EU ISACS, sectorial EU agencies | Number of critical sectors increasing maturity based on NIS360 | Annual (Internal count) | 3 | 3 |
| | | | Number and frequency of services/workflow delivered to NIS sectors | Annual (Internal count) | 21 | 10 |



| | | | | | | |
|---|--|--|--|-------------------------|-----|------------|
| | | | Stakeholder satisfaction | Biennial (Survey) | 94% | 70% |
| 2.4 Perform an annual policy implementation check and improve maturity of sectors | MS and EU institutions, both horizontal and sectorial stakeholders, use the NIS investments, the NIS360 and the cyber posture briefs as reference documents for policy making. | DG CNECT, NIS CG, Sectorial EU ISACS, sectorial EU agencies, AG as necessary | Number of critical sectors assessed by NIS360 and cyber posture briefs | Annual (Internal count) | 10 | at least 6 |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: CNECT, NIS CG, National competent authorities, Sectorial DGs, Sectorial Union Entities, Sectorial competent authority groups, sectorial ISACs

Involve / Engage: NLOs, essential and important entities in the scope of NIS2 and industry associations/representatives, ENISA Cybersecurity Directors Group

ACTIVITY 2 RESOURCE FORECASTS

| | Budget | FTEs |
|------------------------------------|-------------------|------------------------|
| Activity resources from EU subsidy | Budget: € 396.900 | FTE ¹² : 12 |

¹² Target FTEs



Activity 3 Capacity Building

OVERVIEW OF ACTIVITY

This activity seeks to improve the capabilities of Member States, Union Institutions, bodies, and agencies, as well as, public and private stakeholders from NIS 2 Sectors. It focuses on improving stakeholders' resilience and response capabilities and increasing their preparedness.

Furthermore, It also aims at enhancing their skills and behavioural change with regards to cyber hygiene and reduce the cyber skills gap, maintaining the European Cybersecurity Skills Framework (ECSF) by engaging with the relevant communities and stakeholders. ENISA will support Member States in adopting the ECSF by providing practical guidance, promoting a coherent approach to cybersecurity skills development across the Union including the development of European individual cybersecurity skills attestation schemes. The "train the trainers" concept will empower stakeholders to autonomously deploy ENISA's services, share good practices and lessons learnt and material to increase their preparedness and ability to respond to emerging cybersecurity threats and risks (CSA art 6).

In line with CRA (article 10), activity 3 shall also support market surveillance authorities, conformity assessment bodies and SMEs liable under the CRA regulation to develop the appropriate cybersecurity skills following ENISA's ECSF and facilitate collaboration among relevant public and private stakeholders to ensure re-skilling or up-skilling of targeted professionals..

The Agency, in collaboration with relevant Union Entities, Members States operational communities and NIS 2 sectors, will conduct a limited number of targeted exercises (CSA Art 6(1)h) and accompanying trainings (CSA Art 6(1)i) focusing on empowering the trainers and enhancing the resilience, maturity and preparedness of the NIS sectors (in cooperation with activities 2, 4 and 6). In cooperation with CERT.EU, will devise and deliver a targeted capacity building program to assist Union Entities in implementing Regulation (EU) 2023/2841. In addition ENISA will support the Blueprint in the context of Cyber Europe. Given the advanced planning stage of Cyber Europe, ENISA will integrate the strategic / political layer and scoped according to the available resources.

The activity will contribute to the INDEX service package by developing indicators and collecting data to measure progress in closing the cyber talent gap, in line with the EC Communication on the Cybersecurity Skills Academy, and will provide analytical insights on EU cybersecurity capacity, awareness and cyber hygiene of citizens and SMEs of the EU in the context of the State of Cybersecurity in the Union (NIS 2 Article 18).

This activity seeks to develop strong ties with stakeholders and build on the work established by the ENISA cybersecurity Support Action, as well as, the forthcoming ECCC's funded projects on capacity building.

Finally this activity will assist non EU stakeholders (e.g. from Western Balkan or UA) to improve their capacity building mechanisms and will participate in EU US strategic dialogue by exchanging good practices on capacity building.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)

Empowered communities in an involved and engaged cyber ecosystem

Strong cyber security capacity within EU

INDICATOR FOR STRATEGIC OBJECTIVES

Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings)

Percentage of MS that use European Cybersecurity Skills Framework

ACTIVITY 3 OBJECTIVES

| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|---|--|------------------------|---|--------|
| 3.A Maintain and regularly update the European Cybersecurity Skills Framework (ECSF). | EU Communication on Cyber Security Skills Academy Article 10 and 6 | 2027 | Number of MS endorsing the ECSF framework | 18 |
| | | | Stakeholder satisfaction rate | 95% |



| | | | | |
|---|--|------|--|----|
| 3.B Community empowerment through maintaining and evolving relevant toolkits, methodologies and standards | CSA Article 4, 6, 7(5), 10 CRA Article 10 REU Article 10 | 2027 | Number of MS and Union institutions, bodies, offices and agencies using ENISA's toolkits, methodologies and frameworks | 20 |
|---|--|------|--|----|

ACTIVITY 3 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUEN CY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ¹³ |
|--|--|---|---|--------------------------|----------------|---------------------------|
| 3.1 Support the adoption and uptake of EU's Cybersecurity Skills Framework | Measure and report on the skills gap including developing indicators to be used for INDEX and Article 18a | AHWG on Cybersecurity Skills, | Stakeholder satisfaction | Biennial (Survey) | 91% | 93% |
| | Map the skills arising from new policy instruments | ECCC WG 5 on Skills | Number of MS endorsing ECSF | Annual | N/A | 17 |
| | Promote the adoption of ECSF in MS, in training organisations and academia and ensure its regular update in line with the Cyber Skills Academy Communication. Including skills attestation schemes. | | Number of member States mentioning the ECSF in their relevant legislation | Biennial | N/A | 3 |
| | | | Number of Training Organisations endorsing ECSF in their training programs | Annual | N/A | 8 |
| 3.2 Organise targeted exercises and support stakeholders to plan and execute their own exercises | Organise a set of limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders (e.g., Cyclone, CSIRTs Network, Union Entities). Orchestrate the execution of exercises for specific target audiences including those defined in Cooperation Agreements with other EU entities providing tools like methodologies, templates and providing them access to a community of peers. Follow up on the findings of previous exercises and ensure its timely and appropriate implementation. | NLO Network (as necessary) CSIRTs Network (as applicable) | Number of people impacted directly and/or indirectly by exercises organized by ENISA | Annual (Report) | N/A | 10000 |
| | | EU-CyCLONe members (as applicable) NIS Cooperation Group (as applicable) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as applicable) CERT.EU | satisfaction of entities/communities participating in the capacity building activities organized by ENISA | Annual | N/A | 93% |



| | | | | | | |
|---|---|--|--|-------------------|-----|------|
| | Assist Union Entities in implementing Regulation (EU) 2023/2841 (mostly article 4, 11) by providing tools like methodologies, templates and providing them access to a community of peers. | | | | | |
| 3.3 empowering communities to execute their own capacity building programs using ENISA's relevant tools and methodologies | <p>Develop & support communities that will facilitate and multiply the sharing of frameworks, good practices and lessons learnt, covering all Activity 3 initiatives and services.</p> <p>Develop strong ties to the stakeholders and work of the Support Action, as well as, the forthcoming ECCC's funded projects on capacity building and develop synergies with ENISA's services and results</p> | <p>NLO Network (as necessary)</p> <p>CSIRTs Network (as applicable)</p> <p>EU-CyCLONe members (as applicable)</p> <p>NIS Cooperation Group (as necessary)</p> <p>EU ISACs (as applicable)</p> <p>NLO subgroup of Cyber Europe planners (as necessary)</p> <p>Key private stakeholders (as applicable and in line with the ENISA international and stakeholder engagement strategies)</p> | Number of participants in ENISA's communities, multiplying the sharing of frameworks, good practices and lessons learnt. | Biannual (Report) | TBD | 100 |
| | | | Engagement rate, the percentage of active members who are contributing to these communities. | Biannual (Report) | TBD | 40 |
| | | | Community retention rate as percentage of members who remain in the community over a long period | Biannual (Report) | TBD | >70% |
| 3.4 Support stakeholders to organise and deliver successful and trustworthy Cyber Security Challenges competitions by helping to ensure trust, transparency and fairness in the competitions. | <p>By being involved in key governance and oversight activities involving the Jury, Watchdogs, and ECSC governance structures.</p> <p>This includes as well as on-site operations during the ECSC Final, critical for reinforcing ethical standards, managing disputes, aligning operational protocols, and maintaining the credibility of the competition.</p> <p>Providing guidance and connecting the community, especially ECSC Steering Committee, with EU entities and especially the ECCC, thus supporting them to undertake the organisation and execution of ECSC finals and form an elite team to represent Europe in the next ICCs</p> | <p>ECCC staff</p> <p>ECSC executive committee and Steering Committee</p> <p>NLO Subgroup</p> | Stakeholders' satisfaction with ENISA's support to ensure trust, transparency and fairness in cybersecurity challenges (survey). | Annual (Report) | TBD | 60% |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Involve / Engage: Training organisations, private entities of NIS 2 sectors, CSIRTs Network and related operational communities, European ISACs, EU-CyCLONe members, Blueprint., National Competent Authorities through the NIS Cooperation Group Work Streams, AHWG on Awareness Raising and Education, AHWG on Skills, EEAS, DG NEAR, DG CONNECT, Cybersecurity professionals, HWPCI, EDIC, ECCC Working Group 5, European Digital Infrastructure Consortium



| ACTIVITY 3 RESOURCE FORECASTS | | |
|------------------------------------|-------------------|------------------------|
| | Budget | FTEs |
| Activity resources from EU subsidy | Budget: € 541.940 | FTE ¹⁴ : 12 |

¹⁴ Target FTEs

Activity 4 Enabling operational cooperation

OVERVIEW OF ACTIVITY

This activity supports the operational cooperation among Member States, EU entities and the internal coordination between ENISA operational activities.

The main goal of the activity is to provide operations, support and assistance in order to ensure efficient functioning of EU operational networks and cyber crisis management framework outlined in the 2025 EU blueprint. Under the mandate of NIS2, Activity 4 provides daily operations, expertise, organisational support, tools and infrastructure for both the technical layer, the EU CSIRTs Network, as well as the operational layer, the EU CyCLONE - Cyber Crises Liaison Organisation Network, of Union operational cooperation networks, including activities stemming from the healthcare cybersecurity action plan.

Secondly, the activity aims to enhance interaction and trust between these two layers and the overall ecosystem as well as with the NIS Cooperation Group, and the Council of the EU with the goal of bringing closer all networks and communities in order to form an informed, empowered and organised EU cyber crisis management ecosystem.

ENISA further supports operational communities by operating, developing and maintaining secure and highly available networks, interoperable IT platforms, and communication channels. This includes providing operational and maintenance support to EU platforms such as EU Vulnerability Database and when established the CRA Single Reporting Platform as well as other tools used by EU operational networks. Enhanced investment in IT infrastructure is crucial to strengthen business continuity, supply chain management, incident response, and change management, while elevating the maturity of operational IT to ensure resilience and adaptability in an increasingly complex environment.

The activity facilitates synergies with national cybersecurity communities (including civilian, law enforcement, cyber diplomacy, and cyber defence) and EU actors, such as CERT-EU, EC3, and EEAS, to exchange knowledge, best practices, provide advice, and issue guidance. The activity is also internally responsible for the structured cooperation with CERT-EU and as such to identify and act upon synergies between the Agency and Member States' work and the work of the IICB and CERT-EU. It equally drives internally the cooperation with law enforcement and as such the collaboration with Europol/EC3.

The activity equally manages the ENISA Cyber Partnership Programme and information exchange with security vendors and non-EU cybersecurity entities.

Finally, this activity will also seek to contribute to the Unions efforts to cooperate with third countries and international organisations on cybersecurity, including implementing the revised ENISA international strategy¹⁵ and contribute to the ENISA stakeholder strategy.

This activity supports SITAW, INDEX and NIS service packages.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV.

| LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY) | INDICATOR FOR STRATEGIC OBJECTIVES |
|---|--|
| Empowered communities in an involved and engaged cyber ecosystem | Usage of ENISA's secure infrastructure and tools and standard operating procedures coordinated by ENISA. |
| Effective Union preparedness and response to cyber incidents, threats, and cyber crises | EU Vulnerability Database is operationalized by ENISA and used by MS. |
| Consolidated and shared cybersecurity information and knowledge support for Europe | Reporting platform under CRA is operationalized and used by stakeholders. |

ACTIVITY 4 OBJECTIVES

¹⁵ Inline and where applicable with EU International Digital Strategy adopted in June 2025



| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|---|---|------------------------|---|---|
| By [end 2026] strengthen the interaction and trust within and between key EU operational and cybersecurity communities (CSIRTs Network, EU-CyCLONe, HWPCI and NIS Cooperation Group). | Article 7, 10, 15, 16 NIS2 Article 6, 7 CSA Article 16 CRA Article 11 CSOA | 2026 | Assessment of High level of operational interaction across CSIRTs Network, EU-CyCLONe, HWPCI and NIS Cooperation Group. | >60% of stakeholders agree that ENISA has enabled the functioning of supported the building of trust within the network |
| | | | ENISA is judged as a key enabler of trust within and between CSIRTs Network, CyCLONe, HWPCI and NIS Cooperation Group. | >60% of stakeholders agree that ENISA has enabled interaction and trust between the networks and communities |
| Review and implement both the ENISA stakeholder strategy and ENISA international strategy | Article 12 CSA | 2026 | Coherence of ENISA International Engagement with the Agency's strategy. | Updated international strategy |
| | | | Comprehensive knowledge management and stakeholder management system is established. | Establish framework for knowledge management and stakeholder management |
| Develop and maintain relevant operational IT systems and platforms to support all operational communities and enhance synergies. | Article 7, 10, 12, 15, 16 NIS2 Article 7 CSA Article 16 CRA | 2026 | Relevant IT systems are maintained and new mandatory platforms are developed. | IT Operations are consolidated and synergy plan being implemented (2026). |

ACTIVITY 4 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ¹⁶ |
|--|---|---|--|-------------------------|---------------------------|---|
| 4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs Network and EU-CyCLONe members HWPCI and NIS Cooperation Group. | Enhanced Information Sharing and cooperation among the CSIRTs Network and EU-CyCLONe members and enhanced interaction with HWPCI and NIS Cooperation Group. | CSIRTs Network and EU-CyCLONe members, HWPCI and NIS Cooperation Group. | Stakeholder satisfaction | Biennial (survey) | 89% | 89% |
| | | | Continuous use and durability of platforms (including prior to and during large-scale cyber incidents) | Annual (report) | N/A | Core platforms remain operational during at least one large-scale cyber exercise annually |
| | | | Number of joint sessions established. | Annual (report) | 1 joint session per year. | 1 joint session per year. |
| 4.2 Maintain, develop and promote ENISA Cyber Partnership programme aiming at | operationalisation of the | CSIRT Network, EU CyCLONe, | Stakeholder satisfaction | Biennial (survey) | 84% | 80% |



| | | | | | | |
|--|--|--|---|-------------------|------|--|
| information exchange to support the Agency's understanding of threats, vulnerabilities incidents and cyber security events | Cyber Partnership Programme | Union Entities, HWPCI, MB | | | | |
| | | | Number of new and total partners in the ENISA partnership program | Annual (report) | 4 | 4 |
| | | | Percentage of RFI answered by members of partnership program | Annual (report) | N/A | 50% |
| 4.3 Implement the revised ENISA international strategy and outreach | EU values recognised by international stakeholders | MT, EEAS, COM and (MB as required) | Stakeholder satisfaction | Biennial (survey) | 91 % | >90% |
| | International cooperation support ENISA objectives | | Internal satisfaction with international coordination | Annual (survey) | N/A | >70% |
| 4.4. Develop, maintain and upgrade IT systems and platforms for operational activities | Consolidation of operational IT with view to support ENISA operations. | CSIRTs Network and CyCLONe members and NIS Cooperation Group and Business owners for ENISA Operational IT systems. | Stakeholder satisfaction | Biennial (survey) | 89% | >90% |
| | | | IT architecture for external operational IT services | Biennial update | N/A | One IT architecture for Operational IT services |
| | | | ENISA operational IT | Annual (report) | N/A | Key deliverables included in ENISA annual report |
| 4.5 Development of stakeholder and knowledge management systems and frameworks | Implementation of stakeholder strategy | MT and MB as required | Stakeholder satisfaction with knowledge management and stakeholder management system. | Biennial (survey) | N/A | Phase 1 : assessment of operational needs achieved |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: Blueprint actors, EU decision makers, institutions, agencies and bodies, CSIRTs Network Members, EU-CyCLONe Members, HWPCI and NIS Cooperation Group SOCs including National and Cross-border SOCs.

Involve / Engage: NISD Cooperation Group, OESs and DSPs, ISACs

ACTIVITY 4 RESOURCE FORECASTS

| | Budget | FTEs |
|------------------------------------|---------------------|------------------------|
| Activity resources from EU subsidy | Budget: € 1.888.950 | FTE ¹⁷ : 15 |

¹⁷ Target FTEs



Activity 5 Provide effective operational cooperation through situational awareness

OVERVIEW OF ACTIVITY

This activity contributes to cooperative preparedness and response at Union and Member States level through data driven threat analysis, operational and strategic recommendation based on collection of incidents, vulnerability and threat information to contribute to the Union common situational awareness.

ENISA delivers on this activity by collecting and analysing security events, cyber incidents, vulnerability and threats based on its own monitoring, information shared by external stakeholders due to legal obligations¹⁸ or voluntary shared, aggregating and analysing reports, ensuring information flow between the CSIRTs Network, EU-CyCLONE, and other technical, operational and political decision makers at Union level and including cooperation finalized to increase situational awareness with other Union entities services such as relevant Commission services and in particular DG CNECT, CERT-EU, Europol/EC3, and EEAS including EU INTGEN. This activity benefits from ENISA's Cyber Partnership Programme managed under Activity 4 and the Agency international cooperation frameworks.

Moreover the activity includes the preparation of the regular in-depth EU Cybersecurity Technical Situation Report in accordance with CSA art7(6), also known as the EU Joint Cyber Assessment Report (EU-JCAR), regular weekly OSINT reports, joint reports together with CERT-EU and other ad-hoc reports as needed. Under this activity the Agency prepares threat landscapes and provides topic-specific, as well as general, assessments on the expected societal, legal, economic, technological and regulatory impact, with targeted recommendations to Member States and Union institutions, bodies, offices and agencies. Under this activity, a semi-annual report in accordance to NIS 2 Art23(9)¹⁹ is prepared and the work related to the Cyber Solidarity Act – Incident Review Mechanism (Art21) is undertaken

The activity also supports Member States with respect to operational cooperation within the CSIRTs Network and EU-CyCLONE by providing at their request advice to a specific cyber threat, assisting in the assessment of incidents and vulnerability, facilitating technical handling of incidents, supporting cross-border information sharing and analyzing vulnerabilities, including through the EU Vulnerability Database established under NIS2 and the Single Reporting Platform established under the Cyber Resilience Act. This activity is also responsible for preparing dedicated reports and threat briefings for the Council, in particular the HWPCI under the Cyber Diplomacy Toolbox.

The work on the EUVD and CRA Single Reporting platform is complemented through the delivery of vulnerability services for EU stakeholder. This activity manages the participation in the CVE Program, namely the work related to the CVE Root and participation in the CVE governance structures.

In addition the activity implements the agreements between ENISA and DG CONNECT for the contribution to the Commission Situation Center project.

Finally, this activity includes the work underpinning the establishment of the Single Reporting Platform (SRP) as established under the Cyber Resilience Act. In doing so, the Agency will take into account incident reports frameworks implemented under Article 23 of NIS2 and other relevant EU legislation to ensure alignment and future proof architecture for reporting simplification at EU level. Possible developments of the SRP to accommodate other legislations could also be part of the activity.

This activity includes the continuous development and maintenance of a 24/7 monitoring for situational awareness.

The budget of this activity is partially financed through contribution agreement between ENISA and Commission to support work on CRA, CSOA as well contribution to the Commission Situation and Analysis Center.

The activity leads SITAW service package and contributes to the INDEX and NIS service packages.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV.

| LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY) | INDICATOR FOR STRATEGIC OBJECTIVES |
|---|--|
| Empowered communities in an involved and engaged cyber ecosystem Effective Union preparedness and response to cyber incidents, threats, and cyber crises Consolidated and shared cybersecurity information and knowledge support for Europe | EU Vulnerability Database is operationalised 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 Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and successfully operated |

ACTIVITY 5 OBJECTIVES

| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|--|---|------------------------|---|--|
| By [end 2027] build a common situational awareness between Member States based on shared accurate data and underpinned by validated joint analysis | Article 7 of CSA Article 23(9) of NIS2 Article 21 of CSOA | 2025 - 2027 | EU MS contribute to and validate EU JCAR. | -CSAT for JCAR >4 -75% of EU MS contributes to JCAR |

¹⁸ NIS2, CRA and Regulation 2023/2841

¹⁹ In 2025 this activity will fulfil the tasks under CSA Art5(6)a, b, and c. These report will be superseded as provisions in NIS2 Art 23(9) applies



| | | | | |
|--|---|-------------|--|--|
| | | | ENISA knowledge base is open to Member States and leverage information provided by EU MSs | Knowledge base is used by 40 % EU MS. |
| | | | Establish and test processes and procedure for the Incident Review Mechanism under Art 21 of CSOA | Process for IRM is endorsed by EU MS by Feb 2026 CSAT on IRM report is > 4 |
| Provide regularly general as well as specific threat landscapes and threat analysis, based on observed and data driven trends in incidents and vulnerabilities | CSA Art 9 Article 7 of CSA Article 23(9) of NIS2 Article 21 of CSOA Article 14-17 CRA | 2025 - 2027 | Publish ENISA Threat Landscapes | Publish an annual TL CSAT on ETL is >4 from selected communities |
| | | | JCAR includes threat analysis based on incidents and vulnerabilities available within ENISA data repositories (EUVDDB, CIRAS, CRA SRP) | Incident analysis is included in JCAR as of Q4 2025. CRA SRP AEV and Incidents analysis is included by Q4 2026 |
| | | | Ability of ENISA to publish accurate threat analysis based on Incidents, threat analysis, Vulnerabilities and based on Agency own monitoring , shared by external stakeholders due to legal obligations ²⁰ , or voluntarily shared. | 80% of recipients scores quality of threat analysis provided by ENISA above 4 (1-5) |
| | | | | 80% of recipients scores ability of ENISA to use information available to produce threat analysis and recommendation above 4 (1-5) |
| | | | CRA SRP is established and operational | CRA SRP is used to carry on tasks under CRA by Q4 2026 |

ACTIVITY 5 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ²¹ |
|-------------|----------------------------|------------|------------------|-------------------------|----------------|---------------------------|
|-------------|----------------------------|------------|------------------|-------------------------|----------------|---------------------------|

²⁰ NIS2, CRA and Regulation 2023/2841



| | | | | | | |
|--|--|--|--|--------------------|-------|------|
| 5.1 Collect, organise and consolidate information (including to the general public) on common cyber situational awareness, threat analysis, technical situational reports, incident reports, and support consolidation and exchange of information on strategic, operational and technical levels ^{22 23} | Establishment of a Threat Information Management Platform. Publication of, situational awareness and threat analysis reports, production of briefings and summaries of incidents, , and vulnerabilities Increased understanding and timely access to information regarding latest threats, incidents and vulnerabilities | CSIRT Network, EU CyCLONE, Union entities, National Authorities within MSs subscribed to the reports | Overall stakeholder satisfaction | Bi-annual(survey) | 84% | 85% |
| | | | Timeliness and Accuracy of reports | Bi-annual (survey) | 84,2 | 85% |
| 5.2 Provide analysis and risk assessment (such as JCAR and ETL) jointly with other operational partners including Union Entities, Member States, industry partners, and non-EU partners ²⁴ | Union joint reports and briefings, sectorial analysis, threat analysis ²⁵ Recipients receive accurate and timely assessment of threats faced by the EU Internal Market | CSIRT Network, EU CyCLONE, Union entities, HWPCI, Management Board | Stakeholder satisfaction | Bi-annual (survey) | 84,2% | 85% |
| | | | Number of contributing EU MSs to EU JCAR | Annual (report) | 10 | 15 |
| 5.3 Collect and analyse information to report on the cyber threat landscapes ²⁶ | Mapping threats Generate recommendations for stakeholders to take up | NLO, CSIRTs Network / CyCLONE ISACs Advisory Group | Overall stakeholder satisfaction | Bi-annual (survey) | 91.5% | 90% |
| | | | Number of downloads of ETL | Annual (report) | | +10% |
| 5.4 Analyse and report on incidents as required by Art 5(6) of CSA as well as other sectorial legislations (e.g. DORA, eIDAS Art. 10, etc.) ²⁷ | Analysing incidents Generate recommendations for stakeholders to take up | WS3 of the NISD CG, CNW | Stakeholder satisfaction | Biennial (survey) | 91.5% | >91% |

²² Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1

²⁵ Including JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and CNECT Situation Centre



| | | | | | | |
|--|--|----------------------|--|---------------|------------|---|
| <p>5.5 Establish the CRA Single Reporting Platform operationalize EUVD Services²⁸</p> | <p>CRA SRP platform work is scoped and implementation is initiated</p> <p>Operational and business processes are defined together with primary stakeholder</p> | <p>CSIRT Network</p> | <p>Operational process expected for 2025 are defined</p> <p>CRA Platform is operational</p> <p>EU vulnerability database</p> | <p>Survey</p> | <p>N/A</p> | <p>by 11 Sept 2026</p> <p>Key enhancement validated by stakeholders</p> |
|--|--|----------------------|--|---------------|------------|---|

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. CSIRTs Network members, EU-CyCLONe and NIS Cooperation Group), EU Entities, Other technical and operational blueprint actors, Partnership program for 5.3 (with trusted vendors, suppliers and partners), CTL ahWG

Involve / Engage: Other type of CSIRTs and PSIRTs, private sector industry

ACTIVITY 5 RESOURCE FORECASTS

| | Budget | FTEs |
|---|---|-----------------------------|
| <p>Activity resources from EU subsidy</p> | <p>Budget: € 1.274.000</p> | <p>FTE²⁹: 13</p> |
| <p>Other supplementary contribution</p> | <p>Budget planned for 2026: € 263.806 (outputs 5.1 and 5.2) SitCen Budget, €5.754.460 (output 5.5) to implement CRA SRP tasks + €100.000 CRA preparatory work</p> <p>Total contribution Budget: €447.973 (outputs 5.1 and 5.2) for SitCen Budget €11.947.620 (output 5.5) to implement CRA SRP tasks³⁰ + €400 000 prep work for CRA SRP³¹</p> | <p>FTE: 7³²</p> |

²⁹ Target FTEs

³⁰ please refer to annex XI for further details regarding contribution agreements. The amount indicated refers to years 2026 to 2027.

³¹ Contribution Agreements signed with Commission in 2024, applicable until July 2026.

³² Additional FTE financed via contribution agreements (SitCen and CRA SRP) please refer to annex XI for further details regarding contribution agreements



Activity 6: Provide services for operational assistance and support

OVERVIEW OF ACTIVITY

The activity contributes to further develop response capabilities and preparedness at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity through the implementation and delivery of ex-ante and ex-post services. Following the entry into force of the Cyber Solidarity Act, this activity is tasked with the administration and operationalisation of the EU Cybersecurity Reserve, whose administration and operation has been entrusted by the Commission to ENISA. The Reserve requires delivering incident response services and it also includes carrying out the mapping of the services needed by the users of the Reserve, including the availability of such services from legal entities established and controlled by Member States. The Reserve may also involve the provision of preparedness services closely related to incident prevention and response in the form of conversion of pre-committed incident response services, in cases where the latter have not been consumed in full.

This activity also implements the Cybersecurity Support Action, through which the Agency provides services such as: pentest, threat hunting, risk monitoring and assessment, customized exercise, trainings and supports the Member States with incident response. Following the establishment of the Reserve, the Cybersecurity Support Action will be phased out in 2026, with service delivery expected to end in all MS by end of Q2.

In developing the service delivery framework for the aforementioned services, the Agency worked together with the Commission and the users of the Reserve and Support Action in order to tailor the service catalogue to the needs of the users, while maintaining scalability and flexibility. The Agency also maintains the contractual framework with trusted providers, in accordance with the relevant provisions of the Cyber Solidarity Act, in order to ensure availability of all required services for all types of users, including users outside the MS, such as CERT-EU/Union entities and DEP-associated third countries. In order to strengthen the service delivery framework, the Agency has also implemented a framework to assess the impact of delivered services and has introduced a 24/7 incident support capability.

This activities is resourced through the use of 10 Contract Agents recruited as direct cost of the programme and financed through the Commission contribution agreements. ENISA will not be able to resource this activity with its current establishment plan; it follows, that the conditions of recruitment and employment of these resources will differ from those applying to staff under the establishment plan of the Agency. The budget for this activity is provided via three individual contribution agreements, spanning through mid-2028.

In addition to the aforementioned activities, ENISA will in collaboration with CERT-EU work towards operationalising virtual CISO (vCISO) service to provide advisory services to 3 Agencies conducting Risk Assessments, or full Risk Assessment services, depending on the case.

The activity contributes to the SITAW, NIS, INDEX, TREX service packages.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV

| LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY) | INDICATOR FOR STRATEGIC OBJECTIVES |
|---|--|
| Empowered communities in an involved and engaged cyber ecosystem Effective Union preparedness and response to cyber incidents, threats, and cyber crises | Operationalisation 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 |

ACTIVITY 6 OBJECTIVES

| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|---|--|------------------------|---|------------------|
| By end Q2 2026, deliver and complete the ENISA support action. | Articles 6 and 7 of the CSA | 2026 | Ability of ENISA to support EU Member States to further develop preparedness and response capabilities through implementation and delivery of ex-ante and ex-post services delivery. (survey) Complete tasks on time and in budget. (survey) | 4 (1 to 5 score) |
| By end Q2 2026 and onwards, deploy European Cyber Reserve under CSOA. | Articles 6 and 7 of the CSA | 2026 | Reaching consensus on actions and prioritisation thereof with the EC on European Cyber Reserve. (survey) Timely deliver. (survey) | 4 (1 to 5 score) |

ACTIVITY 6 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ³³ |
|-------------|----------------------------|------------|------------------|-------------------------|----------------|---------------------------|
|-------------|----------------------------|------------|------------------|-------------------------|----------------|---------------------------|

³³ Targets will be established during 2025 once the results of 2024 have materialized

| | | | | | | |
|----------------------------------|---|---------------------------|---|--------|-----|-----------------------------------|
| 6.1 EU Cybersecurity Reserve | Operationalisation of the Reserve and delivery of incident response services to the users of the Reserve, with the possibility of conversion of pre-committed services to incident preparedness and response services | MSs, CNECT, CERT-EU | % of MSs for which the Reserve is operational Satisfaction score | Annual | N/A | 90% of MS 4 (1 to 5 score) |
| 6.2 Cybersecurity Support Action | Delivery of ex-ante and ex-post services until completion of the programme | MSs, CNECT, Beneficiaries | % of MSs receiving service under the Support Action Satisfaction score | | N/A | 80% of MS 4 (1 to 5 score) |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States, Selected Beneficiary Entities, Commission, Union Entities, CERT EU
Involve / Engage: EU-CyCLONe, CSIRT Network, DG CONNECT, NIS Cooperation Group (CG), private sector providers³⁴

ACTIVITY 6 RESOURCE FORECASTS

| | Budget | FTEs |
|------------------------------------|--|---|
| Activity resources from EU subsidy | Budget: N/A | FTEs: 4 |
| Other supplementary contribution | <p>This activity is funded by contribution agreements between ENISA and the Commission. The figures below reflect the direct costs related to the implementation of the contribution agreements³⁵.</p> <p>Budget planned for 2026:</p> <ul style="list-style-type: none"> • €4.562.434 contribution agreement signed in 2023³⁶ • €380.977 contribution agreement signed 2024 • €10.835.869 contribution agreement signed in 2025³⁷ | FTEs: 5 FTEs financed from the Contribution Agreement signed in 2023 and 3 FTEs financed from the Contribution Agreement signed in 2025 |

³⁴ ENISA cybersecurity support action services

³⁵ An additional 7% of the contribution agreements budget is reserved for indirect costs incurred by ENISA for implementing the respective actions. This amount is managed by Activities 9, 10 and 11.

³⁶ please refer to annex XI for further details regarding contribution agreements.



Activity 7 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

In line with political priorities of the new EC established in 2024, development, maintenance and promotion of EU cybersecurity certification framework has high significance given its impact on promoting the EU cybersecurity digital market and overall resilience. As the work on certification expands (not only developing schemes, but as of 2025 EUCC and other schemes will be in force hence they will require maintenance, promotion and supporting NCCAs (National Cybersecurity Certification Authorities) with capacity building and uptake initiatives), it is essential to ensure that this Activity is well resourced to cater for the additional streams of work.

This activity encompasses actions that seek to establish and support the EU cybersecurity certification framework by preparing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commissioner on the basis of the Union Rolling Work Program (URWP) or, in duly justified cases, at the request of the Commission or the European Cybersecurity Certification Group (ECCG). This also includes in particular the activities related to the ID Wallet certification as a priority, and other schemes under development (EUCCS, 5G), as well as the activities in view of the 2025 request on Managed Security Services (MSSs) following entry into force of the CSA amendment. Actions also include supporting the maintenance and review, as well as evaluating adopted European cybersecurity certification schemes, in particular the adopted EUCC, as well as capacity building for National Cybersecurity Certification Authorities (NCCAs) and supporting the peer review mechanism in line with the CSA and related implementing regulation. In addition, in this activity, ENISA assists the Commission with regard to the European Cybersecurity Certification Group (ECCG) and existing ECCG sub-groups (EUCC review and maintenance; peer reviews; cryptographic mechanisms) as well as with co-chairing and providing secretariat to the Stakeholder Cybersecurity Certification Group (SCCG).

ENISA has developed one candidate scheme based on an EC request from 2019, in accordance with Art 49.2, which was adopted as Implementing Regulation, the EUCC. ENISA is currently developing 4 other candidate schemes also based on EC requests, the EUCCS, the EUMSS, the EUDIW and the EU5G, in accordance with Art 49.2. The URWP was adopted in Feb 2024, and the most recent request received for the development of an EUDI wallet candidate scheme is in line with Art 49.1; the request for an EU scheme on MSS is in line Art. 48.2, as foreseen by the URWP and the amendment to the CSA, based on the ENISA feasibility study. ENISA also explores feasibility studies on other topics listed in the URWP but for which no candidate scheme request is formally issued, in order to facilitate the delivery of the candidate schemes once the request has been received.

As certification schemes become adopted, with EUCC being the first one in 2024, maintenance activities of schemes will require continuous efforts on behalf of ENISA, in addition to the resources to be allocated to newly requested schemes. Given the finite resources of ENISA, conducting both actions (development and maintenance) would impose a strain on ENISA resources and accordingly respective actions to compensate by deprioritising actions might be needed.

ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Article 50 of the CSA. As of 2024, ENISA seeks to gradually support the cybersecurity certification stakeholders with an online platform that has been set up by the Commission. Furthermore, ENISA contributes to the cybersecurity framework by analysing pertinent market aspects of certification as well as aspects related to the interplay with existing legislations, in particular the Cyber Resilience Act. Other relevant legislations include NIS2, DGA EUDI Wallet, AI Act, Chips Act, Data Act.

The activity leads the CERTI service package and contributes to the NIS service package.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV.

| Link to strategic objectives (ENISA STRATEGY) | Indicator for strategic objectives |
|--|--|
| Empowered communities in an involved and engaged cyber ecosystem Building trust in secure digital solutions | Number of EU certification schemes developed and maintained, number EU regulations making reference to CSA, number of active Member States' NCCAs (e.g. issuing European certificates) |

ACTIVITY 7 OBJECTIVES

| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|---|--|------------------------|---|---|
| Between 2025-2027, timely development of feasibility studies for future potential schemas | CSA, Art. 49 | 2027 | Number of feasibility studies concluded in view of upcoming requests | 3 (pending potential new requests for scheme) |
| | | | Elements of feasibility study reflected/aligned in EC request for new schemes | More than 50% |
| Between 2025-2027, timely finalisation of candidate schemes following formal requests | CSA, Art. 49 | 2027 | Number of drafts of certification schemes delivered to COM (ID Wallet | 2 |

| | | | | |
|---|--------------|------|--|---|
| for drafting new cybersecurity certification schemas | | | Certification and Managed Security Services | |
| | | | ECCG endorsement of draft certification schemes | Positive ECCG endorsement |
| | | | SCCG satisfaction on draft certification schemes (satisfaction survey) | More than 60% |
| Ensure the maintenance of existing schemes and support their roll-out | CSA, Art. 49 | 2027 | Number of schemas maintained with ENISA active involvement | 1 (EUCC) |
| | | | Satisfaction by ECCG on ENISA supporting efforts for documents for maintenance | 75% |
| | | | Number of certificates issued and published under an EU certification scheme; high utilisation rate in the market. | Proportionate ³⁸ number of certificates issued migrating to a new EUCC scheme compared to previous framework |

ACTIVITY 7 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ³⁹ |
|--|---|---|--|-------------------------|---|--|
| 7.1 Drafting and contributing to the preparation (via inter alia feasibility studies) and establishment of candidate cybersecurity certification schemes ⁴⁰ | Scheme meets stakeholder requirements, notably of the Member States and the Commission Take up of schemes by stakeholders Timely delivery by ENISA of all | Ad hoc working groups on certification ECCG European Commission | Stakeholder satisfaction | Biennial (survey) | 72% | 5% increase compared to latest results |
| | | | Number of opinions of stakeholders managed | Annual (report) | 27 MS and the Commission delivered through ECCG | 5% increase compared to latest results |

³⁸ ENISA monitors the certificates issued under SOG-IS and transition to EU CC will have to be proportional to the number of certificates issued.

⁴⁰ notably on the EU Digital Identification Wallets (EUDIW) and Managed Security Services (MSS)



| | | | | | | |
|---|--|--|--|--------------------|---|--|
| | schemes requested in cooperation with the Commission Statutory Bodies and ad hoc Working Groups actively involved | | Number of people/organizations engaged in the preparation of certification schemes | Annual (report) | EUCS scheme: 17 EU5G: 25 EUDI Wallet: 25 MS: 15 | 5% increase compared to latest results |
| 7.2 Implementing and maintaining of the established schemes including evaluation of adopted schemes, reviews and updates of state-of-the-art documents etc. monitoring the dependencies and vulnerabilities of ICT products and services | Review of schemes to improve efficiency and effectiveness Take up of schemes by stakeholders | ECCG European Commission | Stakeholder satisfaction | Biennial | 72% | 5% increase compared to latest results |
| | | | ECCG satisfaction of ENISA efforts on schemes adopted | Triennial (survey) | N/A | 5% increase compared to latest results |
| 7.3 Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks; supporting peer reviews and capacity building of NCCAs. | | ECCG European Commission SCCG NCCAs | Stakeholder satisfaction | Biennial | 72% | 5% increase compared to latest results |
| | | | Feedback from statutory bodies including NCCAs on ENISAs role | Annual (survey) | 72% | 5% increase compared to latest results |
| | | | Satisfaction of ENISAs role in NCCA peer reviews | Triennial (survey) | n/a | 5% increase compared to latest results |
| 7.4 Developing and maintaining the necessary provisions and tools and services concerning the Union's cybersecurity certification framework (incl. certification website, support the Commission in relation to the core stakeholders service platform of CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework etc.) | Supporting in transparency and trust of ICT products, services and processes Stakeholders engagement promotion of certification | ECCG European Commission SCCG | Stakeholder satisfaction | Biennial | 72% | 5% increase compared to latest results |
| | | | Users satisfaction concerning the certification website services | Annual (survey) | N/A | 5% increase compared to latest results |
| | | | Usage of certification website | Annual (report) | N/A | 75% |
| 7.5 Promoting and monitoring the uptake of certification and interplay with other legislative files (e.g. CRA, AI Act, etc.) | Increase in uptake of certification Increase in NCCAs maturity | ECCG European Commission NCCAs | Composite indicator on number of issued certificates and their use | Annual | N/A | TBD |
| | | | Stakeholder satisfaction | Biennial | 72% | 5% increase compared to latest results |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. National Cybersecurity Certification Authorities, ECCG), European Commission, Union institutions, bodies, offices and agencies
Selected stakeholders as represented in the SCCG

Involve/ Engage: Private Sector stakeholders with an interest in cybersecurity certification, Conformity Assessment Bodies, National Accreditation Bodies
Consumer Organisations

ACTIVITY 7 RESOURCE FORECASTS

| | | |
|--|--------|------|
| | Budget | FTEs |
|--|--------|------|



| | | |
|---|-------------------|------------------------|
| <i>Activity resources from EU subsidy</i> | Budget: € 631.610 | FTE ⁴¹ : 10 |
|---|-------------------|------------------------|

⁴¹ Target FTEs

Activity 8 Supporting market, technology and product-security

OVERVIEW OF ACTIVITY

This activity seeks to foster the cybersecurity of technologies, products and services in the European Union along with the development of the cybersecurity market, -industry and -services, in particular SMEs and start-ups, to foster cybersecurity competitiveness, strengthen EU single market and increase the capacity of the Union to reinforce supply chains to the benefit of the internal market. It involves actions to promote and implement 'security by design' and 'security by default' measures in (a) new emerging technologies (including supporting MS and the COM in tackling challenges regarding AI and post-quantum cryptography and 6G) and in (b) ICT products, services and processes, including through development and assessment of technical guidance/specifications, standardisation and adoption of relevant codes of conduct. As such, this activity will support the development of good cybersecurity engineering practices for products, services and technologies. In doing so, the activity will also build an effective role of ENISA in supporting CRA implementation notably in terms of the assessment of draft European harmonised standards, the assessment and the development of technical guidance, market analysis, preparation of conformity assessment and market surveillance activities and collection and analysis of information for the identification of emerging cybersecurity risks in products with digital elements, etc. Preparatory and support actions in view of CRA will continue to increase in the coming years, particularly in the support of MS market and notifying authorities for the Commission and technical advice for implementation to manufacturers, including SMEs.

The actions to support this activity include producing analyses, including standardisation landscape and gap analysis, and guidelines as well as good practices on cybersecurity and data protection requirements, facilitating the assessment, establishment and take up of European and international standards across applicable areas such as for risk management as well as performing regular analysis of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein, as well as reported incidents. The activity aims at strengthening and reinforcing ties with the private sector and promote collaboration among the cybersecurity market players, in order to improve visibility and uptake of trustworthy and secure ICT solutions in the digital single market.

In parallel, the activity aims to provide advice to EU Member States (MS), EU institutes, bodies and agencies (Union Entities) on research needs and priorities in the field of cybersecurity, thereby contributing to the EU strategic research and innovation agenda, notably the ECCC. The ecosystem of the ECCC and the National Coordination Centres (NCCs) will be consulted for these actions. A strong collaboration and mapping of relevant requirements of the market authorities as defined in the CRA will also take place in the context of this activity. To prepare this strategic advice, ENISA will take full account of past and ongoing research, development and technology assessment activities, outputs of other statutory bodies of the cybersecurity landscape such as the NIS Cooperation Group, the CRA Administrative Cooperation Groups (Market surveillance authorities), ECCG, CSIRTs Network, EU-CyCloNe and scan the horizon for emerging and future technological, societal and economic trends that may have an impact on cybersecurity. In this respect, lessons learned and trends from reported incidents and vulnerabilities will also be utilised. ENISA will establish a technology and innovation radar to support these activities.

The activity also encompasses ENISA's support to the European Digital Identity Regulation and the European Digital Identity Cooperation Network, by providing advice and upon request targeted guidelines in order to ensure deployment and uptake of secure digital wallet solutions, as well as foster the trusted services ecosystem.

Finally, this activity supports conformity assessment, also cybersecurity certification, of products with digital elements by monitoring standardisations being used by European cybersecurity of digital products and certification schemes respectively, and by recommending appropriate technical specifications where such standards are not available.

This activity contributes to the INDEX, SITAW, TREX and CERTI service packages.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex XV.

| Link to strategic objectives (ENISA STRATEGY) | Indicator for strategic objectives |
|--|---|
| <p>Empowered communities in an involved and engaged cyber ecosystem</p> <p>Building trust in secure digital solutions</p> <p>Foresight on emerging and future cybersecurity opportunities and challenges</p> | <p>Rate of satisfaction with ENISA's support to the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG)</p> <p>Number of advise and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC</p> |

ACTIVITY 8 OBJECTIVES

| DESCRIPTION | CSA article and other EU policy priorities | TIMEFRAME OF OBJECTIVE | INDICATOR | TARGET |
|---|--|------------------------|-----------------------------------|---|
| By [end 2026] implement a 'market' monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, reports on the trustworthiness of products with digital elements under CRA, including important critical products | CSA Article 8, CRA Articles 52, 59, 60, 8 | 2026 | Timeliness of ENISA reports | Reports delivered on time |
| | | | Acceptance of ENISA reports by MS | 2/3 of MS acknowledging the ENISA reports |



| | | | | |
|---|-----------------------------|------|--|---|
| | | | Validity of ENISA framework | 2/3 MS validating and endorsing ENISA framework |
| Provide continuous comprehensive support to MS market surveillance and notifying authorities and to the COM and manufacturers including SMEs for implementing CRA requirements. | CRA Articles 29, 52, 59, 60 | 2026 | MS and COM stakeholder satisfaction survey | More than 70% |
| Create a technology & innovation radar, to understand the level of impact that new technologies have on cybersecurity | CSA Art. 9, 11 and CRA | 2026 | Number of cybersecurity trends and patterns identified through an evidence-based methodological approach | 5% increase over reference data |
| | | | EU cybersecurity R&I impact assessment | 5% increase over reference data |

ACTIVITY 8 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | Target 2026 ⁴² |
|--|--|--|---|------------------------------|----------------|---------------------------------|
| 8.1 Collect and analyse information on new and emerging information and communications technologies (notably AI and PQC), support the COM and MS with appropriate technical guidelines as necessary, and provide strategic advice to ECCC on the EU agenda on cybersecurity research, innovation and deployment. ⁴³ | Identifying current and emerging ICT gaps, trends, opportunities and threats and providing guidelines thereof Advising EU Funding programmes including the ECCC and its Strategic Agenda and Action Plan. | Academia, Industry and National R&I, MS market authorities Entities (including NCCs) and Union Entities NIS CG, EC including CNECT and JRC, ECCC and NCCs, as appropriate | Stakeholder satisfaction | Biennial (survey) | 91% | 5% increase over reference data |
| | | | Findings endorsed by MS (NCCs and market authorities) | Annual | N/A | 5% increase over reference data |
| | | | Guidelines issued and endorsed by NIS CG | as relevant | N/A | 5% increase over reference data |
| | | | ECCC Strategic Agenda and Action Plan alignment | Annual (survey with ECCC GB) | N/A | 5% increase over reference data |
| 8.2. Market analysis on the main trends in the cybersecurity market on both the demand and supply side, and prepare the framework for the biennial technical report on emerging trends regarding | Improved understanding of the market / industry | Ad hoc working groups cybersecurity market analysis Advisory Group | Stakeholder satisfaction | Biennial (survey) | 88% | 5% increase over reference data |



| | | | | | | |
|--|---|--|---|---|-----|---------------------------------|
| cybersecurity risks in products with digital elements ⁴⁴ | Framework for the ENISA biennial technical report under CRA | NLO (as necessary) MS Market surveillance authorities (as necessary) | Cybersecurity market analysis; cybersecurity product and services | Annual (framework and reports)) | N/A | 5% increase over reference data |
| | | | Endorsement by MS of report on emerging trends regarding cybersecurity risks in products with digital elements | Biennial (report) | N/A | 5% increase over reference data |
| 8.3 Support to the implementation of CRA, including assessment of standards and technical guidance, activities of market surveillance authorities and identification of categories of products for simultaneous coordinated control actions and upon request, conduct evaluations of products that present a significant cybersecurity risk. | <p>Assessment of 41 vertical and horizontal standards (CRA standardisation request)</p> <p>Monitoring and following-up on requirements of market surveillance authorities</p> <p>Identify categories of products; produce a methodology for market surveillance and product testing, including in view of market sweeps; carry out market sweeps</p> <p>Technical recommendations on conformity assessment, including in view of notification of CABs under the CRA</p> <p>Technical guidance for the security-by-design and security-by-default principles including for SMEs</p> <p>Evaluations to be carried out ideally on the basis of input from market</p> | <p>MS Market Surveillance Authorities</p> <p>NLO</p> <p>Commission</p> <p>MS Notifying authorities</p> <p>CRA Expert group</p> | <p>Collection of requirements</p> <p>Matching requirements with deliverables</p> <p>Time to carry out market sweeps</p> <p>Methodology for evaluations</p> <p>Profiles of experts</p> | <p>Assessment of standards on continuous basis starting in 2025</p> <p>Security-by-design and security-by-default technical guidelines (reports, checklists) to be issued in 2026 and updated on continuous basis</p> <p>ENISA SME strategy for the CRA in 2026 and updated on continuous basis</p> <p>Technical support & recommendations on conformity assessment to be issued in 2026 and updated on continuous basis</p> <p>Market sweeps as of 2027 (3-years transition) or earlier if requested</p> <p>Method to evaluate products in 2026, to be updated regularly</p> <p>Guidance and criteria to accept evaluation results in 2026</p> | N/A | 5% increase over reference data |

⁴⁴ The biennial report is a statutory task for ENISA as per Art. 14 of CRA, the first report is expected 2 years after CRA enters into force



| | | | | | | |
|--|---|---|--|--------------------------------|-----|---------------------------------|
| | sweeps; rely on external expertise. | | | to be updated on regular basis | | |
| 8.4 Monitoring developments in related areas of standardisation, analysis of standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification | Monitoring of cybersecurity standardisation activities Input to the EU standardization agenda | CEN/CENELEC/ETSI European Commission Ad hoc working groups (as necessary) Advisory Group NLO (as necessary) | Stakeholder satisfaction | Biennial (survey) | 88% | 5% increase over reference data |
| | | | Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification. | Annual (report) | N/A | 5% increase over reference data |
| 8.5 Supporting the implementation of eIDAS2 Regulation and the deployment and uptake of European Digital Identity Wallets | Best practices and guidelines to support implementation of eIDAS 2 Monitoring of the uptake of Digital Wallets | European Digital Identity Cooperation Network EC | Stakeholder satisfaction | Annual (survey) | | 5% increase over reference data |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. market surveillance authorities and entities with an interest in cybersecurity market monitoring e.g. NCCA, National Standardisation Organisations), European Commission, Union institutions, bodies, offices and agencies, European Standardisation Organisations (CEN, CENELEC, ETSI), Private sector or ad hoc Standards Setting Organisation, EC Joint research centre, National and EU R&I Entities, Academia and Industry, European Cybersecurity Competence Centre and National Cybersecurity Coordination Centre's, EC AI Office, European Digital Identity Cooperation Group, European Data Innovation Board.

Involve / Engage: Private Sector stakeholders via ad hoc working groups, International Organisation for Standardisation / International Electrotechnical Committee, Consumer Organisations, EDPS, EDPB.

ACTIVITY 8 RESOURCE FORECASTS

| | Budget | FTEs |
|------------------------------------|-------------------|------------------------|
| Activity resources from EU subsidy | Budget: € 578.200 | FTE ⁴⁵ : 10 |

3.2 CORPORATE ACTIVITIES

Activities 9, 10 and 11 encompass enabling actions that support the operational activities of the agency.

Activity 9: Performance and sustainability

OVERVIEW OF ACTIVITY

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 9 ANNUAL OBJECTIVES

| DESCRIPTION | LINK TO CORPORATE OBJECTIVES | ACTIVITY INDICATORS | FREQUENCY (DATA SOURCE) | LATEST RESULT | TARGET |
|--|--|--|-------------------------|---------------------|--------------------------------|
| 9.A Enhance corporate performance and strategic planning | Ensure efficient corporate services | Proportion of SPD KPIs meeting targets | Annual | 73% | >80 of indicators outperformed |
| | Continuous innovation and service excellence | Results of Internal control framework assessment | Annual | Effective (Level 2) | Effective level 1or 2 |



| | | | | | |
|---------------------------------------|---|---|--------|--|---|
| | Developing service propositions with additional external resourcing | High satisfaction with essential corporate services in the area of compliance and coordination | Annual | 75% | >60% |
| 9.B Increase corporate sustainability | Ensure climate neutral ENISA by 2030 | Maintain EU Eco-Management and Audit Scheme (EMAS) | Annual | EMAS audit conducted on 27/2/25 | Timely implementation of follow up actions to ensure EMAS certification is maintained |
| | Develop efficient framework for ENISA continuous governance to safeguard high level of IT | Agency IT strategy aligned with corporate strategy Proportion of total IT budget allocated to information security proportional to the level of risks identified across IT systems within Agency | Annual | Revised IT strategy proposal submitted end 2024; strategy to be adopted by Q2 2025 18 % of total IT costs | 70% implementation (ITMC reporting) 20% |

ACTIVITY 9 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ⁴⁶ |
|---|---|--|---|-----------------------------------|----------------|---|
| 9.1 Coordinate the implementation of the Agency's performance management framework, including Agency wide budget management and IT management processes, environmental management and regulatory compliance | Unified day to day practices across the agency upon implementing SPD Annual risk assessment and internal controls assessment performed and reported Legal and regulatory compliance are monitored; issues and areas of improvement identified. Streamlined IT system management across the Agency and in accordance with | MT, ITMC & BMC External and internal audits Statutory bodies | Number of high risks identified in annual risk assessment | Annual (survey, internal reports) | 3 | <3 30% reduction of high risks identified in previous year |
| | | | Effective monitoring of high risks and critical recommendations to follow up on timely implementation of mitigation measures by | | N/A | Risk plans are timely generated, agreed with risk owners and reported to MT (at least |

⁴⁶ Targets will be established during 2025 once the results of 2024 have materialized



| | | | | | | | |
|---|---|--------------------------------------|---|--|--|---|---|
| | <p>ENISA's IT strategy; under ITMC</p> <p>Streamlined budget management across the Agency; under BMC</p> <p>Maintenance of EMAS Certificate</p> | | Business Owners | | | quarterly basis) | |
| | | | Percentage of identified internal controls deficiencies addressed within timelines | | | no critical recommendation issued in 2023 ICF assessment. Out of 3 moderate and 2 major – the recommendations remain valid as the deficiencies have not been fully mitigated. | 100 % for critical, 80 % for major, 60 % for moderate |
| | | | Timely follow-up and resolution of internal and external audits (in particular from IAS and ECA) recommendations and findings | | | | <180 days |
| | | | Number of identified regulatory breaches | | | 3 | 0 for critical/major, <=3 for moderate |
| | | | Percentage of revised and up to date corporate rules (MBD, EDD, policies, processes) | | | 23 MBDs on corporate rules from before 2019 | 60 % corporate rules which have not been reviewed less than three years ago; 80 % corporate rules which have not been reviewed less than four years ago |
| Annual report on ARES maintenance and actions | N/A | Follow up of maintenance and actions | | | | | |

| | | | | | | |
|--|--|--|---|--------|--|---|
| | | | Reduction of CO2 emissions in ENISA HQ | | N/A | Timely submission of report with actions and recommendations |
| | | | Efficiency and effectiveness of ITMC & BMC (survey) | | TMC: 75 % BMC: 63 % | >60 % |
| 9.2 Maintain and enhance ENISA's cybersecurity posture in line with the Agency's multiannual cybersecurity maturity plan (2026 – 2028) | <p>Compliance with Regulation (EU) 2023/2841 on a high common level of cybersecurity within Union entities</p> <p>Timely identification and response to cybersecurity risks</p> <p>Continuous monitoring of IT systems cybersecurity and timely identification of issues and areas of improvement (first level and second level controls)</p> <p>Coordination and implementation of the cybersecurity maturity plan of the Agency for 2026</p> | <p>MT and relevant committees</p> <p>Statutory bodies</p> <p>Interinstitutional Cybersecurity Board (IICB)</p> <p>External and internal audits</p> | Percentage of identified high risk mitigation measures addressed within timelines | annual | All high risks addressed within timelines and/or accordingly reported and planned | >90% |
| | | | Annual risk assessment (RA) and risk treatment plan with the relevant Business Owners | annual | NA | RA and risk treatment plans conducted timely and in line with Regulation (EU) 2023/2841 |
| | | | Cybersecurity measures implemented according to maturity plan and for set timelines | annual | NA | Measures and timelines in accordance with the cybersecurity masterplan |
| | | | Address all potential cybersecurity incidents | annual | NA | All cybersecurity incidents addressed in timely way |
| | | | Cybersecurity trainings for staff and managers | annual | Two training sessions by ISO; training programme and phishing exercise (via dedicated training platform) | >2 training sessions by ISO |
| 9.3 Provide support services in the EU Agencies network and in key areas of the Agency's expertise | Shared services in the area of data protection, legal services and accounting | MT, BMC EUAN (Agencies receiving) | Satisfaction within the EU Agency network with | annual | High satisfaction expressed | 70% satisfaction for the services |



| | | | | | | |
|--|---|---------------------|--|--------|--|--|
| | EUAN troika shared services pilot | ENISA's support) | ENISA support services | | sed by the agencies that received ENISA's services | offered under the EUAN Shared Services Pilot (survey) |
| 9.4 Ensure the implementation of single administration processes across the Agency | Streamlined document management practices | MT, Staff committee | Percentage of staff considering that the information they need to do their job is easily available/accessible within ENISA | Annual | 66% of staff survey respondent agree that ENISA's internal communication is timely and clear (result of last year was 39%) | 50% |
| | | | Response timeliness to external parties (internal reporting) | Annual | High response rates in accordance with ENISA's code of conduct | High response rates in accordance with ENISA's code of conduct |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Agencies Network, relevant Union entities and European Commission, Interinstitutional Cybersecurity Board, Staff Committee, Management Team

ACTIVITY 9 RESOURCE FORECASTS

| | Budget | FTEs |
|---|--|-----------------------|
| Total activity resources | Budget: €432.000 | FTE: 15 ⁴⁷ |
| Other supplementary contribution | Budget: €54.604 SLA with ECCC, see annex XI for additional information | FTE: |

⁴⁷ Target FTEs Including ED, COO, ACOO and accounting officer



| | | |
|--|-----------------------------------|--|
| | Budget: € 1.269.100 ⁴⁸ | |
|--|-----------------------------------|--|

Activity 10: Reputation and Trust

OVERVIEW OF ACTIVITY

This activity seeks to meet requirements set out in 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 that a transparent and proactive approach is taken to maximise the quality and value provided to stakeholders. It also includes contribution to efficiency gains, by optimising the way it engages with stakeholders and offering on demand driven services in addition to the essential services to increase the Agency’s outreach.

The Agency can further build its reputation as trusted entity through consistent messaging, adherence to corporate rules for communications activities and improving knowledge sharing internally and externally.

The legal basis for this activity is Art 4(1), Section 1 and 2 as well as Art 21, 23 and Art 26 of the CSA, the latter of which strongly focuses on ensuring that the public and any interested parties are provided with appropriate, objective, reliable and easily accessible information.

ACTIVITY 10 ANNUAL OBJECTIVES

| DESCRIPTION | LINK TO CORPORATE OBJECTIVES | ACTIVITY INDICATORS | FREQUENCY (DATA SOURCE) | LATEST RESULT | TARGET |
|--|-------------------------------------|--|-------------------------|---------------|---------------------------|
| 10.a Protect and grow the Agency’s brand | Ensure efficient corporate services | Level of trust in ENISA (as per Biannual Stakeholder Survey) | Biennial | 95% | 95% |
| 10.b Improve outreach of ENISA’s mandate | Ensure efficient corporate services | | | | |
| | | Stakeholder satisfaction with ENISA events | Annual | 88% | >80% |
| | | Number of unique website visitors | Annual | N/A | >5% increase year on year |

ACTIVITY 10 OUTPUTS

⁴⁸ Budget from contribution agreements forecasted for implementation of cybersecurity maturity plan led by activity 9 with support from activity 4 and 11. Please see annex XI for further information

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 |
|---|--|--|---|----------------------------|--|---------------------------|
| 10.1 Review and implement the multiannual communications strategy and support stakeholders' strategy including corporate outreach | <p>Enhanced transparency and outreach</p> <p>Engaged communities</p> <p>Increased impact of ENISA activities</p> <p>Relevant and easily accessible information is provided to stakeholders</p> <p>Successful EUAN leadership, communications and EUAN yearly meetings</p> | Management Team and agency stakeholders | | | | |
| | | | Number of social media engagement | Annual (Media monitoring) | 66.3k | 68k |
| | | | Stakeholder satisfaction with ENISA outreach | Biennial (survey) | 96% | >80% |
| | | | Number of total ENISA website visits | Annual (website analytics) | 2.3 million | 1.5 million ⁴⁹ |
| 10.2 Implement internal communications strategy | Engaged staff | Management Team and staff committee | Staff satisfaction with ENISA internal communications | Annual (survey) | 65% | >70% |
| 10.3 Manage and provide the secretariat for statutory bodies, i.e. EB, MB, AG, NLO (excluding certification) | <p>Support the operation and organisation of ENISA statutory bodies</p> <p>Support effectiveness of implementation of work programme (validation of operational outputs)</p> <p>Providing administrative support for the day to day working of the</p> <p>Management board decisions and recommendations from NLO & AG</p> | Statutory bodies, Management Team and Committees | Number of feedback instantiations received per NLO consultation | Annual (Internal report) | 27 for NLO subgroups (3.6 as average for validations in NLO Network) | >6 |
| | | | Number of feedback instantiations received per AG consultation | Annual (Internal report) | 11.3 on average | >8 |
| | | | Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA | Annual (Survey) | 97% | >80% |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: Members of statutory bodies such as Management Board, Advisory Group and National Liaison Officers, Union Entities Network, relevant Union entities and European Commission, Staff Committee, Press

⁴⁹ New website and analytics have impacted measurement.

Involve / Engage: All ENISA stakeholders

ACTIVITY 10 RESOURCE FORECASTS

| | Budget | FTEs |
|--------------------------|----------------------------------|------------------------|
| Total activity resources | Budget: €1.270.815 ⁵⁰ | FTE ⁵¹ :7.5 |

Activity 11 Effective and efficient corporate services

OVERVIEW OF ACTIVITY

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 can grow, stay motivated, and remain engaged. A key priority is competency development, 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.

At the same time, ENISA will continue to strengthen its secure operational environment to the highest standards. It will also explore cloud-based services that meet European and international standards, in line with the ENISA IT strategy.

The activity is responsible for decommissioning the Heraklion data center before end of Q2 2026 and its migration.

ACTIVITY 11 ANNUAL OBJECTIVES

| DESCRIPTION | LINK TO CORPORATE OBJECTIVES | ACTIVITY INDICATORS | FREQUENCY (DATA SOURCE) | LATEST RESULT | TARGET |
|--|--|---|-------------------------|---|--|
| 11.a Enhance people centric services by implementing the Corporate and HR strategy | Effective workforce planning and management | Implementation of Strategic Workforce Planning and Review decisions | Annual | Fully implemented | Fully implemented |
| | Efficient talent acquisition, development and retainment | Implementation of the Corporate and HR strategy | | Vacated staff posts in 2024 were fulfilled within 143 days. The indicated KPI was to fulfil posts within 300 days | Proposal new KPI: Vacated post are completed within 200 days (provide update on new & revisions): Policies introduced Policies updated |
| | Caring and inclusive modern organisation | | | | |

⁵⁰ Including the budget centralized for operational missions and large-scale events

⁵¹ Target FTEs



| | | | | | |
|--|---|--|--------|--|---|
| | | | | | Related MB decisions Related ED decisions |
| | | High participation in staff satisfaction survey | | 80 % | 75 % participation rate |
| 11.b Ensure sustainable and efficient corporate solutions and promote continuous improvement | <p>Ensure efficient corporate services</p> <p>Introduce digital solutions that maximise synergies and collaboration in the Agency</p> <p>Developing service propositions with additional external resourcing</p> <p>Promote and enhance ecologic sustainability across all Agency's operations</p> <p>Develop efficient framework for ENISA continuous governance to safeguard high level of IT and physical security</p> | Implement best practices in sustainable IT solutions | Annual | Fully implemented according to plan | IT strategy updated accordingly |
| | | Limited disruption of continuity of corporate services | Annual | Effective disaster recovery is in place to ensure the Business Continuity Plan of core services. | BCP for corporate IT, facilities, financial and HR services in 2025 |
| | | Handling EU CI at the level of SECRET UE/EU SECRET | Annual | EU CI inspection took place and the report will be sent in 2025. | Operational for the first full year, in 2025 |

ACTIVITY 11 OUTPUTS

| DESCRIPTION | EXPECTED RESULTS OF OUTPUT | VALIDATION | OUTPUT INDICATOR | FREQUENCY (DATA SOURCE) | LATEST RESULTS | TARGET 2026 ⁵² |
|--|---|---|---|-------------------------|----------------|---------------------------|
| 11.1 Manage and provide horizontal, recurrent, administrative services in the area of HR, Finance and Procurement for ENISA staff and partners | <p>Services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently.</p> <p>Implementation of the Unit's annual plan in procurement, L&D, recruitment</p> <p>Set up a Service Level Agreement in areas of HR, Finance, Procurement & Contract Management</p> <p>Establish reporting capabilities in areas of HR, Finance and Procurement (monthly HoUs, quarterly SLT)</p> <p>Introduce MS planner to all CSS services to capture workload indicators</p> <p>Introduce ServiceNow as main ticketing system across all CSS services</p> <p>Expand Service Catalogue to PMO and DG HR</p> <p>Review ENISA CSS inet page</p> | <p>Management Team</p> <p>IT Management Committee</p> <p>Budget Management Committee</p> <p>Staff Committee</p> | Turnover rates | Annual | 4.1% | <5% |
| | | | Establishment plan posts filled | | 98% | >95% |
| | | | Percentage of the implementation of approved Recruitment plan | | 94% | >90% |
| | | | Percentage of the implementation of approved Procurement Plan | | 63.63% | >90% |
| | | | Percentage of budget implementation | | 100% | >95% |
| | | | Average time for initiating a transaction (FIA role) | | 7.51% | <7 days |

⁵² Targets will be established during 2025 once the results of 2024 have materialized



| | | | | | | |
|--|--|--|---|--------|------|---------|
| | | | Average time for verifying a transaction (FVA role) | | 0.19 | <3 days |
| 11.2 Implement Agency's Corporate strategy including HR strategy with emphasis on talent development, growth and welfare | <p>Objectives and goals set out in the corporate and HR strategy are met</p> <p>Launch and evaluation of Staff Satisfaction Survey</p> <p>Implementation of the ED decision on annual workforce review [adopted in April 2024]</p> <p>Revision of following policies:</p> <ol style="list-style-type: none"> 1/ Recruitment & External Mobility 2/ Staffing 3/ Wellbeing & Medical 4/ Probation 5/ MB SNE rules 6/ Amendment Financial Regulations 7/ Management of Indirect costs 8/ Reimbursement of Experts 9/ Physical Security and Access Control 10/ Incident Reporting and Facility Fault Response 11/ Evacuation and Preparedness (Priority 2025) 12/ L & D policy 13/ Trainee policy 14/ Stand-by duty policy | <p>Management Board</p> <p>Management Team</p> <p>Staff Committee</p> <p>EUAN</p> <p>BMC</p> | Number of policies/IR reviewed/ processes revised | Annual | 10 | > 10 |
| | | | Percentage of staff satisfaction with talent development | | 52% | > 50 % |
| | | | Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time | | <10 | <10 |
| | | | Number of implemented competency driven training and development activities | | <10 | < 10 |
| | | | Number of multisource feedback evaluations implemented and followed up | | 16 | > 5 |
| 11.3 Manage and provide horizontal, recurrent support services in the area of facilities, | | Management Team | Staff satisfaction with working environment | Annual | 80 % | >70% |

| | | | | | | |
|---|---|--|---|--------|---------|-------------------------------------|
| security and corporate IT for ENISA staff and partners | Services such as corporate IT, facilities and security are performed efficiently with minimal disruption. | IT Management Committee | Time to respond to IT, safety and security incidents. | | n/a | <3 to respond |
| | Decommission data centre in Heraklion & program manage new data center | Budget Management Committee Staff Committee | Average time to respond to facilities management requests | | 2 days | <1 to acknowledge and <3 to respond |
| | Program to manage EC tools of SUMMA & HRT transition | | | | | |
| | Expand Service Now (Finance, Procurement, HR, Reporting) | | | | | |
| | Improve Physical security services | | | | | |
| 11.4 Enhance operational excellence and digitalisation through modern, safe secure and streamlined ways of working and introducing self-service functionalities | Service such as access management, meeting room facilities, equipment renewal, cloud-based solutions and data availability are efficient. | Management Team IT Management Committee | Critical systems uptime/downtime | Annual | 100 % | 99 % |
| | | | Staff satisfaction with IT resolution | | 82.53 % | 85 % |

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: ENISA staff members and EU Entities

Involve / Engage: Private Sector and International Organisations

ACTIVITY 11 RESOURCE FORECASTS

| | Budget | FTEs |
|--------------------------------|----------------------------------|--------------------------|
| Total activity resources | Budget: €4.495.624 ⁵³ | FTE ⁵⁴ : 21.5 |
| Other supplementary agreements | Budget: € 320.900 ⁵⁵ | |

⁵³ Excluding staff in active employment and recruitment expenditure including 414.500 euros from C1 for data centre migration

⁵⁴ Target FTEs

⁵⁵ Budget from contribution agreements forecasted for date centre migration. Please see annex XI for further information



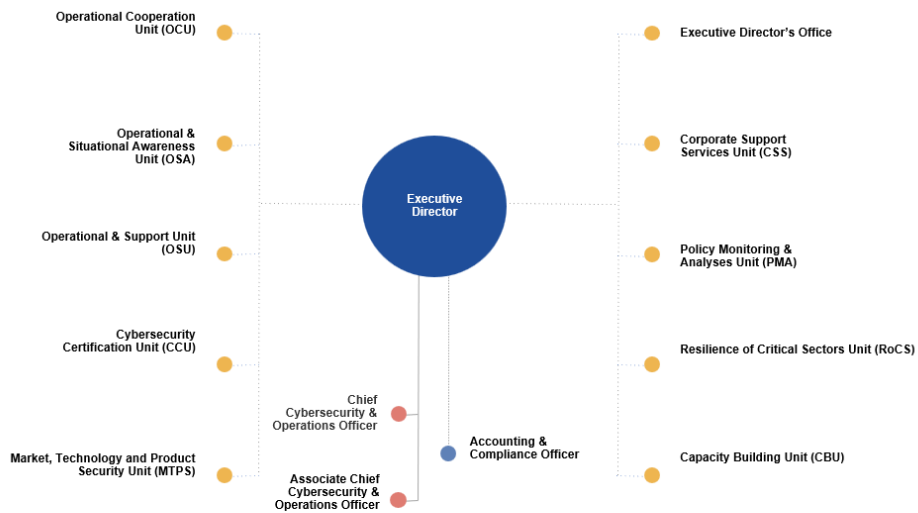


ANNEX

I. ORGANISATION CHART AS OF 01.01.2025



ENISA ORGANISATIONAL CHART



II. RESOURCE ALLOCATION PER ACTIVITY 2026 - 2028

The indicative allocation of the total 2026 financial and human resources following the activities as described in part 3.1 in Section III and the corporate activities as described in part 3.2 in Section III will be 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 8 operational activities as indicated under Section 3.1 of the SPD 2026-2028 (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 operational 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 2026.
- In order to estimate full costs of operational activities, both corporate activities (Activities 9 to 11) should be distributed accordingly to all operational activities based on respective drivers.

| ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2026) | Activities as referred to in Section 3 | Direct and Indirect budget allocation (in EUR) | FTE allocation |
|---|--|--|----------------|
| Support for policy monitoring and development | Activity 1 | 1.872.380 | 10 |
| Cybersecurity and resilience of critical sectors * | Activity 2 | 2.323.002 | 12 |
| Building capacity | Activity 3 | 2.468.042 | 12 |
| Enabling operational cooperation | Activity 4 | 4.296.578 | 15 |
| Provide effective operational cooperation through situational awareness * | Activity 5 | 3.360.610 | 13 |
| Provide services for operational assistance and support * | Activity 6 | 642.034 | 4 |
| Development and maintenance of EU cybersecurity certification framework | Activity 7 | 2.236.695 | 10 |
| Supporting European cybersecurity market, research & development and industry | Activity 8 | 2.183.285 | 10 |
| Performance and sustainability | Activity 9 | 2.530.892 | 15 |
| Reputation and trust | Activity 10 | 1.470.149 | 7,5 |
| Effective and efficient corporate services | Activity 11 | 3.807.135 | 21,5 |
| TOTAL | | 27.190.802 | 130 |

* Activities 2, 5 and 6 are 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 2026 - 2028

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

| Revenues | 2025 | 2026 |
|---|-------------------|-------------------|
| EU contribution | 25.993.311 | 26.495.438 |
| Other revenue (EFTA) | 721.020 | 695.364 |
| Other revenue from other contribution agreements (SLAs, Annex XI) | 24.523.333 | p.m. |
| TOTAL | 51.237.664 | 27.190.802 |

| REVENUES | 2025 amended budget | VAR 2026 / 2025 | Draft Estimated budget 2026 | Envisaged 2027 | Envisaged 2028 |
|---|---------------------|-----------------|-----------------------------|-------------------|-------------------|
| 1 REVENUE FROM FEES AND CHARGES | | | | | |
| 2 EU CONTRIBUTION | 25.993.311 | 1,93% | 26.495.438 | 26.720.032 | 27.236.032 |
| - of which assigned revenues deriving from previous years' surpluses | 150.299 | | 155.877 | 250.000 | 250.000 |
| 3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries) | 721.020 | -3,56% | 695.364 | 695.364 | 695.364 |
| - of which EEA/EFTA (excl. Switzerland) ** | 721.020 | -3,56% | 695.364 | 695.364 | 695.364 |
| - of which Candidate Countries | | | | | |
| 4 OTHER CONTRIBUTIONS *** | 24.463.333 | 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 **** | 60.000 | N/A | p.m. | p.m. | p.m. |
| 7 CORRECTION OF BUDGETARY IMBALANCES | | | | | |
| TOTAL REVENUES | 51.237.664 | -46,93% | 27.190.802 | 27.415.396 | 27.931.396 |

* - 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 2026-2028 average surplus of the previous 3 years (EUR 250 K) was used with 2,79% 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 installments 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 * ** | 2025 | | 2026 | |
|--------------------------|---------------------------|------------------------|---------------------------|------------------------|
| | Commitment appropriations | Payment appropriations | Commitment appropriations | Payment appropriations |
| Title 1 | 15.555.529 | 15.555.529 | 16.031.333 | 16.031.333 |
| Title 2 | 4.159.348 | 4.159.348 | 4.290.159 | 4.290.159 |
| Title 3 | 6.999.454 | 6.999.454 | 6.869.310 | 6.869.310 |
| Total expenditure | 26.714.331 | 26.714.331 | 27.190.802 | 27.190.802 |

| EXPENDITURE (in EUR) | Commitment and Payment appropriations * ** | | | | | |
|---|--|---------------------|-----------------------------|-----------------|-------------------|-------------------|
| | Amended Budget 2/2024 | Amended Budget 2025 | Draft estimated budget 2026 | VAR 2026 / 2025 | Envisaged in 2027 | Envisaged in 2028 |
| Title 1. Staff Expenditure | 14.809.106 | 15.555.529 | 16.031.333 | 3,1% | 16.163.751 | 16.467.977 |
| 11 Staff in active employment | 13.058.316 | 13.840.860 | 14.598.932 | 5,5% | 14.719.518 | 14.996.562 |
| 12 Recruitment expenditure | 517.889 | 508.469 | 217.593 | -57,2% | 219.391 | 223.520 |
| 13 Socio-medical services and training | 824.501 | 688.200 | 626.808 | -8,9% | 631.985 | 643.880 |
| 14 Temporary assistance | 408.400 | 518.000 | 588.000 | 13,5% | 592.857 | 604.015 |
| 15 External services on HR matters | N/A | N/A | | | 0 | 0 |
| Title 2. Building, equipment and miscellaneous expenditure | 3.671.144 | 4.159.348 | 4.290.159 | 3,1% | 4.325.596 | 4.407.010 |
| 20 Building and associated costs | 1.004.965 | 1.081.300 | 1.061.957 | -1,8% | 1.070.729 | 1.090.882 |
| 21 Movable property and associated costs (***) | 0 | 0 | | | 0 | 0 |
| 22 Current corporate expenditure | 516.125 | 687.000 | 336.858 | -51,0% | 339.640 | 346.033 |
| 23 Corporate ICT | 2.150.054 | 2.391.048 | 2.891.344 | 20,9% | 2.915.226 | 2.970.095 |
| Title 3. Operational expenditure | 7.739.551 | 6.999.454 | 6.869.310 | -1,9% | 6.926.050 | 7.056.409 |
| 30 Activities related to meetings and missions | 402.780 | 1.536.000 | 1.290.415 | -16,0% | 1.301.074 | 1.325.562 |
| 36/37 Core operational activities | 7.336.771 | 5.463.454 | 5.578.895 | 2,1% | 5.624.976 | 5.730.847 |
| TOTAL EXPENDITURE | 26.219.801 | 26.714.331 | 27.190.802 | 1,8% | 27.415.396 | 27.931.396 |
| <i>(*) Does not include EUR 174 604 for possible revenue under SLAs with ECCO and EU-LISA, ref. Annex XI</i> | | | | | | |
| <i>(**) Does not include amounts granted under the Contribution Agreements, see annex XI</i> | | | | | | |
| <i>(***) As from 2023, "Movable property and associated costs" have been included in Chapter 21 and 22 for streamlining purpose</i> | | | | | | |

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.

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

Table 3: Budget outturn and cancellation of appropriations (audited)

| Budget outturn | 2022 | 2023 | 2024 |
|--|----------------|----------------|----------------|
| Revenue actually received (+) | 39.227.392 | 25.293.935 | 42.473.035 |
| Payments made (-) | -20.396.780 | -21.118.392 | |
| Carry-over of appropriations (-) | -18.836.095 | -4.228.452 | (16.945.798) |
| Cancellation of appropriations carried over (+) | 248.745 | 149.739 | |
| Adjustment for carry-over of assigned revenue appropriations carried over (+) | 33.743 | 53.469 | 163.909 |
| Exchange rate difference (+/-) | -17,88 | 0 | |
| Total | 276.988 | 150.299 | 155.877 |

Preliminary Budget 2024 outturn amounts to EUR 155 877 (audited).

With steady budget increase over the last years up to EUR 26,2 million in 2024 a commitment rate of 100,00 % (100,00 % in 2023 and 99,93 % in 2022) of appropriations of the year (C1 funds) at year end has been reached which shows the already proven capacity of the Agency to fully implement its annual appropriations.

In 2024 commitment appropriations were cancelled for an amount of EUR 1 080 representing 0,004 % of the total budget.

The payment rate for the full budget of EUR 26,2 million reached 83,05 % (in 2023 - 83,86 %, in 2022 for ENISA 'standard' budget - 84,11 %). The total amount carried forward to 2025 is EUR 4 442 833 or 16,95 %.

No payment appropriations were cancelled during 2024.

The appropriations of 2023 carried over to 2024 were utilized at a rate of 96,19 % (automatic carry-overs) which indicates a proven capability of estimation of needs (in 2023 - 99,20 %). From the total amount of EUR 4 064 543 carried forward, the amount of EUR 154 797 was cancelled (or 3,81 %). This cancellation represents 0,61 % of the total committed appropriations 2023 of EUR 25 182 935 (fund source C1).

IV. HUMAN RESOURCES - QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2026 - 2028

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

Statutory staff and SNE



| STAFF | 2024 | | | 2025 | 2026 | 2027 | 2028 |
|---|--|--------------------------------------|-------------------------|---------------------------------|---------------------------------|---------------------------------|----------------------|
| | Authorised Budget | Actually filled as of 31/12/2024 | Occupancy rate % | Adopted | Envisaged staff | Envisaged staff | Envisaged staff |
| ESTABLISHMENT PLAN POSTS | | | | | | | |
| Administrators (AD) | 64 | 62 | 97% | 64 | 65 | 65 | 65 |
| Assistants (AST) | 19 | 19 | 100% | 19 | 18 | 18 | 18 |
| Assistants/Secretaries (AST/SC) | | | | | | | |
| TOTAL ESTABLISHMENT PLAN POSTS | 83 | 81 | 98% | 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) ⁵⁶ | 32 | 28 | 88% | 32 | 32 | 32 | 32 +p.m. |
| Contract Agents (stemming from contribution agreements) | | | | + 16* CA contribution agreement | + 18* CA contribution agreement | + 18* CA contribution agreement | +p.m. |
| Seconded National Experts (SNE) | 15 | 11 | 73% | 15 | 15 | 15 | 15 |
| | | | | | | | |
| TOTAL STAFF⁵⁷ | 130 | 120 | 92% | 146 | 148 | 148 | 130 |

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

| Human Resources | 2024 | 2025 | 2026 | 2027 | 2028 |
|---------------------------------|---------------|---------------|-------------------|---------------|---------------|
| | Envisaged FTE | Envisaged FTE | Envisaged FTE | Envisaged FTE | Envisaged FTE |
| Contract Agents (CA) | 12 | 16 | 18 ^{58*} | 18* | p.m. |
| Seconded National Experts (SNE) | n/a | n/a | n/a | n/a | n/a |
| TOTAL | 12 | 16* | 18* | 18* | p.m. |

⁵⁶ 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.

⁵⁷ Refers to TAs, CAs and SNEs figures

⁵⁸ Please see annex XI for additional information

Other Human Resources

• Structural service providers

| | Actually in place as of 31/12/2023 | Actually in place as of 31/12/2024 |
|-----------------------|------------------------------------|------------------------------------|
| Security | 7 | 7 |
| IT | 8 | 8 |
| Facilities management | 4 | 4 |

• Interim workers

| | Actually in place as of 31/12/2023 | Actually in place as of 31/12/2024 |
|--------|------------------------------------|------------------------------------|
| Number | 10 | 12 |

Table 2: Multi-annual staff policy plan Years 2024-2028

| Function group and grade | 2024 | | | | 2025 | | 2026 | | 2027 | | 2028 |
|--------------------------|-------------------|-------------|----------------------------------|------------|--------------------------|------------------|-------------|-------------|-------------------------|-------------|-------------|
| | Authorised budget | | Actually filled as of 31/12/2024 | | Authorised ⁵⁹ | | Envisaged | | Envisaged ⁶⁰ | | Envisaged |
| | Perm. Posts | Temp. posts | Perm. Posts | Temp posts | Perm. Posts | Temp. posts | Perm. posts | Temp. posts | Perm. 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 | | 2 | | 3 | | 3 | | 3 | 3 |
| AD 10 | | 4 | | 3 | | 4 | | 4 | | 4 | 4 |
| AD 9 | | 14 | | 15 | | 14 | | 14 | | 14 | 14 |
| AD8 | | 15 | | 11 | | 16 ⁶¹ | | 16 | | 16 | 16 |
| AD 7 | | 13 | | 12 | | 13 | | 14 | | 14 | 14 |
| AD 6 | | 7 | | 13 | | 7 | | 7 | | 7 | 7 |
| AD 5 | | 1 | | | | | | | | | |
| AD TOTAL | | 64 | | 62 | | 64 | | 65 | | 65 | 65 |
| AST 11 | | | | | | | | | | | |
| AST 10 | | | | | | | | | | | |
| AST 9 | | 2 | | 2 | | 1 | | 2 | | 2 | 2 |
| AST 8 | | 1 | | 1 | | 3 | | 2 | | 2 | 2 |
| AST 7 | | 0 | | 0 | | 3 | | 1 | | 1 | 1 |
| AST 6 | | 9 | | 7 | | 6 | | 7 | | 7 | 7 |
| AST 5 | | 4 | | 5 | | 4 | | 4 | | 4 | 4 |
| AST 4 | | 2 | | 2 | | 2 | | 2 | | 2 | 2 |
| AST 3 | | 1 | | 1 | | | | | | | |
| AST 2 | | | | 1 | | | | | | | |
| AST 1 | | | | | | | | | | | |
| AST TOTAL | | 19 | | 19 | | 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 | | 81 | | 83 | | 83 | | 83 | 83 |

⁵⁹ Modification of 2025 establishment plan pending Q1 2025

⁶⁰ Envisaged reflects future reclassification exercises

⁶¹ EU 2025 general budget is not yet published



| Function group and grade | 2024 | | | | 2025 | | 2026 | | 2027 | | 2028 |
|--------------------------|-------------------|-------------|----------------------------------|------------|--------------------------|-------------|-------------|-------------|-------------------------|-------------|-------------|
| | Authorised budget | | Actually filled as of 31/12/2024 | | Authorised ⁵⁹ | | Envisaged | | Envisaged ⁶⁰ | | Envisaged |
| | Perm. Posts | Temp. posts | Perm. Posts | Temp posts | Perm. Posts | Temp. posts | Perm. posts | Temp. posts | Perm. posts | Temp. posts | Temp. posts |
| GRAND TOTAL | 83 | | 81 | | 83 | | 83 | | 83 | | 83 |

External personnel

Contract Agents

| Contract agents | FTE corresponding to the authorised budget 2024 | Executed FTE as of 31/12/2024 | 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 |
|---------------------------|---|-------------------------------|---|--|--|--|
| Function Group IV | 30 | 21 +12 contribution agreement | 30 + 16 contribution agreement | 30 + 18 contribution agreement | 30 + 18 contribution agreement | 30 + pm |
| Function Group III | 2 | 6 | 2 | 2 | 2 | 2 |
| Function Group II | 0 | 0 | 0 | 0 | 0 | 0 |
| Function Group I | 0 | 1 | 0 | 0 | 0 | 0 |
| TOTAL | 32 | 40 | 48 | 50 | 50 | 32 |

Seconded National Experts

| Seconded National Experts | FTE corresponding to the authorised budget 2024 | Executed FTE as of 31/12/2024 | 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 |
|---------------------------|---|-------------------------------|---|--|--|--|
| TOTAL | 15 | 11 | 15 | 15 | 15 | 15 |

Table 3: Recruitment forecasts 2026 following retirement / mobility or new requested posts

| JOB TITLE IN THE AGENCY | TYPE OF CONTRACT (OFFICIAL, TA OR CA) | | TA/OFFICIAL | | CA Recruitment Function Group (I, II, III and IV) |
|-------------------------|---------------------------------------|--|--|---------------------|--|
| | Due to foreseen retirement/mobility | New post requested due to additional tasks ⁶² | Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication * | Internal (brackets) | |

⁶² Posts stemming from the required resources for 2026 work programme (12 FTEs)



| | | | | | |
|------------------|-----|---------------------------|-----|-----|-----|
| Expert | 1 | 5 TA s 6 CA s (FG4 IV) | n/a | n/a | n/a |
| Officer | n/a | 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**

| Grades | AVERAGE SENIORITY IN THE GRADE AMONG RECLASSIFIED STAFF | | | | | | | | Actual average over 5 years | Average over 5 years (According to decision C(2015)9563) |
|---|---|-----------|-----------|-----------|-----------|-----------|--|------|-----------------------------|---|
| | Year 2019 | Year 2020 | Year 2021 | Year 2022 | Year 2023 | Year 2024 | | | | |
| AD05 | - | - | - | - | - | - | | - | 2.8 | |
| AD06 | 3 | - | 1 | 1 | 1 | 2 | | 3,15 | 2.8 | |
| AD07 | - | 1 | - | 2 | 1 | 3 | | 3,5 | 2.8 | |
| AD08 | 1 | 2 | 1 | 3 | 1 | 2 | | 3,9 | 3 | |
| AD09 | - | - | - | - | 2 | | | 2,75 | 4 | |
| AD10 | - | - | - | 2 | - | | | 10,5 | 4 | |
| AD11 | - | - | - | - | - | | | - | 4 | |
| AD12 | - | - | 1 | - | - | | | 10 | 6.7 | |
| AD13 | - | - | - | - | - | | | - | 6.7 | |
| AST1 | - | - | - | - | - | | | - | 3 | |
| AST2 | - | - | - | - | - | | | - | 3 | |
| AST3 | 1 | - | - | 1 | - | | | 6,75 | 3 | |
| AST4 | 1 | 1 | - | - | 1 | 1 | | 2,76 | 3 | |
| AST5 | - | - | 1 | - | 1 | - | | 4,05 | 4 | |
| AST6 | - | 1 | 1 | - | - | - | | 3,5 | 4 | |
| AST7 | - | - | 1 | 1 | 1 | - | | 3,92 | 4 | |
| AST8 | - | - | - | - | - | 2 | | - | 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 | |

C. Gender representation

Table 1: Data on 31.12.2024 statutory staff (only temporary agents and contract agents)

| | | OFFICIAL | | TEMPORARY | | CONTRACT AGENTS | | GRAND TOTAL | |
|--------------------|--------------------------------|----------|---|-----------|--------------|-----------------|---------------|-------------|--------------|
| | | Staff | % | Staff | % | Staff | % | Staff | % |
| Female | Administrator level | - | - | 23 | 28,4% | 14 | 34,1% | 37 | 30,3% |
| | Assistant level (AST & AST/SC) | - | - | 13 | 16,0% | 5 | 12,2% | 18 | 14,8% |
| | Total | - | - | 36 | 44,4% | 19 | 46,3% | 55 | 45,1% |
| Male | Administrator level | - | - | 39 | 48,1% | 19 | 46,3% | 58 | 47,5% |
| | Assistant level (AST & AST/SC) | - | - | 6 | 7,4% | 3 | 7,3% | 9 | 7,4% |
| | Total | - | - | 45 | 55,6% | 22 | 53,7% | 67 | 54,9% |
| Grand Total | | - | - | 81 | 100% | 41 | 100,0% | 122 | 100% |

| TABLE 2: DATA REGARDING GENDER EVOLUTION OVER 5 YEARS OF THE MIDDLE AND SENIOR MANAGEMENT (31.12.2024) | 2020 | | 31.12.2024 | |
|--|--------|-----|-----------------|-----|
| | Number | % | Number | % |
| Female Managers | 2 | 25% | 2 ⁶³ | 29% |
| Male Managers | 6 | 75% | 5 ⁶⁴ | 71% |

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.

⁶³ This category comprises the ED and Heads of Unit level

⁶⁴ This category comprises the ED and Heads of Unit level

D. Geographical Balance

Table 1: Data on 31.12.2024 - 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 | 4,2% | 2 | 7,4% | 6 | 4,9% |
| BG | 2 | 2,1% | | 0,0% | 2 | 1,6% |
| CY | 2 | 2,1% | 2 | 7,4% | 4 | 3,3% |
| CZ | 1 | 1,1% | | 0,0% | 1 | 0,8% |
| DE | 1 | 1,1% | | 0,0% | 1 | 0,8% |
| Double *80 | 5 | 5,3% | 4 | 14,8% | 9 | 7,4% |
| EE | 2 | 2,1% | | 0,0% | 2 | 1,6% |
| EL | 38 | 40,0% | 13 | 48,1% | 51 | 41,8% |
| ES | 3 | 3,2% | | 0,0% | 3 | 2,5% |
| FR | 7 | 7,4% | 1 | 3,7% | 8 | 6,6% |
| HU | 1 | 1,1% | | 0,0% | 1 | 0,8% |
| IT | 8 | 8,4% | | 0,0% | 8 | 6,6% |
| LT | 2 | 2,1% | 1 | 3,7% | 3 | 2,5% |
| LV | 2 | 2,1% | | 0,0% | 2 | 1,6% |
| NL | 4 | 4,2% | | 0,0% | 4 | 3,3% |
| PL | 3 | 3,2% | 1 | 3,7% | 4 | 3,3% |
| PT | 3 | 3,2% | 1 | 3,7% | 4 | 3,3% |
| RO | 6 | 6,3% | 1 | 3,7% | 7 | 5,7% |
| SE | 1 | 1,1% | | 0,0% | 1 | 0,8% |
| SK | | 0,0% | 1 | 3,7% | 1 | 0,8% |
| TOTAL | 95 | 100% | 27 | 100% | 122 | 100% |

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

| MOST REPRESENTED NATIONALITY | 2020 | | 31.12.2024 | |
|------------------------------|----------------|------|-----------------|------|
| | Number | % | Number | % |
| Greek | 29 (out of 74) | 39,2 | 51 (out of 121) | 41,8 |

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

The Management Board of ENISA established – within the Agency's SPD for 2022-2024 – a goal for the Agency to achieve climate neutrality (defined as zero CO₂, CH₄ and N₂O emissions) across all its operations, by 2030.

As a first step, the agency undertook already an exercise in 2022 to map its current climate footprint by conducting audit of past ENISA emissions for which 2019 and 2021 were used as reference years. ENISA further strengthened its environmental management and carried out an overarching audit in course of 2023, on the CO₂ impact of all the operations of the agency in 2023.

In order to ensure that ENISA is on the correct path towards climate neutrality by 2030 and to promote and enhance ecological sustainability across all the agency's operations, the following key actions have been undertaken in course of 2024, towards also acquiring an EMAS certificate towards the end of 2024.

ENISA with the assistance of an external contractor completed a technical study for the assessment of the carbon footprint calculation for 2022 and works towards assessing its 2023 carbon footprint calculation in Q4 2024.

- Several actions for the reduction of GHGs emissions were further implemented that included recycling of office waste in a structured manner (via dedicated recycling bins and guidelines on the proper use of the bins), advancement of the watering system, incorporation of GHG emissions provisions to the agency's public procurement procedures and tenders, awareness raising sessions and dedicated trainings to all staff about EMAS and the greening initiatives of the agency.
- In course of 2024 the registration and implementation of an environmental management system (according to the EMAS regulation) also took place with the creation of EMS (European Management System) templates and procedures.
- An internal audit and environmental performance evaluation took also place in course of 2024.
- The agency also proceeded to the drafting of its environmental statement for which the formal approval by ENISA's management Team is also anticipated in Q4 of 2024.
- An external verification to be concluded in course of Q4 2024.
- Externally communicate via ENISA's website about EMAS and the greening initiatives of the agency (Q4 2024 and Q1 2025).

VII. BUILDING POLICY

Current buildings: Heraklion office is expected to be vacated by the 30th June 2026

| Building Name and type | Location | Location SURFACE AREA(in m ²) | | | RENTAL CONTRACT | | | Host country (grant or support) | Building present value(€) |
|------------------------|----------------|---|-----------------|------------|----------------------|---------------------------|--------------|---|---------------------------|
| | | Office space (m2) | non-office (m2) | Total (m2) | Rent (euro per year) | Duration | Type | | |
| Heraklion Office | Heraklion | 706 | | 706 | | 01/01/2021 to 28/02/2030; | Lease | Rent is fully covered by Hellenic Authorities | N/A |
| 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 |
| Total | Location | 5302 | 2617 | 7920 | | | | | |

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) | 2026 | 2027 | 2028 |
|--------------------------------------|---------|---------|---------|
| Head count (FTEs) | 13-14 | 13-14 | 13-14 |
| Budget (one-off & 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 |
| <p>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.</p> <p>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.</p> | <p>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.</p> <p>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.</p> | <p>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.</p> <p>There is no European School operating in Athens.</p> |

IX. EVALUATIONS

In 2025 ENISA concluded its second biennial stakeholder satisfaction survey for the period 2023 and 2024 of its work programmes. The results of the second stakeholder satisfaction survey shed 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. 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 overall 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 used since 2023 for the assessment of internal controls, together with a comprehensive methodology for enterprise risk assessment across the Agency.

Moreover, since 2021 ENISA has been implementing its Anti-Fraud strategy. The revised Anti-Fraud Strategy (AFS) for the period of 2025-2027 has been adopted by means of the Management Board Decision 2025/03.

The new Anti-Fraud Strategy is based on the ENISA AFS 2021-2024 and further consolidates and further develops the objectives set out previously. ENISA has implemented several tools to improve the prevention and detection of fraud. In particular, ENISA carries out an annual risk assessment exercise, taking into account the fraud risks at the Agency. The new ENISA AFS derives from this knowledge and aims at consolidating and further refining the anti-fraud activities at the Agency in a way which is proportionate to the fraud risks, having due regard to the costs and benefits of the measures to be implemented.

It is noted that the conflict of interest is a risk that has been identified across different categories, i.e. regarding not only contractors of the Agency, but also candidates during recruitment procedures, Selection Board members or members of ENISA statutory bodies or external experts.

The Agency applies the mandatory signing of declarations of conflict of interest and confidentiality declarations by all experts applying to a Call of Expression of Interest (CEI) list and by parties contracted through a procurement procedure. Annual declarations of interest shall also be submitted by members of the Management Board and their alternates, members of the National Liaison officers network, members of the Advisory group and members of the Ad hoc Working Groups. 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.

Declaration of interest shall also be signed by the candidates for taking part in the recruitment procedures is available. It aims 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 | Duration | Counterpart | Short description |
|--------------------------------|--|-------------------|---|---------------------------------------|-------------|--|
| 1 | SLA with ECCC (Activity 9) | 20/12/22 | 54.604 | 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 | 120.000 | 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 HAS assessment / EUCC pilots (Addendum I - LC-03708221) | 19/12/2024 | Up to. EUR 15,25 mil (prefinancing rate 80%) (+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 2) Additional actions following the amendment: 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 (pre-financing 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 forecast of commitment appropriations | 2027 forecast of commitment appropriations | 2028 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 | 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 | Act.4, Act 5, Act.6, Act.7, Act.8, Act.9 Act.11 |
| support of the implementation of the Cyber Resilience Act, notably actions related to development and assessment of technical | until 31/12/2027 | 3/7/25 | 250.000 | 250.000 | 0 | 0 | 125.000 | 125.000 | 0 | Part of the above CA, ref. Act.7 & Act.8 |



| | | | | | | | | | | |
|--|------------------|---------|-------------------|-------------------|-------------------|----------------------|-------------------|----------------------|----------|---------------------------|
| specifications and standards and interplay with European Cybersecurity Certification schemes ⁶⁵ | | | | | | | | | | |
| CRA single reporting platform (feasibility study) | until 31/07/2026 | 9/12/24 | 400.000 | 160.000 | 0 | 240.000 | 160.000 | 0 | 0 | Act.5 |
| 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 | Act.4, Act.6 Act.9 Act.11 |
| Total Budget | | | 72.320.000 | 31.856.667 | 16.000.000 | 24.463.333,33 | 18.008.333 | 13.848.333,34 | 0 | |

| Contribution agreement | 2026 forecast of Contract agents | 2027 forecast of Contract Agents | 2028 forecast Contract Agents | Related Activities |
|---|----------------------------------|----------------------------------|-------------------------------|--------------------|
| Preparedness and Incident Response Support for Key Sectors (Support Action & Situational Analysis Center) | 12 | 0 | 0 | Act.6, Act.5 |

⁶⁵ (Amendment n.1 to the 2024 Contribution Agreement on the Implementation of the “Incident and Vulnerability Response Support and Reporting” Action)



| | | | | |
|---|-----------|-----------|-----------|--|
| Incident and Vulnerability Response Support and Reporting (Support Action, CRASPR and SitCEN) | 6 | 8 | | 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 | 0 | 0 | 0 | Part of the above CA, ref. Act.7 & Act.8 |
| CRA single reporting platform | 0 | 0 | 0 | Act.5 |
| EU Cybersecurity Reserve & Cyber Situation and Analysis Centre | 0 | 10 | 13 | Act.6, Act.5, Act.2 |
| Total | 18 | 18 | 13 | |



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

The international strategy confirms the Agency's mandate in terms of its and focus on the EU and EU actors, while also allowing increased flexibility to engage 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. The Agency's international strategy⁶⁶ was adopted by the MB in 2021. A new international strategy is expected to be presented to the MB for endorsement 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.

XIII. ANNUAL COOPERATION PLAN 2026

The 2026 Annual Cooperation Plan between ENISA, the EU Agency for Cybersecurity, and CERT-EU, EU Cybersecurity Service for the Union institutions, bodies, offices and agencies, bodies and agencies will be annexed to the Single Programming Document 2026-2028 as a separate document.

XIV. PROCUREMENT PLAN 2026

The indicative procedures from ENISA budget (Title 1,2 and 3) for public contracts to be launched in 2026 are detailed as follows:

| ENISA UNIT | TITLE of Contract | TYPE of procedure | Tender launch | Contract signature | Total budget est. 4 years |
|------------|--|-------------------|---------------|--------------------|---------------------------|
| PMA | Supporting ENISA in monitoring and analysis of strategies and policies | Open – 4y FWC | Q1 | Q1 | 800.000 |
| RoCS | Supporting analysis of cybersecurity | Open – 4y FWC | Q4 | 2027 | 1.200.000 |

| | | | | | |
|------------|---|---------------|----|----|-----------|
| | investments and business resilience | | | | |
| CBU | External Cloud based Training Platform Access and Support Services | Open – 4y FWC | Q3 | Q3 | 4.000.000 |
| CBU | Support on the ECSF, attestation schemes, report skills gap | RoC | Q2 | Q2 | 200.000 |
| OCU | Security assessment, monitoring and ICT services | Open – 4y FWC | Q3 | Q4 | 3.000.000 |
| OCU | IT infrastructure management and consultancy services | Open – 4y FWC | Q2 | Q2 | 1.700.000 |
| OCU | Consultancy services to improve incident response and crises management in the EU | Open – 4y FWC | Q1 | Q2 | 1.600.000 |
| CCU | EUCC maintenance | RoC | Q1 | Q1 | 45.000 |
| CCU | Supporting EU5G scheme development | RoC | Q1 | Q1 | 30.000 |
| CCU | Support to ECCC subgroup on crypto | RoC | Q1 | Q1 | 30.000 |
| CCU | Development and maintenance services for the EU cybersecurity index tool | Open – 4y FWC | Q2 | Q3 | 1.000.000 |
| EDO | Tax Consultation Services | Open – 4y FWC | Q2 | Q2 | 200.000 |
| EDO | Events Organisation and Meeting | Open – 4y FWC | Q3 | Q4 | 7.000.000 |



| | | | | | |
|-----|---|---------------------|----|----|-----------|
| | Management service | | | | |
| EDO | Risk assessment, control and governance framework" | RoC | Q1 | Q1 | 25.000 |
| EDO | Penetration tests" for 6 to 8 apps per year (centralised) | RoC | Q1 | Q1 | 70.000 |
| EDO | Maturity assessment, BIA, BCP execution and cybersecurity plans | RoC | Q1 | Q1 | 30.000 |
| CSS | Facilities Management Services | Restricted – 4y FWC | Q3 | Q4 | 1.600.000 |
| CSS | Provision of Medical services | Open – 4y FWC | Q3 | Q4 | 260.000 |

The total indicative budget reserved for procurement is approximately 22.8 million euros.

XV. ENISA STATUTORY OPERATIONAL TASKS FROM EU LEGISLATION 2024

The following list of EU legislations mapped by activity as of September 2024

| <i>EU legislation</i> | <i>Article</i> | <i>Legal provisions</i> | <i>Responsible unit/activity under Art 3(3) MB/2024/10</i> |
|-----------------------|----------------|---|--|
| 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. | ACTIVITY 8 |
| 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 ... | ACTIVITY 3 |



| | | | |
|-----|------------|--|------------|
| 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. | ACTIVITY 4 |
| 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 /.../ | ACTIVITY 5 |
| 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 /.../ | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. /.../ | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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 | ACTIVITY 5 |

| | | | |
|-----|------------|---|------------|
| | | 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. | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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 [...] | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 8 |

| | | | |
|-----|------------|--|------------|
| 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. /.../ | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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. /.../ | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |

| | | | |
|-----|-------------|---|------------|
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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 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 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 shall carry 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 | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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 | ACTIVITY 1 |
| 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 | ACTIVITY 1 |
| 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 | ACTIVITY 1 |
| 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 | ACTIVITY 1 |
| 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; | ACTIVITY 2 |

| | | | |
|-----|------------|---|------------|
| 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; | ACTIVITY 2 |
| 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; | ACTIVITY 2 |
| 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 | ACTIVITY 2 |
| 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 | ACTIVITY 2 |
| 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 | ACTIVITY 2 |
| 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; | ACTIVITY 2 |
| 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 | ACTIVITY 3 |
| CSA | Art 6(1)i | [assist] relevant public bodies by offering trainings regarding cybersecurity, where appropriate in cooperation with stakeholders | ACTIVITY 3 |
| 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 | ACTIVITY 3 |
| 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 | ACTIVITY 3 |
| 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 | ACTIVITY 3 |
| 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 | ACTIVITY 3 |
| CSA | Art 10(d) | [ENISA shall] support closer coordination and exchange of best practices among Member States on cybersecurity awareness and education. | ACTIVITY 3 |
| 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; | ACTIVITY 3 |
| CSA | Art 10(c) | [ENISA shall] assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education; | ACTIVITY 3 |

| | | | |
|-----|------------|--|------------|
| 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 | ACTIVITY 4 |
| 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 | ACTIVITY 4 |
| 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 | ACTIVITY 4 |
| 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 | ACTIVITY 4 |
| 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 | ACTIVITY 4 |
| CSA | Art 7(1) | ENISA shall support operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders | ACTIVITY 4 |
| 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.. | ACTIVITY 4 |
| CSA | Art 7(4)b* | [ENISA shall support Member States with respect to operational cooperation within the CSIRT’s 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 | ACTIVITY 4 |
| CSA | Art 7(3) | ENISA shall provide the secretariat of the CSIRT’s 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. | ACTIVITY 4 |
| 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] | ACTIVITY 4 |
| CSA | Art 7(4)a* | [ENISA shall support Member States with respect to operational cooperation within the CSIRT’s network by) advising on how to improve their capabilities to prevent, detect and respond to incidents [...]; | ACTIVITY 4 |
| 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 CSIRT’s network and the technical and political decision-makers at Union level | ACTIVITY 4 |
| 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; | ACTIVITY 4 |
| 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 | ACTIVITY 4 |

| | | | |
|-----|------------|---|------------|
| | | 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 | ACTIVITY 4 |
| 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 | ACTIVITY 4 |
| 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 | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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 [...] | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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 | ACTIVITY 5 |

| | | | |
|-----|------------|---|------------|
| 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 | ACTIVITY 5 |
| 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 | ACTIVITY 6 |
| 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 | ACTIVITY 6 |
| 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; | ACTIVITY 7 |
| 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; | ACTIVITY 7 |
| 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); | ACTIVITY 7 |
| 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); | ACTIVITY 7 |
| 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). | ACTIVITY 7 |
| CSA | Art 8(2) | ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group pursuant to Article 22(4). | ACTIVITY 7 |
| 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 | ACTIVITY 7 |
| 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 | ACTIVITY 7 |
| 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 | ACTIVITY 7 |
| CSA | Art 49 | {Preparation, adoption and review of a European cybersecurity certification scheme} | ACTIVITY 7 |
| 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. | ACTIVITY 7 |

| | | | |
|-----|------------|---|------------|
| 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. | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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). | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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; | ACTIVITY 7 |
| 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. | ACTIVITY 7 |
| 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) | ACTIVITY 7 |
| 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; | ACTIVITY 8 |
| 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; | ACTIVITY 8 |

| | | | |
|------|------------|--|------------|
| 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. | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| CSA | Art 11(c) | [ENISA shall] contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity | ACTIVITY 8 |
| 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; | EDO |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 4 |



| | | | |
|------|-----------|---|------------|
| 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 | ACTIVITY 4 |
| 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. | ACTIVITY 4 |
| 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 | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |

| | | | |
|------|-----------|--|------------|
| 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 | ACTIVITY 6 |
| 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 | ACTIVITY 6 |
| 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 | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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 | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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. | ACTIVITY 6 |

| | | | |
|------|------------|--|------------|
| 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); | ACTIVITY 6 |
| 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); [| ACTIVITY 6 |
| 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). | ACTIVITY 6 |
| 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 | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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. | ACTIVITY 6 |

| | | | |
|------|------------|---|------------|
| | | 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. | ACTIVITY 6 |
| 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.' | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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. | ACTIVITY 6 |
| 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. [...] | ACTIVITY 8 |
| 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/.../ | ACTIVITY 2 |
| 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 /.../ | ACTIVITY 2 |
| 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 | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |

| | | | |
|------|-------------|--|------------|
| | | 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 | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 8 |
| 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; | ACTIVITY 8 |
| 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; | ACTIVITY 8 |

| | | | |
|--------|---------------------|---|------------|
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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 | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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; | ACTIVITY 8 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |

| | | | |
|------|--------------|---|------------|
| 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). | ACTIVITY 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| NCSS | Art 13 (1) | {Benchmarking} By 13 June 2025, ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. [...] | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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'). | ACTIVITY 2 |
| 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. | ACTIVITY 2 |

| | | | |
|------|-------------|---|------------|
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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 | ACTIVITY 2 |
| 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 2025 issue 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. | ACTIVITY 2 |
| 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. | ACTIVITY 3 |
| 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. | ACTIVITY 3 |
| 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. | ACTIVITY 3 |
| 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. | ACTIVITY 3 |
| 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. | ACTIVITY 4 |

| | | | |
|------|----------------|---|------------|
| 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. | ACTIVITY 4 |
| 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. | ACTIVITY 5 |
| NCSS | Art 37(2)(a) | {Rules on information sharing} If a CSIRT becomes aware of an unpatched actively exploited vulnerability, it shall: (a) share it with ENISA via an appropriate secure information exchange channel without delay, unless otherwise specified in other Union law; | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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; | ACTIVITY 5 |
| 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 | ACTIVITY 1 |
| 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 [...] | ACTIVITY 1 |
| 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 | ACTIVITY 1 |
| 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 | ACTIVITY 1 |
| 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 [...] | ACTIVITY 1 |
| 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). | ACTIVITY 1 |
| 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. | ACTIVITY 1 |
| NIS2 | Art 19(2) | {Peer reviews} /.../ The Commission and ENISA shall participate as observers in the peer reviews. | ACTIVITY 1 |

| | | | |
|------|-------------|--|------------|
| 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. | ACTIVITY 1 |
| 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. | ACTIVITY 1 |
| 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); | ACTIVITY 1 |
| 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. | ACTIVITY 1 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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 [...] | ACTIVITY 2 |
| 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) | ACTIVITY 2 |
| 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 | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |
| 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. | ACTIVITY 2 |

| | | | |
|------|-------------|--|------------|
| 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 | ACTIVITY 3 |
| 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 | ACTIVITY 3 |
| NIS2 | Art 10(10) | {Computer security incident response teams (CSIRTs)} Member States may request the assistance of ENISA in developing their CSIRTs. | ACTIVITY 4 |
| 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: ... | ACTIVITY 4 |
| NIS2 | Art 15(2) | {CSIRTs network} ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs | ACTIVITY 4 |
| 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 | ACTIVITY 4 |
| NIS2 | Art 14(3) | {Cooperation Group} The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. | ACTIVITY 4 |
| 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; | ACTIVITY 5 |
| 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 | ACTIVITY 5 |
| 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 /.../ | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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. | ACTIVITY 6 |
| 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. | ACTIVITY 7 |
| 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 | ACTIVITY 8 |

| | | | |
|------|-------------|---|------------|
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 8 |
| 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. | ACTIVITY 1 |
| 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. | ACTIVITY 3 |
| 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 | ACTIVITY 4 |
| 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 /.../ | ACTIVITY 4 |
| 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. | ACTIVITY 4 |
| 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; | ACTIVITY 5 |
| REU | Art 21(8)* | {Reporting obligations} CERT-EU shall submit to the IICB, ENISA, the EU INCEN and the CSIRT's 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 [...] | ACTIVITY 5 |
| 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. | ACTIVITY 5 |
| 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 | EDO |
| 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; | EDO |

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 - Regulation on horizontal cybersecurity requirements for products with digital elements - REGULATION (EU) 2024/XXXX (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html) NB! NOT OFFICIAL JOURNAL VERSION!

CSOA: Cybersolidarity Act - Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - REGULATION (EU) 2024/XXXX (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0355_EN.pdf) NB! NOT OFFICIAL JOURNAL VERSION! Numeration of articles not yet final!

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)

ECRC: 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 artificial 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

* - denotes responsible for only part of a legal provision

** - denotes shared responsibility of a same legal provision

XVI. CORPORATE STRATEGY GOALS AND INDICATORS

The table below highlights the responsible activity for each corporate objective from the Corporate Strategy including the key goals and means to measure the associated Key Performance Indicators (KPIs). This will be

reviewed on the basis of first year results of the Corporate Strategy (including results from the 2023 Staff Satisfaction Survey) to be reported under 2023 annual activity report. In addition to these principles for resourcing the objectives have been taken into consideration when developing the budget.

| STRATEGIC DIMENSION | OBJECTIVES | ACTIVITY'S TO ACHIEVE OBJECTIVES | KEY GOALS (KPIS/MEANS TO MEASURE THE KPIS) |
|---|---|----------------------------------|--|
| <p><u>People centric organisation</u></p> | <p>Effective workforce planning and management</p> | <p>Activity 11</p> | <ul style="list-style-type: none"> Agency's internal workforce needs for the year n until n+2 are defined and presented to the MB together with the first draft SPD for those years as per annual/internal procedures. Effective FTEs used for SPD activities (as reported in AAR by end of year n) do not diverge from planned FTEs in SPD (as endorsed by MB in the beginning of year n) by more than 5% according to annual/internal procedures. 95% of Agency's staffing posts (TA, CA, SNE) are fulfilled by the end of year according to its annual recruitment results. Vacated staff posts are fulfilled in less than 300 days according to its annual recruitment results. All assignments of staff are reviewed regularly every three years during the Agency's annual/internal procedures. Aggregate loss of FTE across the Agency due to absences (excluding long-term sick leave) is less than three FTEs annually during its annual/internal process. |
| | <p>Efficient talent acquisition, development and retainment</p> | <p>Activity 11</p> | <ul style="list-style-type: none"> Agency has established clear competency targets in line with its established needs and has reviewed them in an annual appraisal exercise. All selection criteria used for the published as well as internal vacancies are solely based on established competencies described in the annual/recruitment process. Agency's proficiency levels across target competencies have increased over the set period according to annual appraisal exercises. 50% of Agency's established workforce needs are addressed through internal talent development (including internal mobility, competitions and appointment) according to its annual internal process. Jobholder satisfaction with the guidance and support received from their Reporting Officers in achieving learning and development goals is high according to the biennial staff satisfaction survey. High level of staff satisfaction for learning opportunities offered and knowledge sharing options according to the biennial staff satisfaction survey. High level of positive peer-review assessments in CDR reports in annual internal process. |
| | <p>Caring and inclusive modern organisation</p> | <p>Activity 11</p> | <ul style="list-style-type: none"> High aggregate staff satisfaction with psychological safety level according to annual staff satisfaction survey. High aggregate staff satisfaction with workspace and related services according to biennial staff satisfaction survey. Agency obtains EU Agency's Network Certificate of Excellence in Diversity and Inclusion by the end of 2025 according to external audit and certification process. High level of satisfaction with Agency's workplace integration, wellness and health programmes, engagement and community mindset for staff according to annual staff satisfaction survey. Staff stress level is decreasing from 2022 levels and is sustained at low levels after 2025 according to annual staff satisfaction survey |
| <p><u>Service centric organisation</u></p> | <p>Ensure efficient corporate services</p> | <p>Activity 9 & 11</p> | <ul style="list-style-type: none"> High satisfaction with essential corporate support services found through an annual MT survey. High satisfaction with demand driven or optional corporate support services found through an annual MT survey. Number of procurement procedures merged, combined or used in interinstitutional FWCs found through an annual internal procedure. |



| | | | |
|---------------------------------|---|-----------------|--|
| | | | <ul style="list-style-type: none"> The percentage of staff (measured in FTEs) engaged in shared corporate service activities within the Agency found through an annual internal procedure. The percentage of staff (measured in FTEs) engaged in shared corporate service activities beyond the Agency with other Union Entities (under SLAs, MoUs or other arrangements) found through an annual internal procedure |
| | Introduce digital solutions that maximise synergies and collaboration within the Agency | Activity 9 & 11 | <ul style="list-style-type: none"> Implement (replace or develop) at least five user-centered, cloud-based, corporate solutions or tools fit for purpose and in line with ENISA's IT strategy and relevant business needs by Q4 2025. Limited disruption of continuity of services across all corporate support service areas measured by annual assessment. To have IT support service standards as technical KPIs in place by Q2 2025 and to have them continuously monitored and observed, to support the maintenance and development of operational IT systems through an annual review. All on-premises systems are maintained within risk levels established by the business owners and all corrective measures recommended by periodic risk assessments are implemented as found in an annual review. |
| | Continuous innovation and service excellence | Activity 9 | <ul style="list-style-type: none"> The percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have not been reviewed less than three years ago as found by an annual review. <p>Percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have been last reviewed more than four years ago as found in an annual review.</p> |
| | Developing service propositions with additional external resourcing | Activity 9 & 11 | <ul style="list-style-type: none"> At least three SLAs signed and in operation with Union Entities covering ENISA's operational services with additional resourcing from beneficiaries by 2025. |
| Sustainable organisation | Ensure ENISA is climate neutral by 2030 | Activity 9 | <ul style="list-style-type: none"> Acquire an EMAS certificate by Q1 2024. 50% of participants in ENISA's organised events and meetings to participate online by 2025, rising to 75% by 2030. 50% of ENISA events and meetings to be organised as hybrid or online by 2025, rising to 75% by 2030. Initiate and by end 2024 agree a tripartite MoU with the Hellenic Authorities and the landlord of ENISA HQ building to reduce the climate impact of the HQ building at least 40% by 2029, by installing solar panels on the non-classified part of the building or procure a green building for the Agency by then. Offset all residual emissions generated through ENISA operations from 2024 onwards |
| | Promote and enhance ecologic sustainability across all the Agency's operations | Activity 9 & 11 | <ul style="list-style-type: none"> Recycle all ENISA residual waste created in its HQ and local offices by 2025. Implement ecological sustainability and climate neutrality criteria for procuring event management and support and for facilities management and support services from external contractors by 2025. Implement ecological sustainability and climate neutrality criteria for all ENISA tenders for corporate service contractors by 2027 and by 2029 for operational activities. Understand best practices in sustainable IT solutions, define an agency-wide approach and include it in the IT Strategy. |

| | | | |
|--|--|----------------------------|---|
| | <p>Develop efficient framework for continuous governance to safeguard high level of IT and physical security</p> | <p>Activity 9 & 11</p> | <ul style="list-style-type: none"> • Review the Agency's IT strategy and align it with the objectives of the corporate strategy by Q3 2024. • Set in place a relevant policy for security compliance for IT and for physical security (including for required EUCI levels) for all relevant internal and external services with a high level of adherence to this KPI from 2025 onwards. • The Agency in a position to handle EUCI at the level of SECRET UE/EU SECRET and be accredited as being able to do so by Q4 2024. • 20% of the total IT budget to be allocated to information security proportional to the level of risks across various IT systems within the Agency by Q4 2024. Implement relevant security requirements and criteria for all relevant ENISA tenders for corporate services by Q1 2025. |
|--|--|----------------------------|---|



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 2026 (Budget 2026)

European Union Agency for Cybersecurity

CONTENTS

1. General introduction
2. Justification of main headings
3. Statement of Revenue 2026
4. Statement of Expenditure 2026

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 2026

The 2026 total revenue amounts to € 27190802 and consists of a subsidy of € 26495438 from the General Budget of the European Union and EFTA countries' contributions € 695364

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 Februarv 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.

ENISA has signed a few SLAs with other EU Agencies for provision of services where revenue is expected to reach € 174.604,00

2.2 Expenditure in 2026

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 2026, which contains 83 Temporary Agent posts.

Total expenditure under Title 1 amounts to € 16.031.333

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to € 4.290.159

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of

Work Programme 2026 and amounts to € 6.869.310

Title 4 - Externally funded activities

Expenditure under Title 4 amounts to p.m.

3. STATEMENT OF REVENUE 2026

| Title | Heading | Voted Appropriations 2024 € | Amended Budget 2024 € | Voted Appropriations 2025 € | Amended Budget 2025 € | Draft Appropriations 2026 € | Remarks - budget 2026 |
|-------|------------------------------|--------------------------------|--------------------------|--------------------------------|--------------------------|--------------------------------|---|
| 1 | EUROPEAN COMMUNITIES SUBSIDY | 24.953.071 | 25.336.397 | 25.716.933 | 25.993.311 | 26.495.438 | Total subsidy of the European Communities |
| 2 | THIRD COUNTRIES CONTRIBUTION | 883.404 | 883.404 | 713.309 | 721.020 | 695.364 | Contributions from Third Countries. |
| 3 | OTHER CONTRIBUTIONS | 0 | 16.000.000 | p.m. | 24.463.333 | p.m. | *Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA under the Digital Europe Programme (DEP), EUR 16.000.000,00 *Contribution Agreement of 09/12/2024 for CRA single reporting platform, EUR 240.000,00. *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 12.000.000,00 *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 |
| 4 | ADMINISTRATIVE OPERATIONS | 0 | p.m. | p.m. | 60.000 | p.m. | *First instalment received under the Service Level Agreement signed with eu-LISA for an amount of EUR 60 000 (out of a maximum of EUR 120 000). |
| | GRAND TOTAL | 25.836.475 | 42.219.801 | 26.430.242 | 51.237.664 | 27.190.802 | |

| Article Item | Heading | Voted Appropriations 2024 € | Amended Appropriations 2024 € | Voted Appropriations 2025 € | Amended Appropriations 2025 € | Draft Appropriations 2026 € | Remarks - budget 2026 |
|-----------------|---|--------------------------------|----------------------------------|--------------------------------|----------------------------------|--------------------------------|---|
| 1 | EUROPEAN COMMUNITIES SUBSIDY | | | | | | |
| 10 | EUROPEAN COMMUNITIES SUBSIDY | | | | | | |
| 100 | <i>European Communities subsidy</i> | 24.953.071 | 25.336.397 | 25.716.933 | 25.993.311 | 26.495.438 | Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security. As per Letter of intent between DG CONNECT and ENISA on the provision of support to Member States to further mitigate the risks of large scale cybersecurity incidents in the short term, dated 20 July 2022, ref. Ares(2022)5473716 - 29/07/2022 |
| 100 | <i>European Communities subsidy - Expansion of Activities 3, 4, 5</i> | n/a | n/a | n/a | n/a | n/a | |
| | CHAPTER 10 | 24.953.071 | 25.336.397 | 25.716.933 | 25.993.311 | 26.495.438 | |
| | TITLE 1 | 24.953.071 | 25.336.397 | 25.716.933 | 25.993.311 | 26.495.438 | |
| 2 | THIRD COUNTRIES CONTRIBUTION | | | | | | |
| 20 | THIRD COUNTRIES CONTRIBUTION | | | | | | |
| 200 | <i>Third Countries contribution</i> | 883.404 | 883.404 | 713.309 | 721.020 | 695.364 | Contributions from Associated Countries. |
| | CHAPTER 2 0 | 883.404 | 883.404 | 713.309 | 721.020 | 695.364 | |
| | TITLE 2 | 883.404 | 883.404 | 713.309 | 721.020 | 695.364 | |
| 3 | OTHER CONTRIBUTIONS | | | | | | |
| 30 | OTHER CONTRIBUTIONS | | | | | | |
| 300 | <i>External funding under Contribution Agreement</i> | n/a | 16.000.000 | p.m. | 24.463.333 | p.m. | *Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA under the Digital Europe Programme (DEP), EUR 16.000.000,00 *Contribution Agreement of 09/12/2024 for CRA single reporting platform, EUR 240.000,00. *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 12.000.000,00 *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 |
| | CHAPTER 30 | n/a | 16.000.000 | p.m. | 24.463.333 | p.m. | |
| | TITLE 3 | n/a | 16.000.000 | p.m. | 24.463.333 | p.m. | |
| 4 | ADMINISTRATIVE OPERATIONS | | | | | | |
| 40 | ADMINISTRATIVE OPERATIONS | | | | | | |
| 400 | <i>Administrative Operations</i> | p.m. | p.m. | p.m. | 60.000 | p.m. | Revenue from administrative operations including SLAs with other EU Agencies. Estimated amount for the year shall be € 174604 |
| | CHAPTER 40 | p.m. | p.m. | p.m. | 60.000 | 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. | p.m. | p.m. | 60.000 | p.m. | First instalment received under the Service Level Agreement signed with eu-LISA for an amount of EUR 60 000 (out of a maximum of EUR 120 000). |
| | GRAND TOTAL | 25.836.475 | 42.219.801 | 26.430.242 | 51.237.664 | 27.190.802 | |

4. STATEMENT OF EXPENDITURE 2026

| Title | Heading | Voted Appropriations 2024 € | Amended Appropriations 2024 € | Voted Appropriations 2025 € | Amended Appropriations 2025 € | Draft Appropriations 2026 € | Remarks - budget 2026 |
|-------|--|--------------------------------|----------------------------------|--------------------------------|----------------------------------|--------------------------------|--|
| 1 | STAFF | 14.739.106 | 14.809.106 | 15.271.440 | 15.555.529 | 16.031.333 | Total funding for covering personnel costs. |
| 2 | BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE | 3.666.898 | 3.671.144 | 4.159.348 | 4.159.348 | 4.290.159 | Total funding for covering general administrative costs. |
| 3 | OPERATIONAL EXPENDITURE | 7.430.471 | 7.739.551 | 6.999.454 | 6.999.454 | 6.869.310 | Total funding for operational expenditures. |

| 4 | EXTERNALLY FUNDED ACTIVITIES | | n/a | 16.000.000 | p.m. | 24.523.333 | p.m. | Total external funding such as contribution agreements and SLAs. |
|------|--|--------------------|-------------------|-------------------|-------------------|-------------------|-------------------|--|
| | | GRAND TOTAL | 25.836.475 | 42.219.801 | 26.430.242 | 51.237.664 | 27.190.802 | |
| 1 | STAFF | | | | | | | |
| 11 | STAFF IN ACTIVE EMPLOYMENT | | | | | | | |
| 110 | <i>Staff holding a post provided for in the establishment plan</i> | | | | | | | |
| 1100 | Basic salaries | | 9.877.711 | 9.877.711 | 10.314.300 | 10.598.389 | 11.110.332 | 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). |
| 111 | <i>Other staff</i> | Article 1 1 0 | 9.877.711 | 9.877.711 | 10.314.300 | 10.598.389 | 11.110.332 | |
| 1110 | Contract Agents | | 2.507.984 | 2.507.984 | 2.428.441 | 2.428.441 | 2.615.195 | 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) | | 672.621 | 672.621 | 814.031 | 814.031 | 873.405 | This appropriation is intended to cover basic salaries and all benefits of SNEs. |
| | | Article 1 1 1 | 3.180.605 | 3.180.605 | 3.242.472 | 3.242.472 | 3.488.600 | |
| 12 | RECRUITMENT/DEPARTURE EXPENDITURE | CHAPTER 11 | 13.058.316 | 13.058.316 | 13.556.771 | 13.840.860 | 14.598.932 | |
| 120 | <i>Expenditure related to recruitment</i> | | | | | | | |
| 1201 | Recruitment and Departure expenditure | | 517.889 | 517.889 | 508.469 | 508.469 | 217.593 | 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 subsistence 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. |
| | | Article 1 2 0 | 517.889 | 517.889 | 508.469 | 508.469 | 217.593 | 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. |
| | | CHAPTER 1 2 | 517.889 | 517.889 | 508.469 | 508.469 | 217.593 | |

| | | | | | | | | |
|------------|---|----------------------|-------------------|-------------------|-------------------|-------------------|-------------------|---|
| 13 | SOCIO-MEDICAL SERVICES AND TRAINING | | | | | | | |
| 132 | Staff Development | | | | | | | |
| 1320 | Staff Development | | 447.501 | 447.501 | 450.000 | 450.000 | 343.000 | 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 | 447.501 | 447.501 | 450.000 | 450.000 | 343.000 | |
| 133 | Staff Welfare | | | | | | | |
| 1332 | Staff Welfare | | 307.000 | 377.000 | 238.200 | 238.200 | 283.808 | 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. |
| | | Article 1 3 3 | 307.000 | 37.700 | 238.200 | 238.200 | 283.808 | 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. |
| | | CHAPTER 1 3 | 754.501 | 824.501 | 688.200 | 688.200 | 626.808 | |
| 14 | TEMPORARY ASSISTANCE | | | | | | | |
| 142 | Temporary Assistance | | | | | | | |
| 1420 | External Temporary Staffing | | 408.400 | 408.400 | 518.000 | 518.000 | 588.000 | This appropriation is intended to cover the costs of temporary assistance (trainees and interim services). |
| | | Article 1 4 2 | 408.400 | 408.400 | 518.000 | 518.000 | 588.000 | |
| | | CHAPTER 1 4 | 408.400 | 408.400 | 518.000 | 518.000 | 588.000 | |
| 15 | External services in HR area | | | | | | | |
| 150 | External services in HR area | | | | | | | |
| 1500 | External services in HR area | | n/a | n/a | n/a | n/a | n/a | This appropriation is intended to cover the costs of external services in HR area such as (but not limited to) consultancy on competencies framework, support on reorganisation matters, annual staff satisfaction survey, consultancy on new HR tools, services provided by the EC including PMO, IDOC, etc. |
| | | Article 1 5 0 | n/a | n/a | n/a | n/a | n/a | |
| | | CHAPTER 1 5 | n/a | n/a | n/a | n/a | n/a | |
| | | Total Title 1 | 14.739.106 | 14.809.106 | 15.271.440 | 15.555.529 | 16.031.333 | |
| 2 | BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE | | | | | | | |
| 20 | BUILDINGS AND ASSOCIATED COSTS | | | | | | | |
| 200 | Buildings and associated costs | | | | | | | |
| 2001 | Building costs | | 1.000.719 | 1.004.965 | 1.081.300 | 1.081.300 | 1.061.957 | 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 | 1.000.719 | 1.004.965 | 1.081.300 | 1.081.300 | 1.061.957 | |
| | | CHAPTER 2 0 | 1.000.719 | 1.004.965 | 1.081.300 | 1.081.300 | 1.061.957 | |
| 22 | CURRENT CORPORATE AND ADMINISTRATIVE EXPENDITURE | | | | | | | |

| | | | | | | | | |
|------------|--|----------------------|------------------|------------------|------------------|------------------|--|--|
| 222 | Consultancy and other outsourced services | | | | | | | |
| 2220 | Consultancy and other outsourced services (incl. legal services) | 438.125 | 438.125 | 612.000 | 612.000 | 317.258 | This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. financial, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy, etc. | |
| | | Article 2 2 2 | 438.125 | 438.125 | 612.000 | 612.000 | 317.258 | |
| 223 | Corporate and Administrative Expenditures | | | | | | | |
| 2230 | Corporate and Administrative Expenditures | 78.000 | 78.000 | 75.000 | 75.000 | 19.600 | 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 courier costs, bank charges, interest paid and other financial and banking costs and other costs of corporate administrative nature. | |
| | | Article 2 2 3 | 78.000 | 78.000 | 75.000 | 75.000 | 19.600 | |
| | | CHAPTER 2 2 | 516.125 | 516.125 | 687.000 | 687.000 | 336.858 | |
| 23 | ICT | | | | | | | |
| 231 | Core and Corporate ICT expenditure | | | | | | | |
| 2312 | Core and corporate ICT costs | 2.150.054 | 2.150.054 | 2.391.048 | 2.391.048 | 2.891.344 | 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 | 2.150.054 | 2.150.054 | 2.391.048 | 2.391.048 | 2.891.344 | |
| | | CHAPTER 2 3 | 2.150.054 | 2.150.054 | 2.391.048 | 2.391.048 | 2.891.344 | |
| | | Total Title 2 | 3.666.898 | 3.671.144 | 4.159.348 | 4.159.348 | 4.290.159 | |
| 3 | OPERATIONAL EXPENDITURE | | | | | | | |
| 30 | ACTIVITIES RELATED TO OUTREACH AND MEETINGS | | | | | | | |
| 300 | Outreach, meetings and representation expenses | | | | | | | |
| 3001 | Outreach, meetings, translations and representation expenses | 387.000 | 402.780 | 768.800 | 768.800 | 643.615 | 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, ACCO as well as missions related to the implementation of Activities 9-11 as defined in the SPD 2026-2028 mainly covering horizontal tasks and other administrative services. | |
| 3002 | Operational missions | n/a | n/a | 512.200 | 512.200 | 382.200 | 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 | n/a | n/a | 255.000 | 255.000 | 264.600 | 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 2026-2028 related to performing operational tasks. | |
| | | Article 3 0 0 | 387.000 | 402.780 | 1.536.000 | 1.536.000 | 1.290.415 | |
| | | CHAPTER 3 0 | 387.000 | 402.780 | 1.536.000 | 1.536.000 | 1.290.415 | |
| 36 | CORE OPERATIONAL ACTIVITIES | | | | | | | |
| 361 | Activity 1 | | | | | | | |
| 3610 | Activity 1 - Support for policy monitoring and development | n/a | n/a | 294.037 | 294.037 | 267.295 | This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT). | |
| | | Article 3 6 1 | n/a | n/a | 294.037 | 294.037 | 267.295 | |
| 362 | Activity 2 | | | | | | | |
| 3620 | Activity 2 - Cybersecurity and resilience of critical sectors | n/a | n/a | 331.024 | 331.024 | 396.900 | This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT). | |
| | | Article 3 6 2 | n/a | n/a | 331.024 | 331.024 | 396.900 | |
| 363 | Activity 3 | | | | | | | |
| 3630 | Activity 3 - Capacity building | n/a | n/a | 691.409 | 691.409 | 541.940 | This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs). | |
| | | Article 3 6 3 | n/a | n/a | 691.409 | 691.409 | 541.940 | |
| 364 | Activity 4 | | | | | | | |
| 3640 | Activity 4 - Enabling operational cooperation | n/a | n/a | 1.537.091 | 1.537.091 | 1.888.950 | This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT). | |
| | | Article 3 6 4 | n/a | n/a | 1.537.091 | 1.537.091 | 1.888.950 | |
| 365 | Activity 5 | | | | | | | |
| 3650 | Activity 5 - Provide effective operational cooperation through situational awareness | n/a | n/a | 1.476.118 | 1.476.118 | 1.274.000 | This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT). | |
| | | Article 3 6 5 | n/a | n/a | 1.476.118 | 1.476.118 | 1.274.000 | |
| 366 | Activity 6 | | | | | | | |
| 3660 | Activity 6 - Provide services for operational assistance and support | n/a | n/a | 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 | n/a | n/a | p.m. | p.m. | p.m. | |
| 367 | Activity 7 | | | | | | | |
| 3670 | Activity 7 - Development and maintenance of EU cybersecurity certification framework | n/a | n/a | 570.089 | 570.089 | 631.610 | This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT). | |

| | | | | | | | | |
|------|--|--------------------|------------|------------|------------------|------------------|------------------|--|
| 368 | Activity 8 | Article 3 6 7 | n/a | n/a | 570.089 | 570.089 | 631.610 | This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT). |
| 3680 | Activity 8 - Supporting European cybersecurity market, research & development and industry | | n/a | n/a | 563.687 | 563.687 | 578.200 | |
| | | Article 3 6 8 | n/a | n/a | 563.687 | 563.687 | 578.200 | |
| | | CHAPTER 3 6 | n/a | n/a | 5.463.454 | 5.463.454 | 5.578.895 | |

| | TITLE 3 | 7.430.471 | 7.739.551 | 6.999.454 | 6.999.454 | 6.869.310 | |
|------|--|-------------------|-------------------|-------------------|-------------------|-------------------|---|
| 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 | n/a | 16.000.000 | 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). 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 | p.m. | n/a | 60.000 | p.m. | 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. | n/a | | p.m. | 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 | n/a | p.m. | p.m. | 240.000 | 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 | n/a | p.m. | p.m. | 12.000.000 | 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). 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 | n/a | p.m. | p.m. | 12.223.333 | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for Cyber Reserve and SitCen which is currently in draft stage. This Contribution Agreement covers Cyber Reserve and SitCen (might span multiple years). |
| 4006 | Activities related to the Contribution Agreement for CRA SRP | n/a | p.m. | p.m. | | p.m. | This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for CRA SRP which is currently in draft stage. This Contribution Agreement covers CRA SRP operation (might span multiple years). |
| | Article 4 0 0 | n/a | 16.000.000 | p.m. | 24.523.333 | p.m. | |
| | CHAPTER 4 0 | n/a | 16.000.000 | p.m. | 24.523.333 | p.m. | |
| | TITLE 4 | n/a | 16.000.000 | p.m. | 24.523.333 | p.m. | |
| | GRAND TOTAL | 25.836.475 | 42.219.801 | 26.430.242 | 51.237.664 | 27.190.802 | |

ESTABLISHMENT PLAN 2026

| Category and grade | Establishment plan as part of voted EU Budget 2025 ¹ | | Modified Establishment Plan 2026 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 | | 4 | | 4 |
| AD 9 | | 14 | | 14 |
| AD 8 | | 16 | | 16 |
| AD 7 | | 13 | | 14 |
| AD 6 | | 7 | | 7 |
| AD 5 | | | | |
| Total AD | | 64 | | 65 |
| AST 11 | | | | |
| AST 10 | | | | |
| AST 9 | | 1 | | 2 |
| AST 8 | | 3 | | 2 |
| AST 7 | | 3 | | 1 |
| AST 6 | | 6 | | 7 |
| AST 5 | | 4 | | 4 |
| AST 4 | | 2 | | 2 |
| 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 Definitive adoption (EU, Euratom) 2025/31 of the European Union's annual budget for the financial year 2025

² The 2026 establishment plan includes request budget neutral amendment to MB to transform AST7 post to AD7 post.