



ENISA SINGLE PROGRAMMING DOCUMENT 2025 -2027

Including Multiannual planning, Work programme 2025 and Multiannual staff planning

JANUARY 2025

CONTACT

For contacting ENISA please use the following details:
info@enisa.europa.eu
website: www.enisa.europa.eu

LEGAL NOTICE

This publication presents the European Union Agency for Cybersecurity (ENISA) Single Programming Document 2025–2027 as approved by the Management Board in Decision No MB/2024/16. The Management Board may amend the Work Programme 2022–2024 at any time. ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source. Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2025

This publication is licenced under CC-BY 4.0 “Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated”.

Copyright for the image on the cover and internal pages: © Shutterstock

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

Luxembourg: Publications Office of the European Union, 2025

| Linguistic version | Catalogue number | ISBN | ISSN | DOI |
|---------------------------|-------------------------|-------------------|-------------|-----------------|
| PDF Web | TP-01-25-001-EN-N | 978-92-9204-686-6 | 2467-4176 | 10.2824/9067232 |



ENISA SINGLE PROGRAMMING DOCUMENT 2025–2027

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

| | |
|---|-----------|
| SECTION I | |
| GENERAL CONTEXT | 15 |
| SECTION II | |
| MULTIANNUAL PROGRAMMING 2025–2027 | 21 |
| 2.1. MULTIANNUAL WORK PROGRAMME | 21 |
| 2.2. HUMAN AND FINANCIAL RESOURCES – OUTLOOK FOR 2025-2027 | 27 |
| 2.2.1. Overview of the past and current situations | 27 |
| 2.3. OUTLOOK FOR 2025–2027 | 32 |
| 2.4. RESOURCE PROGRAMMING FOR 2025–2027 | 33 |
| 2.4.1. Financial resources | 33 |
| 2.4.2. Human resources | 33 |
| 2.5. STRATEGY FOR ACHIEVING GAINS IN EFFICIENCY | 35 |
| SECTION III | |
| WORK PROGRAMME FOR 2025 | 39 |
| 3.1. OPERATIONAL ACTIVITIES | 41 |
| 3.2. CORPORATE ACTIVITIES | 70 |

| | |
|---|------------|
| ANNEX 1 ORGANISATION CHART AS OF 31.12.2024 | 85 |
| ANNEX 2 RESOURCE ALLOCATION PER ACTIVITY 2025–2027 | 88 |
| ANNEX 3 FINANCIAL RESOURCES 2025–2027 | 90 |
| ANNEX 4 HUMAN RESOURCES – QUANTITATIVE | 93 |
| ANNEX 5 HUMAN RESOURCES – QUALITATIVE | 97 |
| ANNEX 6 ENVIRONMENT MANAGEMENT | 102 |
| ANNEX 7 BUILDING POLICY | 103 |
| ANNEX 8 PRIVILEGES AND IMMUNITIES | 104 |

| | |
|---|------------|
| ANNEX 9 EVALUATIONS | 105 |
| ANNEX 10 STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS | 106 |
| ANNEX 11 PLAN FOR GRANTS, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS | 107 |
| ANNEX 12 STRATEGY FOR COOPERATION WITH NON-EU COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS | 108 |
| ANNEX 13 ANNUAL COOPERATION PLAN 2025 | 109 |
| ANNEX 14 PROCUREMENT PLAN 2025 | 110 |

ABBREVIATIONS

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

| | | | |
|----------------|---|---------------|---|
| EIOPA | European Insurance and Occupational Pensions Authority | NISD | NIS Directive |
| EIT | European Institute of Innovation & Technology | NIS2 | NIS2 Directive |
| EMAS | Eco-Management and Audit Scheme | NIS CG | NIS Cooperation Group |
| EMSA | European Securities and Markets Authority | NLO | National Liaison Officers |
| ENISA | European Union Agency for Cybersecurity | OOTS | The Once Only Technical System |
| ENTSO | European Network of Transmission System Operators for Electricity | SC | Secretary |
| ERA | European Railway Agency | SCCG | Stakeholder Cybersecurity Certification Group |
| ETSI | European Telecommunications Standards Institute | SLA | Service-level agreement |
| EUCC | European Union Common Criteria scheme | SMEs | Small and medium-sized enterprises |
| EUCI | European Union classified information | SNE | Seconded national expert |
| EU5G | European Union certification scheme for 5G networks | SOCS | Security Operation Centres |
| EU-LISA | European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice | SOP | Standard Operating Procedure |
| Europol | European Union Agency for Law Enforcement Cooperation | SPD | Single Programming Document |
| FTE | Full-time equivalent | TA | Temporary agent |
| 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 | | |



FOREWORD

This Single Programming Document (SPD) for the years 2025-2027 outlines the steps ENISA will take to enhance the maturity and resilience of cybersecurity in the EU.

Firstly, as the EU took legislative steps to strengthen its cybersecurity framework with the aim of protecting its economy, society and everyday life across Europe, the strategy of the Agency was revised accordingly by the Management Board in 2024 to further clarify and amend the Agency's priorities and focus. This program thus includes the new indicators to measure the success of its strategic objectives. At the same time, the Agency streamlined its operational activities and adjusted its organizational structure to more effectively manage these activities and improve its capacity to deliver more efficiently.

Secondly, approximately half of ENISA's operational resources are allocated towards enabling operational cooperation between Member States, including through dynamic and improved common situational awareness. The contribution agreement of EUR 20 million from the EU budget, for which the European Commission entrusted ENISA to manage in Autumn 2023, will enable the Agency to continue to scale up and expand its support to EU Member States in 2025 and 2026. Furthermore in the end of 2024, the Agency and the European Commission signed another Contribution Agreement, which includes EUR 12 million for the establishment, management of the CRA Single Reporting Platform and EUR 2.55 million for the continuation of the Support Action, which will be implemented by 31st December 2027. The combination of these measures will enable Member States to identify potential cyber risks, assess serious vulnerabilities and take timely action to mitigate attacks and respond effectively to threats.

Thirdly, through this work program ENISA has strengthened its capabilities and capacities to support EU Member States with implementation of the NIS2 Directive, the Cyber Resilience Act and the Cyber Solidarity Act, as well as ensuring the EU cybersecurity certification framework is implemented efficiently.

Through cooperation with Member States and Union bodies, private and public organizations, and various cyber communities as well as through synergies with like-minded international partners, ENISA strives to ensure a secure and trusted digital environment for all businesses and citizens in Europe in the complex geopolitical context and the evolving threat landscape of 2025.

Juhan Lepassaar
Executive Director

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 on cybersecurity matters to Member States and EU institutions, bodies and agencies (Union entities). It contributes to the development and implementation of the Union's cybersecurity policies.

ENISA's aim is to strengthen trust in the connected economy, to boost resilience and trust in the Union's infrastructure and services, and to keep European society and citizens digitally secure. The Agency aspires 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 framework for cooperation. ENISA plays a vital role in fostering cooperation among cybersecurity stakeholders (Member States, Union entities, and other communities). In its efforts, ENISA emphasises complementarity, engages stakeholders based on their expertise and roles 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 opportunities and support early mitigation strategies for challenges thus improving 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, effective and consolidated information and knowledge is the foundation of informed decision-making, along with proactive and reactive protection and resilience based on a better understanding of the threat landscape. The much-needed common understanding and assessment of the 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 an absolute 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 various 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 critical sectors and supporting the 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. Cyberattacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to cyber threats and potential cyber crises. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and Union entities for faster response times and proper coordination of efforts at the strategic, operational and technical levels. Understanding the ongoing situation is the key to be effectively prepared and to be able to respond to cyber incidents, threats and crises.

STRATEGIC OBJECTIVE: 'Strong cybersecurity capacity within the EU'

The frequency and sophistication of cyberattacks is rising steadily while, at the same time, the use of digital infrastructures and technologies is increasing rapidly. The need for cybersecurity skills, knowledge and competences exceeds the supply. The 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 addresses capacity building across the entire spectrum, by investing in young people through competence building and training whilst providing continuous up- and reskilling opportunities for professionals to enable them to keep up with the fast-changing nature of cybersecurity. The focus is not only on increasing the cybersecurity skillset in Member States and contributing to the objectives of the Cybersecurity Skills Academy, but also on making sure that various operational communities always possess the capacity to deal appropriately 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, using the lessons learned from well-planned exercises effectively.

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 Technology (ICT) products, services and processes and ensuring their trustworthiness, a common European approach between social, market, research and foresight, economic and cybersecurity needs brings with it the possibility of influencing the international community by introducing a competitive edge. Using means such as cybersecurity-by-design, market surveillance and certification will enable both the enforcement and promotion of trust in digital solutions.



SECTION I

GENERAL CONTEXT

This Single Programming Document sets out the activities that ENISA will undertake in the years 2025 to 2027 in accordance with the Agency's Regulation (EU) 2019/881 and the Cybersecurity Act¹ which governs the cybersecurity certification of information and communications technology. These activities will take into account ENISA's new Strategy, the transposition of the NIS2 Directive and the expected publication of the Cyber Resilience Act (CRA) and Cyber Solidarity Act (CSoA).

The CRA is set to enter into force in the second half of 2024 and manufacturers will have to place compliant products on the Union's market by 2027. NIS2 entered into force in January 2023 and the transposition deadline was reached on 17 October 2024.

The NIS2 Directive introduces legal measures to enhance cybersecurity across the EU, by imposing obligations on entities in 18 economic sectors concerning security requirements and the notification of incidents. It also mandates that Member States bolster their preparedness, such as by expanding the roles and responsibilities of Computer Security Incident Response Teams (CSIRTs) and relevant authorities. Another key aspect of the NIS2 Directive is its promotion of cooperation among Member

States, reinforcing the Cooperation Group established under the original NIS Directive to facilitate strategic collaboration and information exchange. Additionally, the Directive formalises the EU-CyCLONe Network, which aims to improve preparedness for and coordinated management of large-scale cybersecurity incidents and crises at the operational level, ensuring the regular exchange of pertinent information among Member States and EUIBAs.

The role of ENISA is to support the Commission and the Member States with the implementation of NIS2 at national level, including the implementation of the EU vulnerability database and the registry for digital entities, to support cross border collaboration, including peer reviews, as well as to publish reports on the state of cybersecurity in the Union.

The CRA is anticipated to come into effect in the second half of 2024. This Act establishes common cybersecurity requirements for products with digital elements, including hardware and software, aiming to reduce vulnerabilities and ensure that cybersecurity is prioritised during the design and production stages. It also mandates vulnerability management throughout the product's lifecycle. Manufacturers will be required to comply with these rules 36 months after the Act

1 - Regulation (EU) 2019/881

takes effect. Additionally, reporting obligations for actively exploited vulnerabilities and significant cybersecurity incidents will be enforced 21 months after the Act's entry into force.

The role of ENISA is to receive, together with the CSIRTs, notifications concerning actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements, to establish the CRA's single reporting platform for these notifications, to prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and to collaborate with the European Commission and national authorities in market surveillance.

The CSOA is expected to have taken effect by the end of 2024. This Act establishes measures to enhance the Union's ability to detect, prepare for and respond to cybersecurity threats and incidents. It introduces three key pillars to bolster solidarity at the Union level for the better detection of, preparation for and responses to significant or large-scale cybersecurity incidents. These pillars are the European Cybersecurity Alert System (a pan-European Network of Cyber Hubs), the Cybersecurity Emergency Mechanism, and the European Cybersecurity Incident Review Mechanism.

ENISA will be entrusted with the operation and administration of the EU Cybersecurity Reserve partially or fully, subject to the contribution agreement and shall, with the support of the CSIRTs network and the approval of the Member States concerned, review and assess threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident in the context of the Cybersecurity Incident Review Mechanism.

The revision of Regulation (EU) 910-2014 requires Member States to issue European Digital Identity Wallets certified at a high level of security in 2026. In order to meet this deadline, the Regulation foresees parallel work on national certification schemes and a CSA based EU certification scheme which will become compulsory once available. As a matter of priority ENISA is developing, at the request of the EC, an EU scheme for the EUDI wallet. In addition, ENISA has assisted the EC in developing the Implementation Act on certification and is expected to continue collaborating with MSs in order to assist them in the development of their national schemes.

The Regulation (EU, Euratom) 2023/2841 regarding measures for a high common level of cybersecurity at EU institutions, bodies and agencies (Union entities) was adopted in 2023 and entered into force on 7 January 2024.

The Commission Implementing Regulation (EU) 2024/482 laid down rules for the application of the Cybersecurity Act (CSA) as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

A number of sector-specific cybersecurity initiatives, include the following.

- o Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) which entered into force on 16 January 2023.
- o The Commission Delegated Regulation (EU) 2022/1645 and Commission Implementing Regulation (EU) 2023/203 was adopted in 2022 in the aviation sector.
- o The Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS) was adopted on 11 March 2024.
- o The new European Digital Identity Framework amending Regulation (EU) No 910/2014 entered into force in May 2024.
- o The European Health Data Space (EHDS) Regulation is in the final stages of the adoption process.

Other recent Union legislation relevant to cybersecurity includes among others the Artificial Intelligence Act (AIA), Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act - DMA), Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act - DSA), Regulation (EU) 2023/178 (Chips Act) and Regulation (EU) 2023/2854 (Data Act).

Anticipated future policy context

The adoption and implementation of policy frameworks is one key response area in which the EU is making a difference in cybersecurity, as the policies and initiatives being put in place in the coming years are determining how the EU faces the cybersecurity challenges of today and tomorrow.

The following table places the work of the agency into the anticipated future policy context

| Policy file | Status of policy file | Background and ENISA role / plans |
|-------------------------|-----------------------|--|
| Cybersecurity Act (CSA) | Evaluation | A review is taking place in accordance with Article 67 of the CSA. |
| NIS2 Directive | Implementation | <p>The Commission is gathering input on the draft implementation act under the NIS2 Directive which aims to ensure a high common level of cybersecurity across the Union.</p> <p>The Commission had planned to adopt by 27 October 2024 an implementing act that will establish the technical and methodological requirements for cybersecurity risk-management measures applicable to certain entities in the digital infrastructure, digital service providers, and ICT service management (business-to-business) sectors.</p> |

Threat landscape

The ENISA Threat Landscape report highlights findings on the cybersecurity threat landscape over the course of 2023 and 2024. In the report, seven major cybersecurity threats were identified, with attacks targeting system availability ranking as the most critical, followed closely by ransomware and data threats. The study delved deeply into each threat by examining thousands of publicly documented cybersecurity incidents and events. The report provides a relevant deep-dive on each one of them by analysing several thousand publicly reported cybersecurity incidents and events, including ransomware, malware, social engineering and threats against availability. The report is complemented by a detailed analysis of four distinct categories of threat actors, namely state-nexus actors, cybercrime actors and hacker for hire actors, private sector offensive actors and hacktivists.

As the NIS2 Directive takes effect in 2024, an analysis of the cybersecurity threat landscape across various sectors has been conducted. A significant number of incidents have once again been observed, particularly targeting organisations in public administration (19%), transport (11%), and finance (9%) sectors.

International developments

Building on the developments of the last three years of ENISA's international strategy, the international

cooperation dimension of cybersecurity is likely to continue driving some of ENISA's activities within its mandate of Article 12 of the CSA. In the last few years, ENISA has focused on outreach cooperation with Ukraine and the US as well as seeking strengthened cooperation in the Western Balkans, with NATO and within the EU's Eastern partnership programme.

NON-LEGISLATIVE POLICY DEVELOPMENTS

ENISA Cybersecurity Support Action

During the course of 2023, ENISA developed and implemented the Cybersecurity Support Action to assist EU Member States (MSs) in the short term in view of the immediate and elevated threat of malicious cyber activities due to the ongoing Russian war of aggression against Ukraine. This mechanism aims to complement and not duplicate efforts by MSs and those at the EU level to increase the level of protection and resilience against cyber threats by assisting MSs in their efforts to improve their capability to respond to cyber threats and incidents.

An EU contribution agreement was signed in December 2023 to continue the Cybersecurity Support Action for EUR 20 million from the Digital Europe Programme and implement the Action by 31 December 2026. The work programme now

includes a specific activity earmarked to undertake the Cybersecurity Support Action, highlighting the objectives, outputs and taking into account lessons learned from the implementation in 2023.

The implementation of ENISA's Cybersecurity Support Action illustrates the Agency's capacity to co-ordinate and deliver on such complex services and constitutes a strong asset for the future implementation of the CSoA. While managing the EU's Cybersecurity Support Action, ENISA developed the necessary know-how and tools to deliver both ex-ante and ex-post cybersecurity services in collaboration with EU service providers, which EU Member States may use.

When the Cyber Solidarity Act enters into force, in accordance with the Cyber Solidarity Act, the Commission will partly or fully entrust the administration and operation of the EU's Cybersecurity Reserve to ENISA.

Implementation of the EU's cybersecurity certification framework

ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework (ECCF) by preparing the candidate schemes and supporting their maintenance once adopted. In this task ENISA relies on area experts and operates in collaboration with National Cybersecurity Certification Authorities (NCCAs) across the MSs. It is expected that the candidate cybersecurity certification schemes proposed by ENISA will be adopted as Commission Implementing Regulations.

The schemes adopted under the ECCF will allow for the certification of ICT products, services and processes, and at a later stage (following the entry into force of the CSA Amendment), managed security services (MSS). This is expected to contribute to increasing the level of stakeholder trust in digital solutions across the EU. Currently, the first cybersecurity certification scheme on Common Criteria has been adopted. The draft candidate scheme on cloud services has been submitted to the ECCG for opinion. Once an agreed opinion is available, ENISA will take it into consideration and then deliver the candidate scheme to the Commission.

Furthermore, an ad hoc working group (AHWG) has been supporting ENISA in drafting the candidate cybersecurity certification scheme for 5G networks and a public consultation on the technical specifications for eUICC has been launched. In 2025, a new AHWG is expected to be launched in relation to a scheme for the EU Digital Identification Wallet (EUDIW). Requests for other schemes are likely to follow in line with the Union Rolling Work Programme (URWP), in particular on managed security services.

ENISA is pursuing its strategy of reusing cybersecurity provisions across existing relevant cybersecurity certification schemes that are under development in an effort to contain the footprint of certification and facilitate transition. ENISA is also pro-actively supporting the Commission and the MSs in the maintenance of schemes.

The adopted schemes and those under preparation will also be mapped with the requirements of the CRA to provide the means for assessing the conformity of digital products, services and processes with the provisions of the digital single market in a way that ensures compliance with the requirements of the CRA. This approach sets the stage for other legal instruments on cybersecurity to use the synergetic effects of the cybersecurity certification framework. ENISA is currently responding to a request from the Commission for support with respect to the interplay between the EUCC and the CRA as well as support relating to the technical descriptions of products under the CRA.

ENISA will also support the development of means of certification that would allow the demonstration of compliance with certain requirements of Article 21 of the NIS2 directive, as this directive stipulates that MSs may require entities to use particular ICT products, services and processes, either developed by an essential or important entity or procured from third parties that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.

In terms of the Union rolling work programme that was published in February 2024 by the Commission, ENISA stands ready to support the Commission with the various editions of the programme.

EU crisis management framework

The 2017 Cybersecurity Blueprint describes a framework for EU cybersecurity crisis management, the roles of national and EU-level actors in responding to large-scale cybersecurity incidents and crises, and how existing relevant mechanisms can make full use of existing cybersecurity entities at EU level. It followed a call from the Council for such a blueprint, given that the 2016 NIS Directive did not provide for a Union cooperation framework should large-scale cybersecurity incidents and crises arise.

The Cybersecurity Blueprint proposed a concept and a definition of large-scale cybersecurity incidents which became the basis for the definition of a 'large-scale cybersecurity incident' in the NIS2 Directive, which formally established a mechanism for coordinated action to ensure a rapid and effective response because of the high degree of interdependence between sectors and Member States. Under this mechanism, EU-CyCLONe should work as an intermediary between the technical and political levels during large-scale cybersecurity incidents and crises and should enhance cooperation at the operational level and support decision-making at the political level. In cooperation with the Commission, and in consideration of its competence in the area of crisis management, EU-CyCLONe may build on the CSIRTs network findings and, where feasible, leverage its own capabilities to contribute to the impact analysis of large-scale cybersecurity incidents and crises.

The Council, in its Conclusions on the Future of Cybersecurity of 22 May 2024, 'call[ed] upon the Commission to swiftly evaluate the current cybersecurity Blueprint and, on this basis, propose a revised cybersecurity Blueprint that addresses the current challenges and the complex cyber threat landscape, and to expand the current principles to cover the full lifecycle of crisis management, and that the role of ENISA, along with the roles of the Commission and the High Representative, in line with their competences, should focus in particular on supporting horizontal coordination.'

Cyber defence policy

The Council's conclusions of 22 May 2023 on the EU's policy on cyber defence emphasised the importance of fostering mutually beneficial cooperation between

ENISA, CERT-EU and other EU agencies. ENISA can play a pivotal role in sharing expertise with CSDP military missions and facilitating the exchange of best practices among Member States and the EDA, including the development of a skilled cybersecurity workforce in line with the Cyber Solidarity Act. Deliverables could include specialised training programmes, threat intelligence sharing platforms, and coordinated efforts to improve workforce capabilities through joint simulations and exercises.

Cybersecurity Skills Academy

On 18 April 2023, as part of a cyber package, the Commission adopted a communication on the Cybersecurity Skills Academy inviting actors to take action to close the skills gap in the cybersecurity workforce. The academy aims at fostering the generation of knowledge through education and training by working on a common language for role profiles for cybersecurity and associated skills, namely the European cybersecurity skills framework (ECSF), and also through pilots for attestation schemes for cybersecurity competences.

Ensuring a better channelling and visibility of available funding opportunities for skills-related activities will maximise their impact. All stakeholders need to take action by making concrete cybersecurity pledges and integrating cybersecurity skills into their national strategies, and by defining indicators for monitoring the evolution of the market to better understand the needs and the offers of training. They must also better direct funds towards cybersecurity needs.

ENISA plays a valuable role in the implementation of the tasks outlined by the academy, all in collaboration with relevant stakeholders, namely the European Cybersecurity Competence Centre (ECCC), the National Competence Centres, the NIS CG and others. The recent Eurobarometer survey² on skills confirmed the need for the EU to reinforce cybersecurity skills due to an increasing shortage in these skills; indeed, more cybersecurity specialists are required and the number of staff who are highly aware of cybersecurity issues needs to be increased in every company across the EU.

2 - Eurobarometer survey confirms EU must reinforce cybersecurity skills | Shaping Europe's digital future (europa.eu)



SECTION II

MULTIANNUAL PROGRAMMING 2025–2027

Europe has for decades been taking steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA reviewed and updated ENISA's strategy³ in June 2024, which builds on the Cybersecurity Act (CSA) and outlines how the Agency will strive to meet the expectations of the cybersecurity ecosystem in a medium- to long-term perspective in a manner that is open, innovative and 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.

2.1. MULTI-ANNUAL WORK PROGRAMME

The following table maps the strategic objectives stemming from ENISA's strategy against the activities of the work programme and the associated indicators used to measure the progress of the objectives.

3 - Pending approval at the MB November 2024 meeting

| Strategic objectives | | Vertical strategic objectives | | | |
|---------------------------------|---|--|---|--|---|
| | | Effective and consistent implementation of EU policies on European cybersecurity | Effective Union preparedness to respond to cyber incidents, threats and crises | Strong cybersecurity capacity within EU | Building trust in secure digital solutions |
| Horizontal strategic objectives | Empowered communities in an involved and engaged cyber ecosystem | Uptake of ENISA's recommendations to support Member States and stakeholders in implementing EU legislation | Use of ENISA's secure infrastructure and tools and the added value of the support to operational cybersecurity networks | Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, training) | Number of EU certification schemes developed and maintained, number of EU regulations making reference to the 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 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 MSs, EUIBAs and, on a case by case basis, DEP associated third countries | Extent of advice 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 for the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG) |
| | Consolidated and shared cybersecurity information and knowledge support for Europe | Uptake of recommendations stemming from NIS2 Article 18 report | EU Vulnerability Database is operationalised by ENISA and MSs and stakeholders are highly satisfied with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats | Percentage of MSs that use ECSF | Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and is being operated successfully |

ENISA Corporate Strategy

ENISA's corporate vision is to make a contemporary and attractive workplace available for all, based on trust and inclusion, while developing and transforming itself 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 thing in terms of actions and 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 through a 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 for 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 workforce that is flexible, highly skilled and fit-for-purpose and which 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 EU Agencies, leverage standard technologies where possible and support flexible ways of working.

The table below highlights the activity responsible 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 for the Corporate Strategy (including results from the 2023 Staff Satisfaction Survey) to be reported under the 2023 annual activity report. In addition, 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) |
|------------------------------------|---|----------------------------------|--|
| People centric organisation | Effective workforce planning and management | Activity 11 | <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 in accordance with 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 the year according to its annual recruitment results. • Vacated staff posts are fulfilled in less than 300 days according to 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. |
| | Efficient talent acquisition, development and retention | Activity 11 | <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. |
| | Caring and inclusive modern organisation | Activity 11 | <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 |

| | | | |
|-------------------------------------|---|-------------------|---|
| Service centric organisation | Ensure efficient corporate services | Activities 9 & 11 | <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. • 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 EUIBAs (under SLAs, MoUs or other arrangements) found through an annual internal procedure |
| | Introduce digital solutions that maximise synergies and collaboration within the Agency | Activities 9 & 11 | <ul style="list-style-type: none"> • Implement (replace or develop) at least five user-centred, 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 | Activities 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 previously as found by an annual review. • Percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have been last reviewed more than four years previously as found in an annual review. |
| | Developing service propositions with additional external resourcing | Activities 9 & 11 | <ul style="list-style-type: none"> • At least three SLAs signed and in operation with EUIBAs 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"> • TBC. • 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's HQ building to reduce the climate impact of the HQ building by 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's 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 by procuring event management support, and 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. |
| | Develop efficient framework for continuous governance to safeguard high level of IT and physical security | Activity 9 & 11 | <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 be 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 in proportion 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. |

2.2. HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2025-2027

2.2.1. Overview of the past and current situation

Over the past few years, the Agency has undertaken persistent and sustained efforts to better manage, prioritise and balance the resources allocated to it in order to adjust to the ever-increasing demand for ENISA’s services by Member States and stakeholders. The actions undertaken to address the effective and efficient use of resources have included the following.

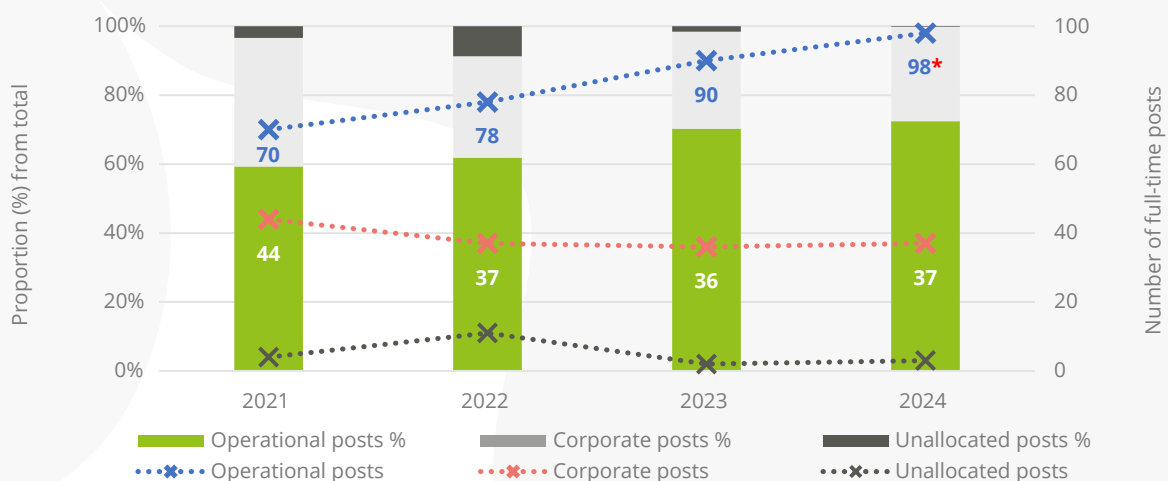
2.2.1.1. Recruiting new talent and increasing operational capacities

The Agency has taken significant strides to improve the fulfilment of its Establishment Plan with an increase from 87% in 2022 to 98% as of 2024. This was despite increasing competition for cybersecurity talent⁴ and – compared to the private sector and the living standards of more economically advanced Member States – the uncompetitive overall salary and support package which the Agency can offer in its host country. In parallel, the Agency has also taken

persistent measures over the past four years to rebalance the allocation of posts towards operational units and functions at the expense of corporate units and functions – the latter of which have been externalised to the maximum extent possible.

This followed the reorganisation of the Agency under the direction of Management Board decision No MB/2020/9, according to which all support and corporate functions (including administrative and secretarial support etc) were to be concentrated in corporate units from 1 January 2020 onwards, leaving in operational units only the posts in which the purpose is entirely linked with operational tasks and functions as described under Title II Chapter II of the Cybersecurity Act (CSA). Although the rebalancing has increased the human resources needed to deliver the operational mandate of the Agency (please see graph below), it has reached its natural limits. Further internal adjustment and reallocation at the expense of corporate activities would mean significant erosion of the Agency’s administrative capacity including its ability to sustain security (IT and physical), legal, financial and procurement, compliance functions and other corporate support systems.

Evolution of the allocation of the Agency's staff policy plan posts 2021-2024



* Including for a limited duration an additional 10 CA posts financed through the dedicated Contribution Agreement under Activity 6 (Activity 5b in SPD2024).

4 - Demand for skilled professionals in the field of cybersecurity is growing, with some estimates of the Joint Research Centre (JRC) pointing to a shortage of 1 million cybersecurity employees within the EU, and 3.5 million worldwide.

2.2.1.2. Addressing critical HR needs through reprioritisation and externalisation of administrative tasks

In 2022 the Agency assessed its internal workforce needs for 2023-2025 within its annual workforce review and concluded that the Agency would need an additional 41.5 FTEs in order to address all external as well as internal expectations. 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 workforce needs to the greatest extent possible.

The Agency, under the direction of its Management Board, took steps in 2023 and 2024 to deprioritise or suppress a number of outputs in the SPD. On that basis and through both restructuring and reallocating existing posts as well as using previously unallocated posts, the Agency was able to allocate a total of 10 FTEs to match the most critical operational and corporate high or medium needs in 2024. It also took steps to further externalise some corporate services and functions (such as administrative and secretarial support and technical financial assistance) which has rendered a service provision comparable to a saving of five FTEs. Thus, through a combination of measures taken by the Management Board within SPD2024 and the Agency in the course of its annual workforce review in 2023, the Agency was able to find an additional 15 FTEs to address both operational and corporate needs.

However, note should be taken that the 2023-2025 internal assessment of workforce needs, which was undertaken at the end of 2022, did not cover fully the needs arising from the CRA nor the CSoA, as neither the full scope of ENISA's future tasks nor the date of application of the proposals were yet clear during the time of assessment. Thus, the 2024 annual workforce review, which covers the estimated needs for 2024-2026, has mapped more fully the needs linked with the Agency's tasks as foreseen in the CRA and the CSoA (please see chapter 2.2. below).

2.2.1.3. Utilising internal and external synergies to gain additional resources and use current resources efficiently

Building service propositions. Based on the strategic discussions with the Agency's Management Board, the Agency developed service packages in key areas of its mandate during 2022-2023. The purpose of the service packages was to better

integrate ENISA's various outputs across different operational activities and thus build impactful and high added-value service propositions for ENISA's key beneficiaries – Member States and EUIBAs – whilst focusing resources by avoiding duplication of efforts (and thus waste of resources) within ENISA as well as with external partners. It also helped the agency to prioritise its actions, build and make better use of internal synergies, and ensure that adequate resources are reserved across the Agency for priority tasks in a transparent manner.

External operational partnerships. Building on the service packages and developing further service propositions across operational activities, the Agency has, over the period 2020 to 2024, developed external partnerships and synergies across all operational activities. This has ensured the efficient use of expertise and human resources by avoiding the duplication of effort – or by building new services – and has helped to increase the Agency's resources. Notable examples include the following.

- Cooperation with the European Commission and the partner DG CNECT in delivering services to increase the preparedness of Member State's critical entities and ensure capacities to assist in incident response if requested has had a huge impact on the Agency's SPD, i.e. on how the Agency delivers its tasks under Activities 3, 5 and 6 (formerly 3, 5a and 5b in SPD2024), and what it delivers. The Agency received from the Commission an additional EUR 15 million budget in 2022-2023 [and an additional EUR 20 million budget for 2024-2026 under the Contribution Agreement signed in Q4 2023, including the possibility of financing a temporary increase of up to 12 CA posts to fulfil the services delivered to the Member States under the Cooperation Agreement (2 CAs for Activity 5 and 8 CAs for Activity 6)]. The cooperation has been instrumental for the Agency in the area of operational support and capacity building and, besides strengthening its current resourcing, has contributed to building a partnership which may be further used under the CSoA.
- Structured cooperation with CERT-EU entered its fourth year in 2024 and it has significantly supported the Agency's ability to deliver its tasks under Activity 5a of SPD2024, namely, to develop better common situational awareness for the

Union, as mandated by Article 7 of the CSA, through the delivery of such joint products as Joint Rapid Reports and Joint Cyber Assessment Reports (including in close cooperation with EC3 and EEAS). The structured cooperation with CERT-EU entered its fourth year in 2024, significantly supporting the Agency's ability to deliver its tasks under Activity 5a of SPD2024. Now, with the new Regulation on Cybersecurity 2023/2841, ENISA and CERT-EU strive to synergise their cooperation even further. This cooperation has been strengthened by joint work on the EUIBA Standard Operating Procedures, which serve as a foundation for coordinated responses to incidents and intelligence sharing with other EU agencies and generate an additional revenue stream for the Agency.

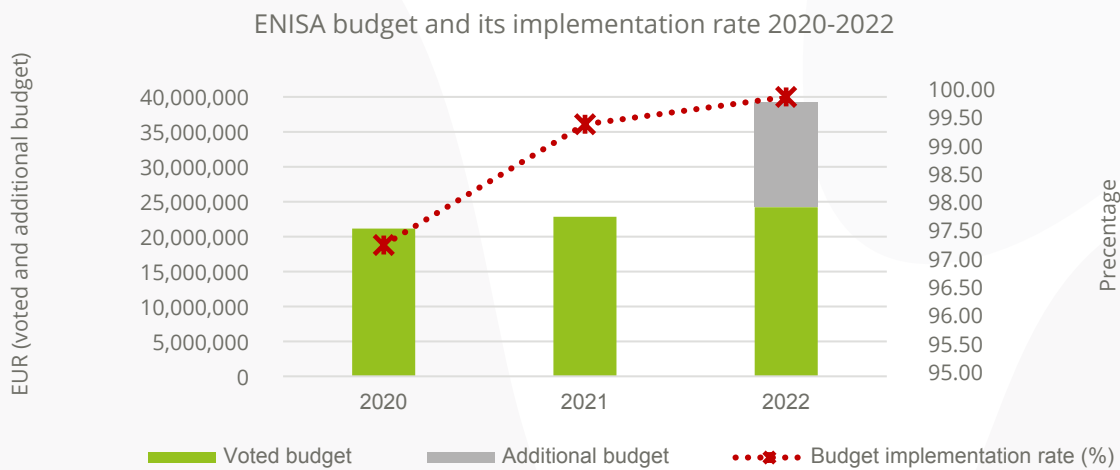
- As an example of the latter, a service level agreement with **EU-LISA**⁵ which covers support services offered by ENISA to EU-LISA on the planning, execution and evaluation of upcoming annual exercises has been renewed annually (2023, 2024 etc), creating a steady additional revenue stream to support the Agency's capacity building efforts (Activity 3).
- An MoU with the **European Cybersecurity Competence Centre (ECCC)** was signed in Q4 2023 with the aim of supporting Activity 3 by developing joint objectives (with relevant programming KPIs) with ECCC to help to tackle the skills gap in cybersecurity under the European Cybersecurity Skills Framework as foreseen in the Commission's communication on the 'European Cybersecurity Skills Academy'. The MoU is also expected to help in exploiting synergies under Activity 8 by setting up a joint cybersecurity market observatory, which should assist in fulfilling ENISA's new market related tasks under the CRA and in coordinating research initiatives across other work programme activities.
- The MoU with the **European Railway Agency** (ERA), which entered into force in 2023, and an extension of the MoUs with the **European Banking Authority** (EBA) and with **ESMA** and **EIOPA**, concerning the implementation of incident reporting under DORA and its alignment with other corresponding NIS2 requirements, help to align ENISA's support for MSs under the critical sectors of NIS2 with the activities of other Union bodies in these sectors, including in the area of cybersecurity requirements (with ERA) and incident reporting (with EBA, ESMA and EIOPA). This strengthens the Agency's ability to assist stakeholders in implementing or reporting on NIS2 requirements under Activity 2 and Activity 8 in SPD2024. There is a potential for further additional external resourcing income with the potential use of ENISA's enabled CIRAS platform for incident reporting under DORA.
- **Shared services and partnerships in corporate and administrative areas.** In late 2022 the Agency signed a service level agreement to create corporate synergies with the European Cybersecurity Competence Centre (ECCC) covering accounting, data protection and information security. ENISA has thus been acting as a corporate service provider for the ECCC in the area of accounting and data protection as of January 2023. The Agency has been further providing legal support services to the European Centre for the Development of Vocational Training (CEDEFOP) under the MoU which also foresees cooperation in joint procurement, shared financial services, human resources, IT solutions and in the area of data protection. Shared service agreements are also in place with the European Union Intellectual Property Office (EUIPO) and the Agency has continued to build on its shared services strategy and further build upon the partnership model with other EUIBAs – in particular with the corporate service centres of the European Commission – and is also exploring new avenues [such as, for example, with EIT and EIOPA, with whom the Agency launched a joint service centre for HR, procurement and corporate cybersecurity support services in 2024]. During 2023, the Agency continued supporting the network in relation to the implementation of cybersecurity requirements in Regulation 2023/2841 on common binding rules on cybersecurity for Union entities, particularly through a pilot project on shared services for cybersecurity risk management, such as a virtual CISO. This pilot project has been developed in close cooperation with CERT-EU and six other Union entities that volunteered to participate. These cooperation formats have delivered efficiency gains and/or generated additional external income, enabling the Agency to prioritise reallocating posts to operational tasks (see 2.1.1 above).

5 - European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice

2.2.1.4. Maximising to the outmost the use of existing budgetary resources

Though all Agencies are expected to commit all their voted budget, the minimum benchmark is set at 95%. Thus, the margin of manoeuvre between maximum and minimum is 5%, which as the budget of the Agency grows, can yield a notable difference. Over 2021-2023 the Agency significantly increased its budget implementation rate to ensure that it used all the resources to the maximum extent possible (see graph below). Those persistent efforts, which included a combination of measures – such

as imposing financial KPIs on all budget managers, better budgetary planning and monitoring etc – have increased the budget implementation rate to 100% in the past two years. As the overall budget of the Agency has increased, this high implementation rate meant that in 2023, for example, the Agency executed a commitment rate of 100% of its voted budget. Cumulatively over 2021-2023, by increasing its budget implementation rate, the Agency has committed a total of EUR 1 802 058.78 more, an investment that would have been lost if the budget implementation rate had remained at its 2020 level (97%) during past three years.



Similar efforts have been taken to ensure the full implementation of all carry-over funds (C8). In this regard note should be taken that in 2023 the Agency

was able to pay out the vast majority of the additional EUR 15 million which was budgeted in late 2022 (the final C8 payment rate in 2023 was 96.14% for the voted budget and 99% for the ENISA support fund).

Summary table

| | 2021 | 2022 | 2023 | 2024 | TOTAL (cumulative) |
|--|------|---------------|------------|---------------|-----------------------|
| Additional posts allocated in Staff Policy Plan (FTE) | 3 | 5 | 2 | 0 | 10 |
| Additional posts availed outside Staff Policy Plan (FTE) | 0 | 0 | 0 | 12 | 12 |
| Reallocated existing posts (FTE) | 4 | 8 | 8 | 2 | 22 |
| FTE gained through externalisation of admin. functions | 0 | 0 | 0 | 5 | 5 |
| ...out of which long-term intramural contractors | 0 | 0 | 0 | 5 | 5 |
| ...out of which short-term interim intramural service providers | | | 12 | | 12 |
| ...others | | | 0 | | 0 |
| Operational revenue in addition to Union budget (EUR'000) | 120 | 15 000 | 320 | 20 120 | 35 480 |
| ...from European Commission | 0 | 15 000 | 0 | 20 000 | 35 000 |
| ...from other EUIBAs | 120 | 120 | 120 | 120 | 480 |
| Corporate revenue in addition to Union budget (EUR'000) | 0 | 0 | 200 | 200 | 400 |
| Total additional revenue (EUR'000) | | 15 000 | 320 | 20 320 | 35 880 |

Over the last three years the Agency has taken steps to use its human and budgetary resources more efficiently. Whilst its headcount in its Staff Policy Plan has increased by 10 FTEs from 118 in 2021 to 128 in 2023 – which has helped it to address new tasks – the Agency has used the internal restructuring of posts as

the main tool to allocate resources to new priorities. A total of 20 posts have been restructured and reallocated over the last three years in this way. This proves that the Agency is agile and able to address new service needs when they emerge.

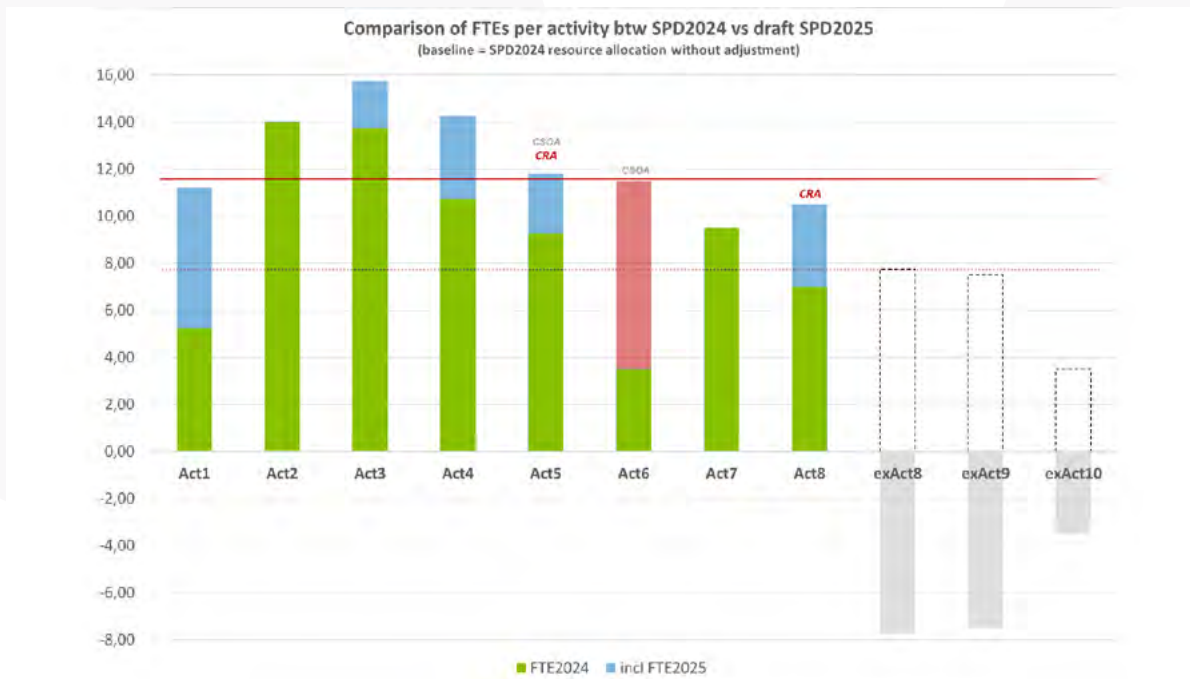
2.3 OUTLOOK FOR THE YEARS 2025-2027

The multi-annual financial framework for 2021-2027 that laid down the EU's long-term budget could not foresee the cumulative effects to the rapidly deteriorating cybersecurity threat landscape – including the effects of the Russian war of aggression against Ukraine. The Union's attack surface has increased which has also brought new challenges to manage supply-chain security. The political leadership of the EU has noted that: "The increasing level of cyber threats in a very difficult geopolitical context nowadays is putting under high stress the resources of all stakeholders involved in cybersecurity, including also those of ENISA /.../."⁶

Moreover, new Union legislation, such as the Cyber Resilience Act (CRA), the European Digital Identity Regulation (eIDAS2) and the Cyber Solidarity Act (CSOA), will bring new tasks to the Agency which demand strenuous resourcing between 2025-2027. Though the financial statements accompanying the CRA only allocated two additional FTEs, the CSOA does not allocate any new resources to the Agency. ENISA will put forward its estimations as regards to the resourcing needs which the Agency must address both in the context of the CRA and CSOA. In doing so, the Agency builds on the letter of 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 Agency must nevertheless prepare for any potential outcome, including the possibility that no new resources will be allocated to it. Therefore, in the 2025 draft work programme, ENISA has consolidated and restructured its operational outputs and activities. This consolidation, besides using existing synergies better, will also increase the budget as well as the median FTE counts per activity from slightly below 8 FTEs in 2024 to almost 12 FTEs. This is important as the higher median FTE count will give operational activities more 'operational depth' to absorb any unforeseen urgent work which might emerge. It also gives operational activities more room to manoeuvre - to reallocate resources within the activity should new priorities arise. The graph below shows the new FTE count per activity (using the 2024 allocation as the baseline), and reallocating the FTEs linked to the outputs of the three suppressed operational activities to the new activities. It does not include the FTE needs linked with new tasks emerging from the CRA and CSOA, though Activities 5 and 8 are marked as activities which could potentially incorporate the tasks related to the CRA, and Activities 5 and 6 to those of the CSOA.



6 - Former commissioner Thierry Breton, in his 06 September 2023 response letter to the Management Board.

Both the human resource requirements forecasted in the current draft of the SPD as well as ENISA's budgetary needs exceed those foreseen by the current establishment plan and budget projections. While ENISA remains committed to the continuous improvement of its administrative and operational efficiency, the Agency has almost exhausted all possible internal and external actions that it can take to resolve the insufficiency of its allocated resources. Therefore, unless further resources are allocated, ENISA in consultation with the MB and considering the priorities of the MSs and Commission would need to de-prioritise and limit the scope of its services within the existing tasks as well as within new tasks in its operational mandate.

2.4 RESOURCE PROGRAMMING FOR THE YEARS 2025-2027

2.4.1. Financial resources

The Agency has signed a EUR 20 million Contribution Agreement with the Commission for the years 2024-2026 so that ENISA can continue the Cybersecurity Support Action, with an agreement for finalising the implementation by 31 December 2026. Besides this additional revenue, which is used strictly for the purpose of supporting ENISA's ex ante and ex post services, the current total appropriations in the EU's Budget for 2025 amount to EUR 26.4 million.

In developing the first budgetary estimates of the first draft 2025 work programme, the Agency has taken into account its imperative needs and priorities and objectives as set out in the Corporate Strategy. In order to enable the above to be achieved, the Management Board has set the following benchmarks, which affect the Agency's budgetary and human resource planning in 2025-2027:

- The Agency's investment into the development of talent be a minimum of 4% of expenditure foreseen for the salaries of staff in active employment;
- The Agency dedicates at least 20% of its total investments to core, corporate and operational IT systems in order to ensure the cybersecurity of these systems;

- The Agency offsets 100% of its CO₂, CH₄ and N₂O emissions (approximately 150t) which will be generated across all its activities and as a result of its operations in the relevant budgetary period;
- Corporate overhead which shall be budgeted from the expenditure of all operational activities to ensure technical support for essential corporate services shall not be higher than 7% of the aggregated operational budget (Title III);
- The Agency's welfare (excluding medical) expenditure is at a maximum of 5% of expenditure foreseen for the salaries of staff in active employment;
- The Agency's expenditure on movable property and related costs for retaining a modern workplace is at a maximum of 1% of expenditure foreseen for the salaries of staff in active employment.

These factors mean that without an increase in the contribution from the Union, the Agency's operational budget (Title III) cannot be maintained at 2024 levels, which was already negatively impacted by a decrease of approximately 16.93% as compared to 2023.

Therefore, the current regular budget level is not sufficient for the Agency to fulfil its operational mandate, given the increased legislative and policy expectations and demands for its services in response to the heightened threat level. The Agency's budgetary needs, which are estimated on the basis of the development of the 2025 work programme, far exceed the Agency's budgetary means. The identified budget requirements the Agency forecasted when preparing the draft SPD25-27 in January to enable it to fulfil its mandate, and by extension the demands of stakeholders, amounted to an additional EUR 3.2 million.

2.4.2. Human resources

Though the level of ENISA's human resources should be reviewed in their entirety as regards their adequacy in terms of ENISA's revised strategic objectives and in the course of the potential revision of its mandate, this document focuses on the most critical human resource needs stemming from new

legislative tasks that will come into force within the scope of the 2025-2027 programming period.

Within the CRA the initial estimates of resources were not adequate and aligned with the tasks assigned to ENISA. Thus, based on the functions that ENISA needs

to develop and maintain and its assessment of the related needs of its internal workforce, ENISA has estimated that its new CRA related needs total 9 FTEs over 2025-2027. They are summarised in the table below, as well as brought out under activities 5 and 8.

Table 1: Increase of critical workforce needs (FTE) to fulfil CRA tasks

| Basis for and description of functional needs | 2025 | 2026 | 2027 | TOTAL |
|--|----------|----------|----------|----------|
| Article 14-17 (vulnerabilities and incidents notification) incl: <ul style="list-style-type: none"> Reporting, management and analysis Developing and maintaining relevant high security systems and environment | 2 | 3 | - | 5 |
| Chapter V (market surveillance and enforcement) incl: <ul style="list-style-type: none"> Capacities to monitor, evaluate and analyse cybersecurity risk of products Cooperation with market surveillance authorities and economic operators | 1 | 1 | 2 | 4 |
| Total | 3 | 4 | 2 | 9 |

It should be noted that all of the CRA related tasks are sensitive and require the highest levels of confidentiality and integrity from jobholders. All jobholders potentially engaged for Article 11 tasks also need to hold a valid personal security clearance at the SECRET UE/EU SECRET level. Overall, the work related to CRA should preferably be carried out by TA/AD jobholders with the appropriate grade. Also, CRA functions and job-roles which can be synergised with other existing functions and tasks have been assessed separately and are not included in the FTE count shown in table 1 above.

In the Cyber Solidarity Act, the Commission estimates that new assignments need about 7 FTEs to be implemented and propose that these 7 FTEs

are reallocated from ENISA's existing resources by deprioritising other operational activities. Preliminary lessons learned from the implementation of the Cybersecurity Support Action were presented to the Management Board during its meeting in November 2023, highlighting that the actual FTE allocation for ENISA Support Action in 2023 was 20% to 30% higher than originally estimated (~15 FTEs) and adequate resourcing will need to be made available should the Commission request ENISA to operate and administer the Cybersecurity Reserve. Although the scope of activities have yet to be defined, based on the functions that ENISA needs to develop and maintain and its assessment of the related needs of its internal workforce, ENISA's estimated new CSOA-related needs total 16 FTEs over 2025-2027. They are summarised in the table below, as well as being brought out under activities 5 and 6.

Table 2: Increase of critical workforce needs (FTE) to fulfil CSOA tasks

| Basis for and description of functional needs | 2025 | 2026 | 2027 | TOTAL |
|--|----------|----------|----------|-----------|
| Article 12 (cybersecurity reserve) incl: <ul style="list-style-type: none"> Mapping and identifying the needs of member states and third countries Operation and administration of the reserve Maintaining 24/7 capabilities and cooperation | 2 | 4 | 8 | 14 |
| Article 18 (cybersecurity incident review mechanism) <ul style="list-style-type: none"> Developing and maintaining collaboration with relevant stakeholders Reviewing, analysing and reporting capabilities | 1 | 1 | - | 2 |
| Total | 3 | 5 | 8 | 16 |

It should be noted that, in the current Contribution Agreement covering Support Action, the Commission has already agreed that ENISA is to engage 10 CAs for a limited term (until 2026) in excess of the headcount forecast under the Staff Policy Plan. Some of these resources could be used to support ENISA's potential role under the Cybersecurity Reserve should the Commission ask ENISA to operate and administer it. Also, the Contribution Agreement model with additional CAs could also be applied to operationalising the Cybersecurity Reserve with an appropriate scope from 2026 onwards, as the 2024-2026 Contribution Agreement is phased out. Nevertheless, all the jobholders potentially engaged for the Cybersecurity Reserve need to hold a valid personal security clearance at the SECRET UE/ EU SECRET level. Moreover, though some of the jobholders for CSOA related functions can certainly be employed at the CA level, the Agency also needs two TA/AD level senior officers (in 2025) to scope the needs of member states and third countries and steer the work, as well as an additional two TA/AD level officers (to be engaged 2025-2026) to support tasks foreseen in Article 18 of the CSOA. Also, CSOA functions and job-roles which can be synergised with other existing functions and tasks have been assessed separately and are not included in the FTE count shown in Table 2 above.

In summary, by the end of 2024, if the legislative and political expectations for the Agency as already announced materialise, ENISA's budgetary and

human resource means will have been stretched to their absolute limits. Unless the FTE needs stemming from new tasks are addressed, the Agency in close cooperation with the MB will need to severely limit and deprioritise its existing operational activities in 2025 and 2026 within the programming period of 2025-2027, in order to reallocate FTEs to new emerging tasks. This will in turn limit ENISA's ability to deliver its overall mandate and objectives in their entirety.

2.5 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

Given the current constraints on 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 2025-2027 ENISA will thus further rigorously pursue all the five 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;

- Using internal and external synergies to gain additional resources and use current resources efficiently, in particular through external operational partnerships; and
- Maximising to the utmost extent possible the use of existing budgetary resources.

Within the programming period 2025-2027 ENISA will continue to develop and review its operational service packages, to ensure internal alignment and synergies between its structural entities. It will pursue targeted structural adjustments to consolidate capacity, streamline its structure and align its operational organisation with the activities of its work programme.

Beyond and on top of further elaborating and updating its service packages and internal structures, ENISA aims to build partnerships with Member States (including by exploring short- and medium-term secondments and exchanges of staff with relevant national authorities) and strengthen synergies with a number of EU institutions, agencies and bodies. This includes proposing joint operational objectives and KPIs in work programmes, thus further using external support and mobilising external resources for the benefit of ENISA's 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 following.

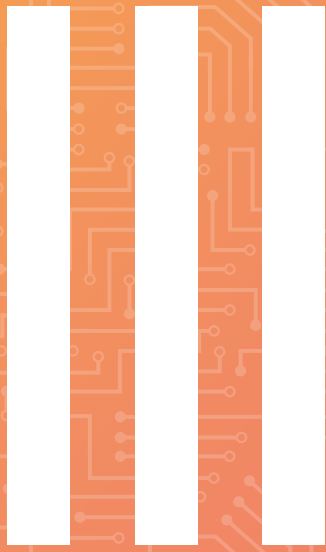
The Agency continues to implement its work programme by systematic use of its statutory bodies (NLO Network, ENISA Advisory Group), as well as other statutory groups in which ENISA is involved such as the Stakeholder Cybersecurity Certification Group (SCCG as set out in CSA Article 22), the NISD Cooperation Group and its work-streams, the ECATS Article 18 group eIDAS regulation, and other expert groups created under EU law and its own ad hoc groups of experts, where appropriate to avoid duplications of effort, 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. In this way the Agency will fulfil its obligation, as outlined in Article 3(3) of the CSA, to avoid duplication of the activities of Member States and take into consideration the existing expertise of

Member States. 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 in consultation with relevant external experts.

ENISA also intends to analyse and assess the 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 the MB 2020/09 thresholds and the requirements of the Corporate Strategy are met. Digitalisation of services, self-service functionalities and service optimisation will also be 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.

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, threat-sharing frameworks, allowing for the exchange of data in real-time and collaborative incident responses. ENISA will also prioritise the creation of interoperable tools and interfaces, such as CRA, DORA, IR and the 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 optimising operational costs.





SECTION III

WORK PROGRAMME FOR 2025

This is the main body of the Work Programme. It describes what the agency aims to deliver through its operational and corporate activities during the year 2025 towards achieving its strategy and expected results. A total of eight operational activities and three corporate activities have been identified to support the implementation of ENISA's mandate in 2025.

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.

Service catalogue

In 2022 the Agency introduced the concept of a service catalogue to allow management to focus efforts and resources in a highly structured and more efficient manner to obtain specific objectives. ENISA's service catalogues are organised into individual service packages. A service package is a collection of cybersecurity products and services that span a number of activities and contribute to the objectives of a discrete service package. A service package is a

means of centralising all services that are important to the stakeholders that use it. The Agency will continue to review and prioritise 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:

- NIS directive (NIS) led by Activity 2 - cybersecurity and resilience of critical sectors;
- Training and exercises (TRES) led by Activity 3 - capacity building;
- Situational Awareness (SITAW) led by Activity 5 - providing effective operational cooperation through situation awareness;
- Certification (CERTI) led by Activity 7 - development and maintenance of EU cybersecurity certification
- Cybersecurity index (INDEX) led by Activity 1 - support for policy monitoring and development.

Stakeholders and engagement level

The management of stakeholders is instrumental to the proper functioning and implementation of ENISA's work programme. On 29 March 2022 the Management Team adopted ENISA's Stakeholders Strategy. This Strategy lays down the main principles and our approach towards the engagement of stakeholders at the Agency-wide level. The implementation of the Stakeholders Strategy is linked with the implementation of the Single Programming Document (SPD) through the activities.

Each activity includes a list of stakeholders and the expected or planned engagement level for each stakeholder. The engagement level refers to the degree of the stakeholder's interest and influence in the activity for stakeholders classified as either partner or involve / engage. Stakeholders classified as 'Partner' refers to stakeholders with high influence and high interest, usually business owners and others with significant decision-making authority. They are typically easy to identify and to engage with actively. Stakeholders classified as 'involve / engage' have high influence but low interest. These are typically stakeholders with a significant decision-making authority but lacking the availability or the interest to be actively engaged.

KPIs / metrics

In 2020 the Agency developed and introduced a new set of key performance indicators and related metrics for measuring the performance of the activities. These metrics are described in the Single Programming Document for each activity and are made up of both quantitative and qualitative metrics. Quantitative metrics are those that measure a specific number through a certain formula, whereas qualitative metrics are those that are more of a subjective opinion based on the information received; however even these are quantified in order to be interpreted and measured. The work programme for 2025 includes indicators for measuring the new strategic objectives from the updated ENISA strategy, indicators and targets for measuring the objectives of activities and indicators at the output level to measure the performance of the outputs.

3.1. OPERATIONAL ACTIVITIES

ACTIVITY 1: Support for policy monitoring and development



Overview of activity



This activity seeks to bolster policy initiatives on novel or emerging areas of technology by providing technical, fact-driven and tailor-made policy analyses and recommendations. ENISA will support EU institutions and MSs on new policy initiatives⁷ through evidence-based inputs into the policy development process. ENISA, in coordination with the Union's institutions and MSs will also conduct policy monitoring to support them in identifying potential areas for policy development based on technological, societal and economic trends, identify gaps, overlaps and synergies among policy initiatives under development, as well as develop monitoring capabilities and tools to regularly and consistently be able to provide advice on the effectiveness of existing Union policy and law in accordance with the EU's institutional competencies in the area via the "Implementation Check" model, together with Activities 2 and 8 in particular.

This activity delivers on ENISA's strategic objectives 'Cybersecurity as an integral part of EU policies' and 'Efficient and effective cybersecurity knowledge management for Europe'. In particular, work under this Activity shall provide strategic long-term analysis, guidance and advice on current policy challenges and opportunities. In terms of knowledge management, ENISA will work towards consolidating data, information and indicators concerning the status of cybersecurity across MSs, including through input from National Cybersecurity Strategies and the EU average. Efforts in developing and maintaining the EU cybersecurity index and developing, reviewing and following up on the biennial report on the state of cybersecurity in the Union under Article 18 of NIS2 will continue.

This cross cutting activity leads ENISA's efforts towards delivering the cybersecurity index (INDEX) and policy analyses to better map the needs of MSs and their 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. Value can also be added by using, among other sources, information from foresight, incident reporting and vulnerabilities in collaboration with Activities 4, 5 and 8.

Activity 1 leads the Index service package and support the NIS, TREX and CERTI service packages.

The legal basis for this activity is Articles 5 and 9 of the CSA and Article 18 of the NIS2.

Link to strategic objective (ENISA strategy)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective and consistent implementation of EU policies for cybersecurity
- Foresight on emerging and future cybersecurity opportunities and challenges

Indicator for strategic objectives



- Uptake of recommendations stemming from NIS2 Article 18 report.
- Number of identified future and emerging areas reflected in the policy initiatives and interventions

7 - Initiatives on NIS2 sectors such as space, health, AI, data spaces, digital resilience and response to current and future crises.

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 | Assessment of ENISA advice on EU policy (stakeholder survey, desktop research) | 75% stakeholder satisfaction from ENISA's advice (among EU policy makers) By end of 2025 policy analysis framework is endorsed |
| 1.B By Q3 2026 and in collaboration with Activity 2, ensure that two-thirds of policy observations within the first State of Cybersecurity in the Union report have been realised | Art 18 NIS2 | 2026 | Assessment of MSs use of the Art 18 report (stakeholder survey, desktop research) | Two-thirds of MSs are using Art 18 report as input for their cybersecurity strategies All MSs use ENISA support and tools for the work on their NIS Strategies |

ACTIVITY 1 OUTPUTS

| Description | Expected Results Of Output | Validation | Output Indicator | Frequency (Data Source) | Latest Results | Target 2025 |
|---|---|---|---|--|----------------|---|
| 1.1 Assist MSs to implement, assess and review National Cybersecurity Strategies and policies. Enhance a culture of trust and cooperation among MSs, also through peer reviews and by developing a code of conduct. | Stakeholders receive technical advice with the evidence needed for policy-making activities and the definition of implementation measures | Union Institutions (COM, EP, Council) NIS CG, including relevant work streams NLOs, including relevant sub-groups | Develop and pilot peer review framework, including code of conduct | | n/a | By end of 2025 both endorsed |
| 1.2. Collect and present relevant evidence by maintaining and developing EU cybersecurity index and State of Cybersecurity in the Union report. | | | Assessment of ENISA advice on EU policy | Biennial Survey, annual dialogues, and annual desktop research | 93% | >90% stakeholder satisfaction |
| 1.3. In coordination with Activities 2, 4 and 8, develop and maintain analyses on time-sensitive observations offering technical advice for policy development. | | | Assessment of timeliness of advice provided during policy development | | n/a | >70% stakeholder satisfaction with timeliness |

Stakeholders and Engagement Levels



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

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

ACTIVITY 1 RESOURCE FORECASTS

| | Budget | FTEs |
|--------------------------|----------------------------------|----------------------|
| Total activity resources | Budget: EUR 353 037 ⁸ | FTE: 10 ⁹ |

8 - of which €59 000 centralised to missions and the budget for large-scale events.

9 - Target FTEs.

ACTIVITY 2: Cybersecurity and resilience of critical sectors¹⁰



Overview of activity



This activity supports Member States and EU Institutions with the implementation of the NIS2. The objectives of this activity are the rapid and harmonised implementation of NIS2, to increase the maturity of NIS sectors and to ensure NIS2-aligned implementation of sectorial resilience policies, such as DORA for resilience in the finance sector and the Network code for the cybersecurity of cross-border electricity flows. This activity includes an annual check on the implementation of policy, which relies on direct information from companies in the NIS sectors.

Under this activity ENISA provides support to the workstreams of the NIS Cooperation Group and the implementation of the NIS CG work programme. In this period the focus is on supporting the transposition of NIS2, the NIS2 implementing acts and the implementation of new tasks under NIS2 such as the EU registry for digital infrastructure entities. ENISA's goals here are to develop effective NIS2 frameworks for risk management, security measures and incident reporting, which can also be used beyond the NIS2, for example, under DORA, creating a single framework or approach for risk management, security measures and incident reporting in the EU.

Secondly, ENISA supports MSs and the Commission by addressing specific threats and risk scenarios for the Union, such as by supporting the 5G toolbox process and other Union coordinated risk evaluations such as Nevers, the Council Cyber Posture¹¹, the Union's coordinated assessments of supply chain risks (under the NIS2), and the Union's coordinated preparedness tests (aka resilience stress tests, under the Cyber Solidarity Act). After supporting the MSs and Commission with developing the necessary frameworks, methodologies and scenarios, in 2026 ENISA will also support the MSs and the Commission with carrying out a Union coordinated preparedness test of resilience and a Union coordinated assessment of supply chain risks. Alignment with Activity 8 will be a priority. It would also support potential work conducted by the EU and Member States on the security and resilience of submarine cables, under existing (NIS2, CERG) or future cooperation bodies.

Thirdly, the activity also addresses sector-specific issues, working with sectorial stakeholders in the NIS sectors, providing targeted service bundles ('sustain', 'build', 'involve', 'prepare') depending on the needs of each sector. For each sector, ENISA will support a working group of relevant national authorities, but also engage with the industry either by supporting EU ISACs or by organising industry events to facilitate public-private dialogue on cybersecurity. Besides supporting the four highly critical sectors, namely telecoms, energy-electricity, finance and the Internet's infrastructure (aka core Internet), ENISA also supports sectors with low to medium levels of maturity, such as health, rail and public administration. This activity provides important sectorial input to other SPD activities, such as cyber exercises and training (Activity 3) and situational awareness (Activity 5).

Finally, there is a dedicated output for checking the implementation of these policies, by directly surveying companies in the NIS sectors to ensure that the NIS2 sectorial rules and other *lex specialis* do not only remain on paper but actually improve the level of security in 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).

This activity leads the NIS service package and contributes to the INDEX, TREX and SITAW service packages. The legal basis for this activity is Articles 5 and 6 (1)(b) of the CSA.

¹⁰ - The term critical sectors is used in this context to cover ALL sectors within the scope of NIS2.

¹¹ - [st09364-en22.pdf \(europa.eu\)](#).

Link to strategic objective (ENISA strategy)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective and consistent implementation of EU policies for cybersecurity

Indicator for strategic objectives



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 best practices and international standards. | CSA Article 5, Article 6 and NIS2 | Development of frameworks 2025 | Framework's development | 2 frameworks developed |
| | | Frameworks pilot by 2026 | Implementation of pilot programme (number of sectors piloting the frameworks, feedback scores on the usability) | 20 MSs to adopt/use/endorse the frameworks |
| | | Full implementation by 2027 | | >75% usability score |
| 2.B Provide continuous comprehensive support to MS for implementing Union's regulatory requirements on cybersecurity and raising resilience across critical sectors. | CSA Articles 5 and 6 and NIS2 | 2027 | Requests received by the NIS CG or MSs 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. | CSA Article 5 [possibly NCCS] | 2027 | Assessment of maturity based on updated NIS360 methodology | >2 sectors improving maturity |

ACTIVITY 2 OUTPUTS

| Description | Expected Results Of Output | Validation | Output Indicator | Frequency (Data Source) | Latest Results | Target 2025 |
|---|---|---|--|-------------------------|-----------------------|---|
| 2.1 Support Member States in their implementation of the NIS2 | NIS2 frameworks for risk management, security measures and incident reporting achieving harmonisation | DG CNECT, NIS CG | Framework usage | Annual (Internal count) | n/a | 10 MSs to adopt, use or endorse the frameworks |
| | | | EU register for digital entities is used by all MSS | Annual (Report) | n/a | 20 MSs to use the registry |
| | | | Alignment between DORA and NISD2 | Satisfaction survey | n/a | >80% |
| 2.2 Support Member States with EU toolboxes, EU coordinated risk evaluations, and EU coordinated preparedness tests | Support Union-wide risk evaluations and risk scenarios and their follow-up (5G, Nevers) Coordinated risk assessment of critical supply chains | DG CNECT, NIS CG | Stakeholder satisfaction | Biennial (Survey) | 94% | >90% |
| | | | Risk assessment framework for critical supply chains | Annual (Internal count) | n/a | One coordinated risk assessment for one domain or sector |
| | | | Number of sectorial situational awareness reports | Annual (Internal count) | 6 | 12 |
| 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 | Stakeholder satisfaction | Biennial (Survey) | 94% | >90% |
| | | | Number of critical sectors increasing maturity (from build to sustain or involve - NIS360) | Annual (Internal count) | 3 | 5 |
| | | | Number and frequency of services or workflows delivered to NIS sectors according to the maturity of the sector | Annual (Internal count) | 21 | 24 |
| 2.4 Perform an annual check on policy implementation | MSs 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 | Stakeholder satisfaction | Biennial (Survey) | 94% | >90% |
| | | | Number of critical or essential sectors covered by NIS Investments | Annual (Internal count) | 10 subsectors covered | 12 subsectors covered |
| | | | Number of critical sectors assessed by NIS360 and cyber posture briefs | Annual (Internal count) | 10 | 12 |
| | | | Implementation tracker | Annual (Internal count) | n/a | Five requests stemming from the implementation of NIS2 in MSS |

Stakeholders and engagement levels



Partners: CNECT, NIS CG, National competent authorities, Sectorial DGs, Sectorial EU agencies, National competent authorities, Sectorial ISACs

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

ACTIVITY 2 RESOURCE FORECASTS

| | Budget | FTEs |
|---------------------------------|---|-----------------------------|
| Total activity resources | Budget: EUR 468 024¹² | FTE¹³: 12 |

12 - of which €137,000 centralised to missions and the budget for large-scale events .

13 - 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, enhancing their skills and behavioural change with regards to cyber hygiene, and increasing their preparedness.

Following an integrated approach and on the basis of the European Cyber Security Skills Framework (ECSF), capacity building is achieved by developing and conducting large-scale and/or sectorial exercises and training, designing and executing awareness raising programmes on cybersecurity risks and good practices, and by facilitating gamified Capture the Flag (CTF) competitions at national and EU level.

Secondly, this activity contributes to Agency's reporting duties on the current State of Cybersecurity in the Union (NIS2 Article 18) by providing insights on the cybersecurity capabilities of private and public stakeholders and on the cybersecurity awareness and hygiene of citizens. In that context, the activity will contribute to the INDEX (activity 1) by developing indicators and collecting relevant data to measure the progress towards closing the cyber talent gap, in line with the EC Communication on the Cybersecurity Skills Academy.

Thirdly, this activity will maintain and regularly update the European Cybersecurity Skills Framework (ECSF) by engaging with the relevant communities and stakeholders (in cooperation with activities 1, 2, and 4). On the basis of ECSF, it will develop, deploy, promote and maintain tools, frameworks and material that enable stakeholders, in particular NIS sectors, to independently execute their own cybersecurity capacity building programmes using ENISA's services through a pricing model.

Furthermore, the Agency, in collaboration with relevant EUIBAs and operational communities in Members States, will conduct a limited number of targeted exercises and training sessions focusing on empowering the trainers with the intention to enhance the resilience, maturity and preparedness of NIS sectors (in cooperation with activities 2, 4 and 6). In addition, the Agency will step up its efforts to support the development of new cybersecurity professionals through gamified cybersecurity training sessions (such as Team Europe training) and educational programmes in cooperation with National Competence Centres (NCCs) and other relevant stakeholders.

The plan is to gradually transfer knowledge and empower MSs, in particular NCCs, national operational communities and the ECCC, and to organise and financially support CTF training sessions at national and EU level with ENISA maintaining a facilitating role.

The previous output 9.2 (Promote cybersecurity topics and good practices) from work programme 2024 has been suppressed in 2025 in order for the resources to be re-allocated to higher priority tasks.

This activity leads the TRES service package and supports the INDEX, SITAW and NIS service packages.

The legal basis for this activity is Articles 6, 7(5) and 10 of the CSA, Art 18(1) of NIS2, Article 10 of CRA and Article 10 of REU.

Link to strategic objectives (ENISA STRATEGY)



Empowered communities in an involved and engaged cyber ecosystem
 Strong cybersecurity capacity within the EU

Indicator for strategic objectives










Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, training sessions)
 Percentage of MSs that use the 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 MSs endorsing the updated ECSF framework | 23 |
| | | | Stakeholder satisfaction rate | 95% |
| 3.B Between 2025-2027, enhance the cybersecurity skills and capabilities of at least 100 000 professionals in the EU. | CSA Articles 4, 6, 7(5) and 10 CRA Article 10 REU Article 10 | 2027 | Number of professionals whose skills have been directly or indirectly improved by capacity building activities | 100 000 professionals |
| | | | Satisfaction survey of stakeholders on ENISA's capacity building activities | 70% |
| 3.C Between 2025-2027, ensure that ENISA has put in place frameworks to support the development of at least 100 000 additional cybersecurity professionals in EU. | CSA Articles 4, 6, 7(5) and 10 CRA Article 10 REU Article 10 | 2027 | Stakeholder satisfaction survey on new frameworks put in place | 75% |

ACTIVITY 3 OUTPUTS

|  Description |  Expected Results Of Output |  Validation |  Output Indicator |  Frequency (Data Source) |  Latest Results |  Target 2025 |
|---|--|--|--|--|---|--|
| 3.1 Support the adoption and uptake of EU's Cybersecurity Skills Framework | <p>Review and update ECSF in line with the CyberSkills Academy Communication</p> <p>Measure and report on the skills gap, including developing indicators to be used for INDEX and Article 18a</p> <p>Promote the adoption of ECSF in MSs, in training organisations and academia and ensure its regular update.</p> | <p>AHWG on Cybersecurity Skills,</p> <p>ECCC WG 5 on Skills</p> | <p>Stakeholder satisfaction</p> <p>Number of MSs endorsing ECSF</p> <p>Number of training organisations endorsing ECSF in their training programmes</p> | <p>Biennial (Survey)</p> <p>Annual</p> <p>Annual</p> | <p>91%</p> <p>n/a</p> <p>n/a</p> | <p>95%</p> <p>10</p> <p>15</p> |
| 3.2 Organise targeted exercises and support stakeholders to plan, execute their own exercises | <p>Organise a set of limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders</p> <p>Develop, deploy and promote exercises tools and frameworks that enable stakeholders, in particular in NIS2 sectors, to independently execute their own cybersecurity exercises</p> <p>Develop a community of 'train the planners' that leverages the tools, platforms and frameworks developed by ENISA</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 applicable)</p> <p>EU ISACs (as applicable)</p> <p>NLO subgroup of Cyber Europe planners (as applicable)</p> <p>CERT EU</p> | <p>Number of people impacted directly and/or indirectly by exercises organised by ENISA</p> <p>Number of sectorial authorities, including EUIBAS, using ENISAs exercise solutions and frameworks</p> <p>Number of MSs participating in the community of 'train the planners'</p> | <p>Annual (Report)</p> <p>Annual</p> <p>Annual</p> | <p>n/a</p> <p>n/a</p> <p>n/a</p> | <p>>7.000</p> <p>5</p> <p>10</p> |
| 3.3 Organise targeted trainings and awareness programmes and support stakeholders to plan, execute their own trainings / programs | <p>Develop, deploy and promote trainings and awareness raising tools, frameworks and content that enable stakeholders, in particular NIS2 sectors, to independently execute their own training or awareness raising programmes</p> <p>Develop a community of 'train the trainers' that leverages the tools, platforms and frameworks developed by ENISA</p> <p>Harmonise training activities sponsored by Cyber Security Support Action</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>Number of participants in ENISA online based training sessions</p> | <p>Annual (Report)</p> | <p>3800</p> | <p>4000 (depending on Support Action contribution)</p> |

| | | | | | | |
|--|--|---|--|-----------------|-------|--------|
| | | | Number of participants in ENISA's train-the-trainer and train-the-planner events | Annual (Report) | 220 | > 250 |
| | | | Number of professionals impacted by ENISA's awareness raising in a box | Annual (Report) | n/a | 10 000 |
| 3.4 Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC) | Deliver the ECSC final Form and train an elite team representing Europe at the ICC Create challenges and a platform (OpenECSC) with access to potentially new cyber security professionals | ECSC Steering Committee NLO Subgroup | Number of countries represented in Team Europe cohort | Annual (Report) | 24 | 26 |
| | | | Number of users participating in OpenECSC and national CTFs, who are potentially new cybersecurity professionals | Annual (Report) | 3 000 | 20 000 |

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 stakeholders, SOCs including National and Cross-border SOCs, 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.

ACTIVITY 3 RESOURCE FORECASTS

| | Budget | FTEs |
|-----------------------------------|---|-----------------------------------|
| Total activity resources | Budget: EUR 796 409¹⁴ | FTE¹⁵: 12 |
| Other supplementary contributions | EUR 120.000 from Service Level Agreement with EU-LISA to provide support on exercises | Other supplementary contributions |

14 - of which €105 000 centralised to missions and the budget for large-scale events.

15 - Target FTEs.

ACTIVITY 4: Enabling operational cooperation



Overview of activity

This activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities. The main goal of the activity is to provide support and assistance in order to ensure the efficient functioning of EU operational networks and cyber crisis management mechanisms, including the revision of the Blueprint. Under our NIS2 mandate, activity 4 provides expertise, organisational support, tools and infrastructure for both the technical layer (EU CSIRTs Network) and the operational layer (EU CyCLONE - Cyber Crises Liaison Organisation Network) of Union operational cooperation networks.

Secondly, the activity aims to enhance interaction and trust between these two layers, the NIS Cooperation Group, and the HWPCI. ENISA supports operational communities by developing and maintaining secure and highly available networks, IT platforms, and communication channels. This includes developing the EU Vulnerability Database and launching the CRA Single Reporting Platform. The activity is also internally responsible for 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.

Thirdly, this activity manages the ENISA Cyber Partnership Programme and information exchange with security vendors and non-EU cybersecurity entities. ENISA will contribute to the next steps in enhancing the EU's cyber crisis management framework following the NIS2 and the 2022 Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, complementing the EU's coordinated response to large-scale cybersecurity incidents and crises. In addition, this activity supports the ENISA Cybersecurity Support Action. Finally, this activity will also provide for the delivery of the tasks mandated by the Cyber Solidarity Act within the Cybersecurity Incident Review Mechanism (at the request of the Commission or national authorities - the EU-CyCLONE or the CSIRTs network). ENISA will be responsible for the review of specific significant or large-scale cybersecurity incidents and will be required to deliver a report that includes lessons learned and, where appropriate, recommendations to improve the Union's cyber response.

Fourthly, the activity also maintains IT systems and platforms for all ENISA's operational activities and develops a comprehensive knowledge and stakeholder management system. This 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 and best practices, provide advice and issue guidance.

Finally, this activity will also seek to contribute to the Union's efforts to cooperate with third countries and international organisations on cybersecurity, including revising ENISA's international strategy and stakeholder strategy.

This activity supports SITAW, INDEX and NIS service packages.

The legal basis for this activity is Articles 9, 10, 11, 12, 14, 15, 16 and 17 of NIS2, Articles 6, 7, 12 and 16 of the CSA and Article 11 of the CSOA (final text pending).

Link to strategic objectives (ENISA STRATEGY)



- 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

Indicator for strategic objectives



- Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks
- EU Vulnerability Database is operationalised by ENISA resulting in a high satisfaction rate (by MSs and stakeholders) with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threat

ACTIVITY 4 OBJECTIVES

| Description | CSA Article And Other EU Policy Priorities | Timeframe Of Objective | Indicator | Target |
|---|---|------------------------|---|--|
| 4.A 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) | Articles 7, 10, 15 and 16 NIS2 Articles 6 and 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 or 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 |
| 4.B 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. | Established framework for knowledge management and stakeholder management |
| 4.C Develop and maintain relevant operational IT systems and platforms to support all operational communities and enhance synergies. | Articles 7, 10, 12, 15 and 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 designed (2025) and implemented (2026). |

ACTIVITY 4 OUTPUTS



| Description | Expected Results Of Output | Validation | Output Indicator | Frequency (Data Source) | Latest Results | Target 2025 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% | >90% |
| | | | Continuous use and durability of platforms (including prior to and during large-scale cyber incidents) | Annual (report) | n/a | >60% use of platforms |
| | | | Number of joint sessions established. | Annual (report) | 1 joint session per year. | 2 joint sessions per year with operational outcomes. |
| 4.2 Maintain, develop and promote the ENISA Cyber Partnership programme to enable the exchange of information to support the Agency's understanding of threats, vulnerabilities, incidents and cyber security events | Operationalisation of the Cyber Partnership Programme | CSIRT Network, EU CyCLONe, EUIBAs, HWPCI, MB | Stakeholder satisfaction | Biennial (survey) | 84% | >90% |
| | | | Number of new and total partners in the ENISA partnership programme | Annual (report) | 4 | 6 |
| | | | Percentage of RFI answered by members of partnership programme | Annual (report) | n/a | 65% |
| 4.3 Implement ENISA's international strategy and outreach | EU values recognised by international stakeholders International cooperation supports ENISA objectives | MT, EEAS, COM (and MB as required) | Stakeholder satisfaction | Biennial (survey) | 91% | 1% increase (from previous year – decrease in duplication) |
| | | | Staff satisfaction with international coordination | Annual (survey) | n/a | >80% |
| 4.4 Develop comprehensive CVD platforms by operationalising the EU Vulnerability Database and designing the CRA Single Reporting Platform. | EU VD is deployed. CRA Single Reporting Platform is being developed | CSIRTs Network. | Stakeholder satisfaction | Biennial (survey) | N/A | 66% by 2027 |
| | | | | | | |

16 - Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023

| | | | | | | |
|--|---|---|---|-------------------|-----|---|
| 4.5. Develop and maintain IT systems and platforms for operational activities. | Consolidation of operational IT with view to supporting ENISA operations. | CSIRTs Network and CyCLONe members, HWPCI and NIS Cooperation Group and Business owners for ENISA's Operational IT systems. | Stakeholder satisfaction | Biennial (survey) | 89% | >90% |
| | | | IT architecture for external operational IT services | Biennial update | n/a | Completed by end of 2025. |
| | | | ENISA operational IT | Annual (report) | n/a | All operational IT systems are consolidated under one IT operational manager by 2025. One third of current systems are updated every year to reach 100% in 2027. |
| | | | EU Vulnerability Database | Annual (report) | n/a | EU Vulnerability Database is produced and users are trained. |
| | | | CRA Single Reporting Platform | Annual (report) | n/a | Technical specifications of the CRA Single Reporting Platform are available and the service provider is contracted to start implementation. |
| 4.6 Development of stakeholder and knowledge management systems and frameworks | | | Stakeholder satisfaction with knowledge management and stakeholder management system. | Biennial (survey) | n/a | >60% by 2026 |

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 FORECAST

| | Budget | FTEs |
|---------------------------------|---|-----------------------------|
| Total activity resources | Budget: EUR 1 652 091¹⁷ | FTE¹⁸: 15 |

17 - of which €115 000 centralised to missions and the budget for large-scale events .

18 - Target FTEs.

ACTIVITY 5: Provide effective operational cooperation through situational awareness



Overview of activity



This activity contributes to cooperative preparedness and responses at the level of the Union and Member States through data driven analyses of threats and risks, operational and strategic recommendations based on the collection of incidents, information on vulnerabilities and threats in order to contribute to the Union's common situational awareness.

ENISA delivers on this activity by collecting and analysing security events, cyber incidents, vulnerability and threats based on its own monitoring, shared by external stakeholders due to legal obligations¹⁹ or voluntary shared. The Agency aggregates and analyses reports, ensuring information flow between the CSIRTs Network, EU-CyCLONE, and other technical, operational and political decision-makers at the Union level to increase situational awareness with the services of other EU entities such as relevant Commission services and in particular DG CNECT, CERT-EU, Europol/EC3, and EEAS including EU INTCEN. This activity actively benefits from ENISA's Cyber Partnership Programme managed under Activity 4 and the Agency's international cooperation frameworks.

Secondly, the activity includes the preparation of the regular in-depth EU Cybersecurity Technical Situation Report in accordance with CSA Article 7(6), also known as the EU Joint Cyber Assessment Report (EU-JCAR), regular weekly OSINT reports, Joint Rapid 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 for Member States and Union institutions, bodies, offices and agencies. Under this activity, a semi-annual report in accordance with NIS 2 Article 23(9)²⁰ is prepared and the work related to the Cyber Solidarity Act – Incident Review Mechanism (Article 18*) - is undertaken.

Thirdly, this activity also supports Member States with respect to operational cooperation within the CSIRTs Network and EU-CyCLONE by providing, at their requests, advice on a specific cyber threat, assisting in the assessment of incidents and vulnerabilities, facilitating the technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities using the EU Vulnerability Database 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 Diplomatic Toolbox.

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

Finally, under this activity the work that underpins the establishment of the Single Reporting Platform as set up under the Cyber Resilience Act is carried out. In doing so, the Agency takes into account the frameworks for **incident reports** implemented under Article 23 of NIS2 and other relevant EU legislation to ensure alignment and to future proof the architecture for the simplification of reporting at the EU level.

This activity includes the continuous development and maintenance of a 24/7 monitoring and incident support capability in combination with activity 6.

The budget for this activity is partly financed through a contribution agreement between ENISA and the Commission to support the work on the CRA and CSOA (final text pending) as well a contribution to the Commission Situation and Analysis Centre.

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

The legal basis for this activity is Articles 5(6), 7(4)(6)(7) and 9 of the CSA, Article 23(9) of NIS2, Article 18 of the CSOA and Articles 14-17 of the CRA.

19 - NIS2, CRA and Regulation 2023/2841

20 - In 2025 this activity will fulfil the tasks under CSA Article 5(6) a, b and c. These reports will be superseded as provisions in NIS2 Art 23(9) apply.

Link to strategic objectives (ENISA STRATEGY)



- 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

Indicator for strategic objectives






- EU Vulnerability Database is operationalised by ENISA and a high satisfaction rate (by MSs and stakeholders) with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats
- Reporting platform under the 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 |
|--|--|------------------------|---|---|
| 5.A By end 2027 build a common situational awareness between Member States based on accurate shared data and underpinned by validated joint analysis | Article 7 of CSA | 2025 - 2027 | Content of JCAR is contributed and validated by Member States | Produce at least one comprehensive joint analysis report every quarter, contributed and validated by at least 75% of Member States (EU-JCAR). |
| | Article 23(9) of NIS2 | | ENISA Data repository is open to and includes also information directly provided by Member States | Data repository is accessible by MSs Percentage of information in the data repository validated or provided by MSs is above 75% and 100% or significant event impacting EU MSs |
| | Article 18 of CSOA | | Establish and test processes and procedures for the Incident Review Mechanism under Article 18 of CSOA | Process for IRM is established and endorsed by MSs |
| 5.B Provide regular and general as well as specific threat landscapes and threat analyses, based on observed data-driven trends in incidents and vulnerabilities | Article 9 of CSA | 2025 - 2027 | Produce ENISA Threat Landscapes | Maintain the regular publishing schedule for general threat landscape reports (yearly) and specific threat analysis and sectorial reports (e.g. bi-monthly). |
| | Article 7 of CSA | | JCAR includes threat analysis based on incidents and vulnerabilities available within ENISA data repositories (EUVDB, CIRAS, CRA SRP) | Incident analysis is included in JCAR as of Q3 2025 EUVDB vulnerability analysis is included by Q2 2025 CRA SRP AEV and incidents analysis are included by Q4 2026 |
| | Article 23(9) of NIS2 | | Ability of ENISA to produce accurate threat analyses based on incidents, vulnerabilities and threat information based on the Agency's own monitoring, shared by external stakeholders due to legal obligations ²¹ , or voluntarily shared, | 80% of Member States score quality of threat analyses provided by ENISA above 4 (on scale 1-5) |
| | Article 18 of CSOA | | | 80% of Member States score ability of ENISA to use available information to produce threat analyses and recommendations above 4 (on scale 1-5) |
| | Articles 14-17 CRA | | CRA SRP is established and operational | CRA SRP is used to carry on tasks under CRA by end of 2026 |

21 - NIS2, CRA and Regulation 2023/2841.

ACTIVITY 5 OUTPUTS

|  |  |  |  |  |  |  |
|--|--|---|--|--|---|---|
| Description | Expected Results Of Output | Validation | Output Indicator | Frequency (Data Source) | Latest Results | Target 2025 |
| 5.1 Collect, organise and consolidate information (including from the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, operational and technical levels ²² | Establishment of a Threat Information Management Platform. | CSIRT Network, EU CyCLONE, Union entities, National Authorities within MSs subscribed to the products | Stakeholder satisfaction | Biennial (survey) | 84% | >90% |
| | Production of briefings, reports, and summaries of incidents, threats, and vulnerabilities Increased understanding and timely access to information regarding latest threats, incidents and vulnerabilities | | Timeliness and Accuracy of reports | Annual (survey) | n/a | >85% |
| 5.2 Provide analysis and risk assessment jointly with other operational partners including EUIBAs, Member States, industry partners, and non-EU partners | Union joint assessment and reports, sectorial analysis, threats and risk analysis. ²³ | CSIRT Network, EU CyCLONE, Union entities, HWPCI, Management Board | Stakeholder satisfaction | Biennial (survey) | 84% | >90% |
| | Recipients receive accurate and timely assessment of threat actors and associated risks to the EU Internal Market | | Number of contributing MSs to EU JCAR | Annual (report) | n/a | >40% |
| 5.3 Collect and analyse information to report on cyber threat landscapes | Mapping threats, Generating recommendations for stakeholders to take up | NLO, AG and Cybersecurity Threat Landscape AhWG | Stakeholder satisfaction | Biennial (survey) | 91.5% | >5% compared to 2023 |
| | | CSIRTs Network | Number of downloads of ETL | Annual (report) | | >5% increase year on year |
| 5.4. Analyse and report on incidents as required by Article 5(6) of CSA as well as other sectorial legislation (e.g. DORA, eIDAS Art 10, etc.) | Analysing incidents Generating recommendations for stakeholders to take up | WS3 of the NISD CG, ECASEC and ECATS groups | Stakeholder satisfaction | Biennial (survey) | 91.5% | >5% compared to 2023 |
| 5.5 Developing the CRA Single Reporting Platform and operationalise EU vulnerability database | CRA SRP platform work is scoped and implementation is initiated Operational and business processes are defined together with primary stakeholder | CSIRT Network | Operational processes expected for 2025 are defined Implementation work is started. | Survey | n/a | 80% of the stakeholders agree on the established process and score them >4 |

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

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

Stakeholders and engagement levels



Partners: EU Member States (including CSIRTs Network members and EU-CyCLONe), EU Institutions, bodies and agencies, other technical and operational blueprint actors, partnership programme for 5.3 (with trusted vendors, suppliers and partners), CTL AHWG

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

ACTIVITY 5 RESOURCE FORECAST

| | Budget | FTEs |
|---|--|--------------------------------------|
| Total activity resources from direct annual budget | Budget: EUR 1 566 118 ²⁴ | FTE ²⁵ : 13 ²⁶ |
| Other supplementary contributions | Budget: TBD (outputs 5.1 and 5.2) ²⁷ and TBD ²⁸ for CRA Platform | 2 ²⁹ |
| Other supplementary contributions on-going | Budget: (outputs 5.1 and outputs 5.2) forecast EUR 223 000 from existing contribution agreement signed in 2023 | 2 ³⁰ |

24 - Of which €90 000 centralised to missions and the budget for large-scale events.

25 - Target FTEs, Current Staff 12 plus foreseen 2 FTE for CRA SRP and 1 FTE for Incident Review Mechanism.

26 - Including 2 FTE – Contract Agents are hired through the Contribution Agreement signed with Commission in 2023 under Cybersecurity Support Action and Situation Centre.

27 - Allocation depending on the final text of the contribution agreement to be signed with Commission in 2024. Allocation is expected to be 15 000 000 to support cybersecurity actions, situation centre and implementation of CRA single reporting platform. Please refer to annex XI for further details regarding contribution agreements, final text pending. The amount indicated refers to years 2025 to 2027.

28 - Allocation depends on the final text of the Contribution Agreements to be signed with Commission in 2024.

29 - FTE allocation depends on the final text of the Contribution Agreement to be signed with Commission in 2024.

30 - 2 FTEs – Contract Agents are hired through the Contribution Agreement signed with Commission in 2023 under Cybersecurity Support Action and Situation Centre.

ACTIVITY 6: Provide services for operational assistance and support



Overview of activity



The activity contributes to the further development of capabilities to prepare and respond at the level of the Union and Member States for large-scale cross-border incidents or crises related to cybersecurity through the implementation and delivery of ex-ante and ex-post services. It implements the Cybersecurity Support Action through which the Agency provides services such as penetration testing, threat hunting, risk monitoring and assessment, customised exercises and training, and supports the Member States in responding to incidents.

The Agency will leverage the lessons learned and the mechanisms that were put in place during the first year of the Cybersecurity Support Action in 2023. This will refocus the service catalogue as the processes and methodologies will be further adapted to better suit the needs of the Member States, allowing for more flexibility and scalability.

The types and level of services have been agreed with a single point of contact within each EU Member State and the final benefiting entities.

This activity includes the establishment of a 24/7 monitoring and incident support capability in combination with activity 5.

This activity is resourced through the use of 10 Contract Agents to be absorbed as a direct cost of the programme and financed through the Commission contribution agreement. ENISA would not be able to resource this activity within its current establishment plan. The budget for this activity is to be implemented during 2025 and 2026.

This activity will be adjusted when the Cyber Solidarity Act enters into force. According to the Cyber Solidarity Act, the Commission shall entrust, partly or fully, the administration and operation of the EU Cybersecurity Reserve to ENISA. The Reserve entails delivery of incident response services and it also includes the mapping of the services needed by the users of the Reserve, including the availability of such services for legal entities established and controlled by Member States.

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

The legal basis for this activity is Articles 6 and 7 of the CSA.

Link to strategic objectives (ENISA STRATEGY)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective Union preparedness and response to cyber incidents, threats and cyber crises

Indicator for strategic objectives



- Operationalisation of the EU Cybersecurity Reserve of which the administration and operation is to be entrusted fully or partly to ENISA and used by MSS, EUIBAs and on a case-by-case basis by DEP associated third countries

ACTIVITY 6 OBJECTIVES

| Description | CSA Article And Other EU Policy Priorities | Timeframe Of Objective | Indicator | Target |
|--|--|------------------------|---|------------------|
| 6.A By end Q2 2026, deliver and complete ENISA support actions | 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) |
| 6.B. By end Q2 2026 and onwards, deploy European Cyber Reserve under CSOA. | Articles 6 and 7 of the CSA | 2026 | Reaching consensus with the EC on European Cyber Reserve. (survey) Timely deliver. (survey) | 4 (1 to 5 score) |

ACTIVITY 6 OUTPUT



| Description | Expected Results Of Output | Validation | Output Indicator | Frequency (Data Source) | Latest Results | Target 2025 |
|---|--|---------------------------------|---|-------------------------|----------------|---------------|
| 6.1 Provide penetration testing (pentest) and threat hunting services towards selected entities within EU Member States ³¹ | Pentest and Threat Hunting services are delivered in a timely and accurate manner to MSs | MSs, CNECT, Beneficiaries | Percentage of MSs requesting the service Satisfaction score | | n/a | 50% >4 |
| 6.2 Provide customised exercises and training for selected entities within EU Member States | Customised exercise and training services are delivered in a timely and accurate manner to MSs | MSs, CNECT, Beneficiaries | Percentage of MSs requesting the service Satisfaction score | | n/a | 50% >4 |
| 6.3 Support risk monitoring and assessment for selected entities within EU Member States | ENISA is able to provide regular risk monitoring towards specific targets or at national level, including by leveraging commercial of-the-shelf platforms, as well as providing specific risk assessment and threat landscapes as requested by MSs | MSs, CNECT, Other beneficiaries | Percentage of MSs requesting the service Satisfaction score | Annual | n/a | 50% >4 |
| 6.4 Support incident response and incident management of selected entities within EU Member States | ENISA provides 24/7 support for incident response to MSs | MSs, CNECT, other beneficiaries | Percentage of MSs requesting the service Support provided in a timely manner Satisfaction Score | | n/a | 50% >4 |

31 - The beneficiaries of Activity 5 services are specified in the Contribution Agreement.

Stakeholders and engagement levels



Partners: EU Member States, selected beneficiary entities, Commission

Involve / Engage: EU-CyCLONe, CSIRT Network, DG CONNECT

ACTIVITY 6 RESOURCE FORECASTS

| | Budget | FTEs |
|---|---|---|
| Total activity resources from direct annual budget | Budget: n/a | FTE: 4 |
| Other supplementary contributions | Budget: TBD ³² | FTEs: TBD |
| Other supplementary contributions on-going | Budget: forecast EUR 9 773 866.89 from existing contribution agreement signed in 2023 | 9 FTEs financed from existing Contribution Agreement signed in 2023 |

³² - Allocation depending on the final text of the contribution agreement to be signed with the Commission in 2024. Allocation is expected to be EUR 15 000 000 to support Cybersecurity action, situation centre and implementation of the CRA single reporting platform. Please refer to annex XI for further details regarding contribution agreements, final text pending. The amount indicated refers to the years 2025 to 2027.

ACTIVITY 7: Supporting Development and maintenance of EU cybersecurity certification framework



Overview of activity



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 Programme (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 certification of ID Wallets (support for national schemes and for the development of an EU scheme) as a priority, and other schemes under development (EU5G, 5G), as well as activities related to upcoming requests in line with the URWP, such as the one related to managed security services following entry into force of an amendment to the CSA. These actions also include supporting the maintenance and review as well as evaluation of the adopted European cybersecurity certification schemes, in particular the adopted scheme from 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 regulations on implementation. 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 review; cryptographic mechanisms) as well as with co-chairing and providing a secretariat for the Stakeholder Cybersecurity Certification Group (SCCG).

ENISA has developed a one candidate scheme based on an EC request from 2019, in accordance with Article 49.2, which was adopted as an implementing regulation, the EUCC. ENISA is currently developing two other candidate schemes also based on EC requests, the EU5G and the EU5G, in accordance with Article 49.2. The URWP was adopted in Feb 2024, and a recent request received for the development of an EUDI wallet candidate scheme is in line with Article 49.1. In anticipation of a possible request for an EU scheme on MSS, as foreseen by the URWP and the amendment to the CSA, ENISA is developing a feasibility study. ENISA has also explored the possibility of the certification of AI, which is also highlighted in the URWP but for which no request for a candidate scheme is expected soon.

ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Article 50 of the CSA. As from 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 laws, in particular the Cyber Resilience Act. Other relevant pieces of legislation 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 legal basis for this activity is Article 8 and Title III Cybersecurity certification framework of the CSA.

Link to strategic objectives (ENISA STRATEGY)



- Empowered communities in an involved and engaged cyber ecosystem
- Building trust in secure digital solutions

Indicator for strategic objectives



- Number of EU certification schemes developed and maintained, number of 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 |
|---|--|------------------------|---|---|
| 7.A Between 2025-2027, timely development of feasibility studies for future potential schemas | CSA Article 49 | 2027 | Number of feasibility studies concluded in view of upcoming requests, including managed security services (on-going) | 3 (pending potential new requests for scheme) |
| | | | Elements of feasibility study reflected/ aligned with EC request for new schemas | More than 50% |
| 7.B. Between 2025-2027, timely finalisation of candidate schemas following formal requests for drafting new cybersecurity certification schemas | CSA Article 49 | 2027 | Number of drafts of certification schemas delivered to COM (ID Wallet Certification and, pending formal COM request, Managed Security Services) | 2 |
| | | | ECCG endorsement of draft certification schemas | Positive ECCG endorsement |
| | | | SCCG opinion on draft certification schemas (satisfaction survey) | More than 60% |
| 7.C Ensure the maintenance of existing schemas and support their roll-out | CSA Article 49 | 2027 | Number of schemas maintained with active involvement by ENISA | 1 (EUCC) + EUCS pending final approval |
| | | | Satisfaction by ECCG on ENISA's supporting efforts for documents for maintenance | 75% |
| | | | Number of certificates issued and published under an EU certification scheme; high rate of use in the market. | Proportionate ³³ 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 2025 |
|---|--|--|---|-------------------------|----------------|--|
| 7.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemas | Scheme meets stakeholder requirements, notably those of Member States and the Commission Take up of schemas by stakeholders Timely delivery by ENISA of all schemas requested in cooperation with the Commission Statutory Bodies and ad hoc working groups actively involved | Ad hoc working groups on certification | Stakeholder satisfaction | Biennial (survey) | 82% | 75% |
| | | ECCG | Number of opinions of stakeholders managed | Annual (report) | n/a | 100 opinion items per scheme |
| | | European Commission | Number of people or organisations engaged in the preparation of certification schemas | Annual (report) | n/a | At least 20 ad hoc Working Group Members from third-party Experts; at least 15 Member States joining ad hoc Working Groups |
| 7.2 Implementation and maintenance of established schemas including evaluation of adopted schemas, participation in peer reviews etc., monitoring the dependencies and vulnerabilities of ICT products and services | Review of schemas to improve efficiency and effectiveness Take up of schemas by stakeholders | ECCG | Stakeholder satisfaction | Biennial | 82% | 75% |
| | | European Commission | ECCG satisfaction of ENISA efforts on schemas adopted | Triennial (survey) | n/a | 75% |
| | | | Satisfaction with ENISA's role in NCCA peer reviews | Triennial (survey) | n/a | 75% |
| 7.3 Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks | | ECCG | Stakeholder satisfaction | Biennial | 82% | 75% |
| | | European Commission | Feedback from statutory bodies including NCCAs on ENISA's role | Annual (survey) | n/a | 75% |
| | | SCCG | | | | |

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

| | | | | | | |
|--|---|---------------------|--|-----------------|-----|-----|
| 7.4 Developing and maintaining the necessary provisions, tools and services concerning the Union's cybersecurity certification framework (incl. certification website, supporting the Commission in relation to the core stakeholders service platform of CEF (Connecting Europe Facility) for collaboration, publication and promotion of the implementation of the cybersecurity certification framework etc.) | Transparency and trust in supporting ICT products, services and processes | ECCG | Stakeholder satisfaction | Biennial | 82% | 75% |
| | | European Commission | User satisfaction with the services on the certification website | Annual (survey) | n/a | 75% |
| | Stakeholders engagement in promotion of certification | SCCG | Use of the certification website | Annual (report) | n/a | 75% |

Stakeholders and engagement levels



Partners: EU Member States (including National Cybersecurity Certification Authorities, ECCG), European Commission, EU Institutions, Bodies 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 |
|---------------------------------|---|-----------------------------|
| Total activity resources | Budget: EUR 697 089³⁴ | FTE³⁵: 10 |

34 - of which €127 000 is centralised to missions and the budget for large-scale events.

35 - Target FTEs.

ACTIVITY 8: Supporting European cybersecurity market, research & development and industry



Overview of activity



This activity seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular for SMEs and start-ups, to reduce dependence from outside and increase the capacity of the Union and 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 ICT products, services and processes, including through standardisation and the adoption of relevant codes of conduct. As such, this activity also seeks to lay the ground for an effective role for ENISA in the CRA, notably in terms of market analysis, the preparation of market sweeps, and the collection and analysis of information for the identification of emerging cybersecurity risks in products with digital elements, etc.

Secondly, the actions to support this activity include producing analyses and guidelines as well as good practices on cybersecurity and data protection requirements, including eIDAS2 and trust services, facilitating the establishment and take up of European and international standards across applicable areas such as risk management as well as performing regular analyses 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 as well as incidents that have occurred. The activity aims at strengthening and reinforcing ties with the private sector and promoting collaboration among cybersecurity market players, in order to improve the visibility and uptake of trustworthy and secure ICT solutions in the digital single market.

At the same time, this activity aims to provide advice to EU Member States (MSs), EU institutes, bodies and agencies (EUIBAs) on research needs and priorities in the field of cybersecurity, thereby contributing to the EU's strategic research and innovation agenda, notably the ECCC.

To prepare this strategic advice, ENISA will take full account of past and ongoing research, the development and assessment of technology, outputs of other statutory bodies in the cybersecurity landscape such as the NIS Cooperation Group, ECCG, CSIRTs Network, EU-CyCloNe. The Agency will also 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 used.

ENISA will also conduct regular consultations with relevant user groups, projects (including EU funded projects), researchers, universities, institutes, industry, start-ups and digital innovation hubs to consolidate information and identify gaps, challenges and opportunities in research and innovation from the various quadrants of the community. The ecosystem of the ECCC and the National Coordination Centres (NCCs) will be involved in these consultations. A strong collaboration with, and the mapping of the relevant requirements of, the market authorities as defined in the CRA will also take place in the context of this activity.

Finally, this activity supports cybersecurity certification and the assessment of the conformity of products with digital elements by monitoring the standards being used by European cybersecurity certification schemes and digital products, 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 legal basis for this activity is Articles 8 and 11 and Title III of the CSA, as well as the CRA, the eIDAS2 Regulation, the AI Act (Article 67) and the Data Governance Act (Article 29).

Link to strategic objectives (ENISA STRATEGY)

- Empowered communities in an involved and engaged cyber ecosystem
- Building trust in secure digital solutions
- Foresight on emerging and future cybersecurity opportunities and challenges



Indicator for strategic objectives



- Rate of satisfaction with ENISA's support for the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCC), number of advisories and the level of support given on Research and Innovation Needs and Priorities for the ECCC and its uptake by the ECCC

ACTIVITY 8 OBJECTIVES

| Description | CSA Article And Other EU Policy Priorities | Timeframe Of Objective | Indicator | Target |
|---|--|------------------------|---|--|
| 8.A 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 critical products and services with digital elements under the CRA | CRA (final text pending) | 2026 | Timeliness of ENISA reports | Reports delivered on time |
| | | | Acceptance of ENISA reports by MSs | 2/3rds of MSs endorsing ENISA reports |
| | | | Validity of ENISA framework | All MSs validating and endorsing ENISA framework |
| 8.B Provide continuous comprehensive support to MSs' market supervisory authorities and to the COM for implementing CRA requirements. | CRA (final text pending) | 2026 | MSs and COM stakeholder satisfaction survey | More than 70% |
| 8.C. Create a technology and innovation radar, to understand the level of impact that new technologies are having on cybersecurity | CSA Article 9 and CRA (final text pending) | 2026 | Number of cybersecurity trends and patterns accurately identified through an evidence-based methodological approach | 5% increase over reference data |
| | | | Assessment of impact of EU cybersecurity R&I | 5% increase over reference data |

ACTIVITY 8 OUTPUTS

| Description | Expected Results Of Output | Validation | Output Indicator | Frequency (Data Source) | Latest Results | Target 2025 |
|---|---|--|--|------------------------------|----------------|-------------|
| 8.1 Collect and analyse information on new and emerging information and communications technologies and provide strategic advice to ECCC on the EU agenda on cybersecurity research, innovation and deployment. | Identifying current and emerging ICT gaps, trends, opportunities and threats Advising EU Funding programmes including the ECCC and its Strategic Agenda and Action Plan. | Academia, Industry and National R&I, MSs market authorities, Entities (including NCCs) and EUIBAs EC including CNECT and JRC, ECCC and NCCs, as appropriate | Stakeholder satisfaction | Biennial (survey) | 91% | >90% |
| | | | Findings endorsed by MSs (NCCs and market authorities) | Annual | n/a | > 60% |
| | | | Alignment with ECCC Strategic Agenda and Action Plan | Annual (survey with ECCC GB) | n/a | > 60% |

| | | | | | | |
|---|---|--|--|--|-----|--|
| 8.2. Market analysis of the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes and prepare biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements | Improved understanding of the market and industry | Ad hoc working groups for cybersecurity market analysis ECCG (as necessary) SCCG Advisory Group NLO (as necessary) MSs Market authorities | Stakeholder satisfaction | Biennial (survey) | 88% | 60% |
| | | | Cybersecurity market analysis; cybersecurity products and services | Annual (report) | n/a | All reports produced as planned (Y out of Y reports) |
| | | | Endorsement by MSs of report on emerging trends regarding cybersecurity risks in products with digital elements | Biennial (report) | n/a | 27 MSs endorse report |
| 8.3 Support 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. | Produce a catalogue of market surveillance authorities; survey requirements of market surveillance authorities; identify categories of products; produce a methodology on market sweeps; carry out market sweeps Evaluations to be carried out ideally on the basis of input from market sweeps; rely on external expertise. This output should be carried out under A7 Certification | NLO / NCCA Commission SCCG (as appropriate) | Collection of requirements Matching requirements with deliverables Time to carry out market sweeps Methodology for evaluations Profiles of experts | Catalogue, survey and categories of products in 2025-26 Market sweeps as from 2027 (3-year transition) or earlier if requested Method to evaluate products Guidance and criteria to accept evaluation results | n/a | Stakeholder satisfaction above 60% |
| 8.4 Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification | Alignment with standards | SCCG Advisory Group NLO (as necessary) | Stakeholder satisfaction | Biennial (survey) | 88% | 60% |
| | | | Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification | Annual (report) | n/a | All reports produced as planned (Y out of Y reports) |

Stakeholders and engagement levels



Partners: EU Member States (including market authorities and entities with an interest in cybersecurity market monitoring, e.g. NCCA, National Standardisation Organisations), European Commission, EU Institutions, Bodies 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 Centres.

Involve / Engage: Private sector stakeholders (entrepreneurs, start-ups and investors) with an interest in cybersecurity market and/or standardisation, International Organisation for Standardisation / International Electrotechnical Committee, Consumer Organisations.

ACTIVITY 8 RESOURCE FORECASTS

| | Budget | FTEs |
|---------------------------------|---|-----------------------------|
| Total activity resources | Budget: EUR 697 887³⁶ | FTE³⁷: 10 |

36 - Of which €134 200 centralised to missions and the budget for large-scale events..

37 - Target FTEs.

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



This activity seeks to achieve requirements under Article 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 the Agency's operations. In addition in line with Article 4(2) of the CSA this activity includes contributions to gains in efficiency, e.g. via shared services in the EU Agencies network and in key areas by relying on the Agency's own expertise (e.g. cybersecurity risk management).








Under this activity ENISA seeks to deliver, as a service-centric and sustainable organisation, key objectives of the Agency's Corporate Strategy by establishing a framework for the thorough assessment of quality, ensuring proper and functioning internal controls and compliance checks, as well as maintaining a high level of cybersecurity across all the Agency's corporate and operational activities. In terms of resource management, the Budget Management Committee coordinates the Agency's adherence to the principles of financial management. 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 Articles 4(1) and 4(2) of the CSA as well as Articles 24 to 28, Article 41 and Articles 32 to 33 (re ENISA's financial rules and combatting 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 | 13 metrics were unchanged, 21 underperformed and 58 overperformed | >80 of indicators overperformed |
| | Continuous innovation and service excellence | Results of assessment of Internal control framework | Annual | Effective (Level 2) | Effective level 1/2 |
| | Developing service propositions with additional external resourcing | High satisfaction with essential corporate services in the area of compliance and coordination | Annual | n/a | >60% |
| 9.B Increase corporate sustainability | Ensure climate neutral ENISA by 2030 | Maintain EU Eco-Management and Audit Scheme (EMAS) | Annual | n/a | Implement follow up actions to ensure EMAS certification is maintained |
| | Develop efficient framework for ENISA's continuous governance to safeguard a 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 | n/a n/a | 70% implementation (ITMC reporting) 20% |

ACTIVITY 9 OUTPUTS

|  |  |  |  |  |  |  |
|--|--|---|---|--|---|--|
| Description | Expected results of output | Validation | Output indicator | Frequency (data source) | Latest results | Target 2025 |
| <p>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</p> | Unified day-to-day practices across the agency upon implementing SPD | MT, ITMC & BMC External and internal audits Statutory bodies | Number of high risks identified in annual risk assessment | Annual | 3 | <= 3 |
| | Annual assessments of risk and internal controls performed and reported | | Effective monitoring of high risks and critical recommendations to follow up on timely implementation of mitigation measures by business owners | | n/a | Quarterly status reporting to the MT Internal controls assessment including reporting on implementation for year N-1 Risk assessment |
| | Legal and regulatory compliance monitored; issues and areas for improvement identified | | Percentage of identified deficiencies in internal controls addressed within timelines | | n/a | 100% for critical, 80% for major, 60% for moderate |
| | Outcomes are included in the annual assessments of risk and internal controls | | Timely follow-up and resolution of internal and external audits (in particular from IAS and ECA) recommendations and findings | | | Monitoring audit action plans Results of corrective actions taken during year N-1 are reported in the current year AAR |
| | Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy under ITMC | | Number of identified regulatory breaches | | 3 | <=3 |
| | Streamlined budget management across the Agency, under BMC | | Percentage of revised and up to date corporate rules (MBD, EDD, policies, processes) | | n/a | Review 50% of corporate rules which have not been reviewed in the last 4 years; 60% of corporate rules which have not been reviewed in the last 5 years. Provide or confirm motivation for non-revision, as baseline requirement |
| | A plan to reduce CO2 emissions at ENISA's HQ | | Annual report on ARES maintenance and actions | | n/a | 80% resolution of identified open issues, incorporating lessons learned |
| | | | Reduction of CO2 emissions in ENISA HQ | | n/a | By >5%; provide motivation if expected rate is unattainable, as baseline provision |
| | | | Efficiency and effectiveness of ITMC & BMC (survey) | | n/a | > 60% |

| | | | | | | |
|---|--|---|---|--------|-----|--|
| 9.2 Maintain and enhance ENISA's cybersecurity posture | Compliance with new regulations on a high common level of cybersecurity within Union entities Timely identification and response to cybersecurity risks Continuous monitoring of cybersecurity of IT systems and timely identification of issues and areas for improvement (first level and second level controls) | MT and relevant committees | Percentage of identified high risk mitigation measures addressed within timelines | annual | n/a | 90% |
| | | External and internal audits | | | | |
| | | Statutory bodies | Annual risk assessment (RA) and risk treatment plan with the relevant business owners | annual | n/a | Implement annual risk assessment follow up actions. |
| | | | Implement action plan for implementation of cybersecurity risk management measures in line with Regulation (EU) 2023/2841 | annual | n/a | Report on the level of accomplishment of action plan |
| | | | Address all potential cybersecurity incidents | annual | n/a | Respond to >90% of tickets submitted to ServiceNow |
| | | | Cybersecurity training for staff and managers | annual | n/a | At least two training sessions a year |
| 9.3 Provide support services to the EU Agencies network and in key areas of the Agency's expertise and chair EUAN in 2025 | Cybersecurity advisory on implementation of the new regulation on a high common level of cybersecurity within Union entities and in co-operation with CERT-EU Shared services in the area of data protection, legal services and accounting | MT, BMC EUAN (Agencies receiving ENISA's support) | Satisfaction within the EU Agency network with ENISA support services | annual | n/a | >80% |
| 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 or accessible within ENISA | Annual | 29% | 55% |
| | | | Response timeliness to external parties (internal reporting) | Annual | n/a | 48h |

Stakeholders and engagement levels



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

ACTIVITY 9 RESOURCE FORECASTS

| | Budget | FTEs |
|-----------------------------------|---|-----------------------|
| Total activity resources | Budget: EUR 743 000 | FTE: 14 ³⁸ |
| Other supplementary contributions | Budget: EUR 54 604 SLA with ECCC, see annex XI for additional information | FTE: 0 |

38 - Including ED, COO, advisor and accounting officer

ACTIVITY 10: Reputation and Trust



Overview of activity



This activity seeks to meet the requirements set out in Article 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 contributing to efficiency gains by optimising the way it engages with stakeholders and offering on demand services in addition to essential services to increase the Agency's outreach.

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







In this activity, ENISA will deliver essential and demand driven communications services as described in ENISA's Corporate Strategy.

The legal basis for this activity is Article 4(1), Sections 1 and 2, as well as Articles 21, 23 and 26 of the CSA, in which the latter 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% |
| | | ENISA brand management | Annual | n/a | Target set in crisis communications playbook by 2025 |
| 10.B Improve outreach of ENISA's mandate | Ensure efficient corporate services | Corporate satisfaction with essential communication and administrative assistants services | Annual (MT survey) | n/a | 60% |
| | | Corporate satisfaction with demand driven communication and assistants services | Annual (MT survey) | n/a | 60% |
| | | Stakeholder satisfaction with ENISA events | Annual | n/a | >60% |
| | | Number of unique visitors | Annual | | >10% increase year on year |

ACTIVITY 10 OUTPUTS

|  Description |  Expected results of output |  Validation |  Output indicator |  Frequency (data source) |  Latest results |  Target 2025 |
|---|---|--|--|--|--|---|
| 10.1 Review and implement the multiannual communications strategy and support stakeholders' strategy including corporate outreach | Enhanced transparency and outreach | Management Team and agency stakeholders | Number and types of activities at each engagement level (stakeholder strategy implementation) | Annual (Internal report) | n/a | Stakeholder strategy under review |
| | Engaged communities | | Number of social media engagements | Annual (Media monitoring) | 75k | >80k |
| | Increased impact of ENISA activities | | Stakeholder satisfaction with ENISA outreach | Biennial (survey) | n/a | >80% |
| | Relevant and easily accessible information is provided to stakeholders | | Number of total ENISA website visits | Annual (website analytics) | 2.03 million | >2.5 million |
| | Successful EUAN leadership, communications and EUAN yearly meetings | | Website availability | Annual (website analytics) | 97% | >97% |
| 10.2 Implement internal communications strategy | Engaged staff | Management Team and staff committee | Staff satisfaction with ENISA internal communications | Annual (survey) | 39% | >60% |
| 10.3 Manage and provide the secretariat for statutory bodies, i.e. EB, MB, AG, NLO (excluding certification) | Support for the operation and organisation of ENISA statutory bodies | Statutory bodies, Management Team and Committees | Number of feedback instances received per NLO consultation | Annual (Internal report) | n/a | >6 |
| | Support the effectiveness of implementation of work programmes (validation of operational outputs) | | Number of feedback instances received per AG consultation | Annual (Internal report) | n/a | >8 |
| | Provision of administrative support for the day to day workings of the Management board's decisions and recommendations from NLO & AG | | Satisfaction of statutory bodies with ENISA's support to fulfil their tasks as described in CSA | Annual (Survey) | n/a | >80% |
| | | | Satisfaction of statutory bodies with ENISA portals | Annual (Survey) | n/a | >80% |

Stakeholders and engagement levels



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

Involve / Engage: All ENISA stakeholders

ACTIVITY 10 RESOURCE FORECASTS

| | Budget | FTEs |
|---------------------------------|----------------------------|----------------|
| Total activity resources | Budget: EUR 760 000 | FTE:8.5 |

ACTIVITY 11:

Effective and efficient corporate services



Overview of activity



This activity seeks to meet Article 3(4) of the Cybersecurity Act which calls upon 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 them with the Agency’s goals and needs, by attracting, retaining and nurturing talent while enhancing its reputation as an agile, knowledge-driven organisation where staff can grow, stay motivated and remain engaged. A key priority is the development of competency, positioning ENISA as an ‘employer of choice’ and a rewarding place to work for all.








The Agency strives to maximise 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’s IT strategy.

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 retention | Implementation of the Corporate and HR strategy | | n/a | Actions implemented according to the timelines |
| | Caring and inclusive modern organisation | High participation in staff satisfaction survey | | 64% | 75% participation rate |
| 11.B Ensure sustainable and efficient corporate solutions and promote continuous improvement | Ensure efficient corporate services | Implement best practices in sustainable IT solutions | Annual | n/a | IT strategy updated accordingly |
| | Introduce digital solutions that maximise synergies and collaboration in the Agency | Limited disruption of continuity of corporate services | Annual | n/a | BCP for corporate IT facilities, financial and HR services in 2025 |
| | Developing service propositions with additional external resourcing | Handling EUCl at the level of SECRET UE/EU SECRET | Annual | n/a | Operational for the first full year in 2025 |
| | Promote and enhance ecologic sustainability across all Agency's operations | | | | |
| | Develop efficient framework for ENISA's continuous governance to safeguard high level of IT and to ensure physical security services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently | | | | |

ACTIVITY 11 OUTPUTS

|  |  |  |  |  |  |  |
|---|---|--|---|---|---|---|
| Description | Expected results of output | Validation | Output indicator | Frequency (data source) | Latest results | Target 2025 ³⁹ |
| 11.1 Manage and provide horizontal, recurrent administrative services in the area of resources for ENISA staff and partners | Services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently. | Management Team IT Management Committee Budget Management Committee Staff Committee | Turnover rates | Annual | 4.9% | <5 % |
| | | | Establishment plan posts filled | | 98% | >95% |
| | | | Lag between vacancy announcement to candidate selection | | n/a | <300 days median across all posts |
| | | | Percentage implementation of approved Recruitment plan | | n/a | >90% |
| | | | Percentage implementation of approved Procurement Plan | | n/a | >90% |
| | | | Percentage procurement procedures launched via e-tool (PPMT) | | 100% | >90% |
| | | | Percentage budget implementation | | 100% | >95% |
| | | | Average time for initiating a transaction (FIA role) | | n/a | <7 days |
| | | | Average time for verifying a transaction (FVA role) | | n/a | <3 days |
| | | | Number of budget transfers | | 2 | <4 |
| Late payments resulting in interest payments | 9% | <10% | | | | |

39 - Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023

| | | | | | | |
|---|---|--|---|--------|------|-------------------------------------|
| 11.2 Implement Agency's Corporate strategy including HR strategy with emphasis on talent development, growth and welfare | Objectives and goals set out in the corporate and HR strategy are met. | Management Board Management Team Staff Committee EUAN BMC | Number of policies/IR reviewed | Annual | n/a | >1 |
| | | | Number of processes revised | | n/a | >1 |
| | | | Percentage of staff satisfaction with talent development | | 58% | >50% |
| | | | Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time | | n/a | >95% |
| | | | Number of implemented competency driven training and development activities | | n/a | >1 |
| | | | Number of multisource feedback evaluations implemented and followed up | | n/a | >5 |
| 11.3 Manage and provide horizontal, recurrent support services in the area of facilities, security and corporate IT for ENISA staff and partners | Services such as corporate IT, facilities and security are performed efficiently with minimal disruption. Upgrade of meeting rooms | Management Team IT Management Committee Budget Management Committee Staff Committee | Staff satisfaction with working environment | Annual | 74% | >70 % |
| | | | Time to respond to safety and security incidents. | | n/a | <1 to acknowledge and <3 to respond |
| | | | Average time to respond to facilities management requests | | n/a | <1 to acknowledge and <3 to respond |
| 11.4 Enhance operational excellence and digitalisation through modern, safe, secure and streamlined ways of working, and introducing self-service functionalities | Services such as access management, meeting room facilities, equipment renewals, cloud-based solutions and data availability are efficient. | Management Team IT Management Committee | Critical systems uptime and downtime | Annual | 100% | 99% |
| | | | Staff satisfaction with IT resolution | | 84% | 85% |

Stakeholders and engagement levels



Partners: ENISA staff members and EU Institutions, Bodies and Agencies

Involve / Engage: Private sector and international organisations

ACTIVITY 11 RESOURCE FORECASTS

| | Budget | FTEs |
|--------------------------|-----------------------|------------|
| Total activity resources | Budget: EUR 4 631 348 | FTE: 21.25 |

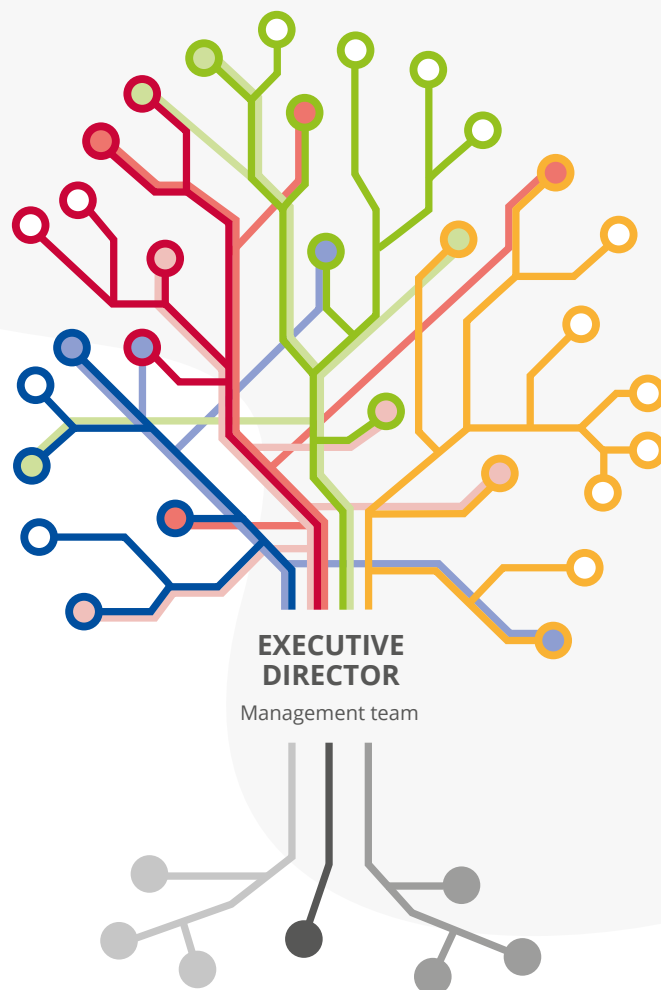


A large, bold, white capital letter 'A' is centered on a blue background. The background is filled with a repeating pattern of white circuit board traces, including lines, right-angle turns, and small circular nodes, creating a dense, technical aesthetic.

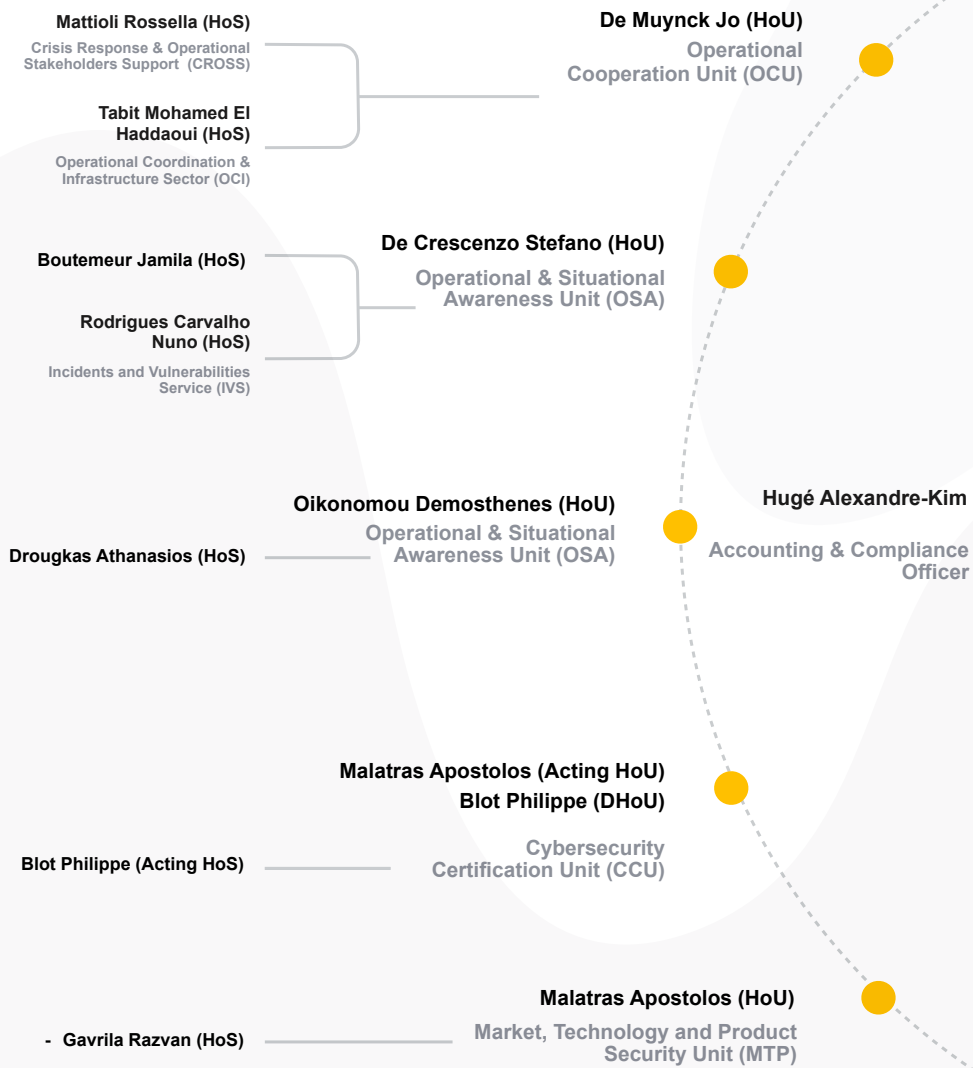
A

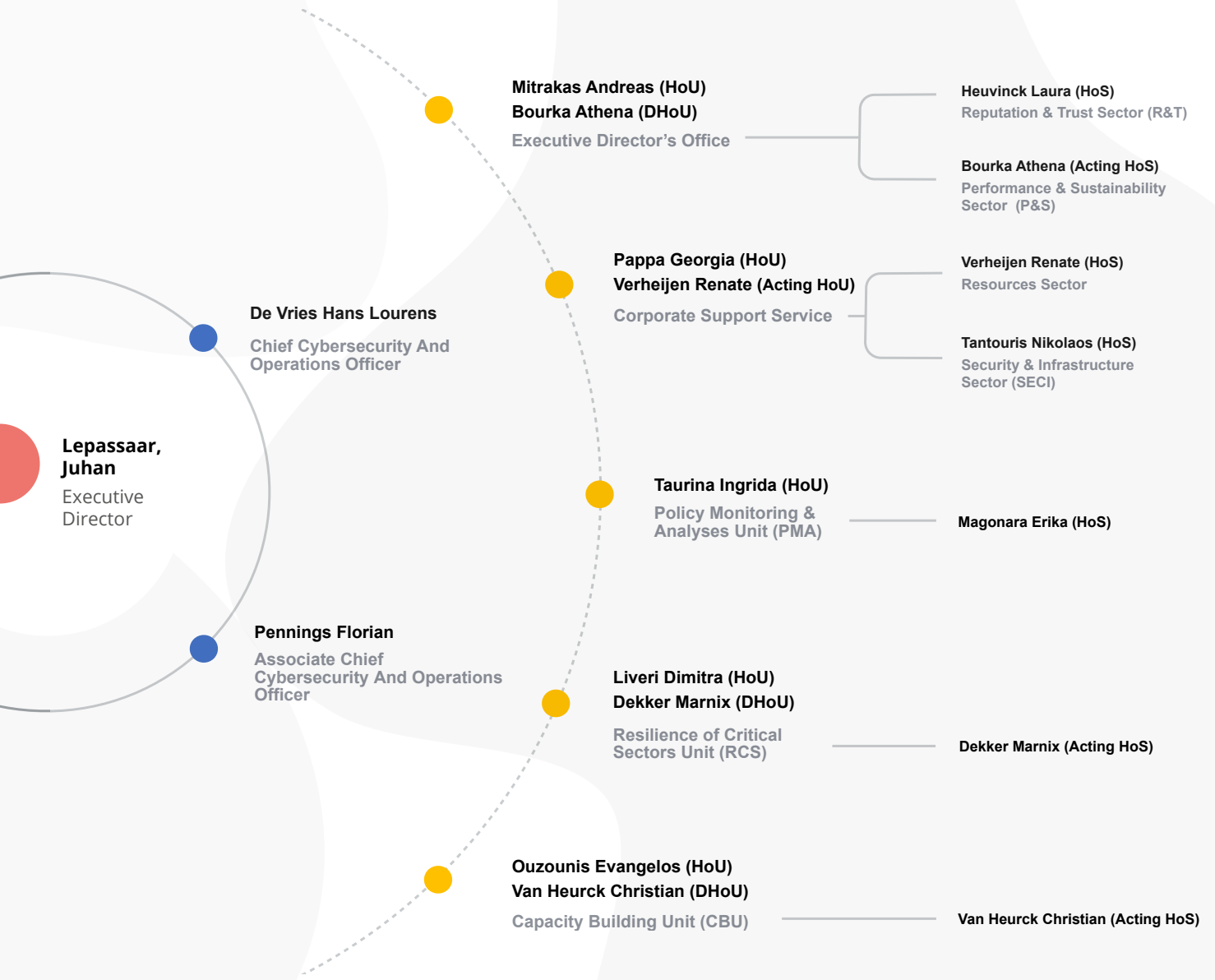
ANNEX 1

ORGANISATION CHART AS OF 31.12.2024



Administrative organigramme





ANNEX 2

RESOURCE ALLOCATION PER ACTIVITY 2025–2027

The indicative allocation of the total financial and human resources for 2025 for the activities described in part 3.1 in Section III and the corporate activities described in part 3.2 in Section III are presented in the table below. The allocation will be done after the direct budget and FTEs indicated for each activity are finalised, with the indirect budget being assigned on the basis of causal relationships.

The following assumptions are used in the simplified ABB methodology:

- The budget granted to ENISA through the Contribution Agreement signed in 2023 is not included in the calculations as the activities (as well as the budget) defined in that agreement cover 2024 to 2026.
- The 12 FTEs granted to ENISA through the Contribution Agreement signed in 2023 are not included in the calculations as their direct and indirect costs should be fully covered by the Contribution Agreement.
- The budget allocation for each activity includes the direct and indirect costs attributed to each activity.
- The direct budget is the cost estimate of each of the eight operational activities as indicated in Section 3.1 of the SPD 2025-2027 (carried out under Articles 5-12) in terms of the goods and services to be procured.
- The budget for operational missions and large-scale operational events is allocated to operational activities (Activities 1-8) based on the number of direct FTEs under each activity.
- The indirect budget is the estimated cost of salaries and allowances, buildings, IT equipment and miscellaneous operating costs attributable to each activity. The indirect budget is allocated to activities based on various drivers. The main driver for the allocation of costs is the expected number of direct FTEs for each operational activity in 2025.
- In order to estimate the full costs of operational activities, all corporate activities (Activities 9 to 11) should be distributed according to all the operational activities based on related drivers.

Table

| ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2025) | Activities as referred to in Section 3 | Direct and Indirect budget allocation (in EUR) | FTE allocation |
|---|--|--|----------------|
| Support for policy monitoring and development | Activity 1 | 1 831 516.52 | 10.27 |
| Cybersecurity and resilience of critical sectors | Activity 2 | 2 168 320.81 | 12.27 |
| Building capacity | Activity 3 | 2 528 705.60 | 12.27 |
| Enabling operational cooperation | Activity 4 | 3 824 113.17 | 1,27 |
| Provide effective operational cooperation through situational awareness | Activity 5 | 3 313 414.95 | 12.27 |
| Provide services for operational assistance and support * | Activity 6 | 488 119.14 | 3.27 |
| Development and maintenance of EU cybersecurity certification framework | Activity 7 | 2 107 568.15 | 10.27 |
| Supporting European cybersecurity market, research & development and industry | Activity 8 | 2 101 166.31 | 10.27 |
| Performance and sustainability | Activity 9 | 2 550 997.35 | 14.27 |
| Reputation and trust | Activity 10 | 1 974 345.60 | 8.27 |
| Effective and efficient corporate services | Activity 11 | 3 541 974.40 | 21.27 |
| TOTAL | | 26 430 242.00 | 130.00 |

* Activity 6 is implementing activities agreed under the Contribution Agreement signed in 2023 for which a budget of EUR 20 million has been granted as well as 12 FTEs for the implementation of the agreed activities during 2024-2026.

ANNEX 3

FINANCIAL RESOURCES

2025–2027

Table 1. Revenue (excluding additional financing through contribution agreements)

| Revenue | 2024 | 2025 |
|--------------------------------|-------------------|-------------------|
| EU contribution | 24 953 071 | 25 716 933 |
| Other revenue (EFTA) | 883 404 | 713 309 |
| Other revenue (SLAs, Annex XI) | 174 604 | 174 604 |
| TOTAL | 26 011 079 | 26 604 846 |

| Revenue | 2024 adopted budget | VAR 2025 / 2024 | Draft Estimated budget 2025 | Envisaged 2026 | Envisaged 2027 |
|---|---------------------|-----------------|-----------------------------|-------------------|-------------------|
| 1. Revenue from fees and charges | | | | | |
| 2. EU contribution | 24 953 071 | 1,95% | 25 716 933 | 26 213 532 | 26 719 532 |
| – of which assigned revenues deriving from previous years' surpluses ** | 320 868 | | 150 299 | 0 | 0 |
| – of which Reserve conditional to approval of NIS2 Directive | 883 404 | -19,25% | 713 309 | 716 654 | 738 500 |
| 3. Third countries' contribution (including EEA/ EFTA and candidate countries) | 883 404 | -19,25% | 713 309 | 716 654 | 738 500 |
| – of which EEA/EFTA (excl. Switzerland)** | | | | | |
| – of which Candidate Countries | | | | | |
| 4. Other contributions* | | n/a* | | | |
| 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*** | 174 604 | 0,00% | 174 604 | 174 604 | 174 604 |
| 7. Correction of budgetary imbalances | | | | | |
| TOTAL REVENUES | 26 011 079 | 2,28% | 26 604 846 | 27 104 790 | 27 632 636 |

* - after the move to the new building, Hellenic Authorities make rental payments directly to the building owner, therefore no subsidy is paid to ENISA

** - for the purpose of calculation of EFTA funds for 2026-2027 average surplus of last 3 years was used with 2,79% EFTA proportionality factor 2025

*** - revenue foreseen from the existing SLAs signed with ECCC and eu-LISA, ref. Annex XI

Table 2. Expenditure (excluding revenue for services rendered and additional financing through contribution agreements)

| Expenditure * ** | 2024 | | 2025 | |
|--------------------------|---------------------------|------------------------|---------------------------|------------------------|
| | Commitment appropriations | Payment appropriations | Commitment appropriations | Payment appropriations |
| Title 1 | 14 739 106 | 14 739 106 | 15 271 440 | 15 271 440 |
| Title 2 | 3 666 898 | 3 666 898 | 4 159 348 | 4 159 348 |
| Title 3 | 7 430 471 | 7 430 471 | 6 999 454 | 6 999 454 |
| Total expenditure | 25 836 475 | 25 836 475 | 26 430 242 | 26 430 242 |

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

| Expenditure (in EUR)* ** | Commitment and Payment appropriations * ** | | | | | |
|---|--|---------------------|-----------------------------|-----------------|-------------------|-------------------|
| | Adopted Budget 2023 | Adopted Budget 2024 | Draft estimated budget 2025 | VAR 2025 / 2024 | Envisaged in 2026 | Envisaged in 2027 |
| Title 1. Staff Expenditure | 12.719.412 | 14.739.106 | 15.271.440 | 3,6% | 15.560.308 | 15.865.299 |
| 11 Staff in active employment | 11.019.993 | 13.058.316 | 13.556.771 | 3,8% | 13.813.205 | 14.083.951 |
| 12 Recruitment expenditure | 404.684 | 517.889 | 508.469 | -1,8% | 518.087 | 528.242 |
| 13 Socio-medical services and training | 923.735 | 754.501 | 688.200 | -8,8% | 701.218 | 714.962 |
| 14 Temporary assistance | 371.000 | 408.400 | 518.000 | 26,8% | 527.798 | 538.143 |
| Title 2. Building, equipment and miscellaneous expenditure | 3.519.470 | 3.666.898 | 4.234.348 | 15,5% | 4.314.443 | 4.399.009 |
| 20 Building and associated costs | 1.357.750 | 1.000.719 | 1.081.300 | 8,1% | 1.101.753 | 1.123.348 |
| 21 Movable property and associated costs (***) | 0 | 0 | 0 | n.a. | 0 | 0 |
| 22 Current corporate expenditure | 472.650 | 516.125 | 809.000 | 56,7% | 824.303 | 840.460 |
| 23 Corporate ICT | 1.689.070 | 2.150.054 | 2.344.048 | 9,0% | 2.388.387 | 2.435.201 |
| Title 3. Operational expenditure | 8.944.613 | 7.430.471 | 6.924.454 | -6,8% | 7.055.434 | 7.193.725 |
| 30 Activities related to meetings and missions | 438.600 | 387.000 | 693.800 | 79,3% | 706.924 | 720.780 |
| 36/37 Core operational activities | 8.506.013 | 7.043.471 | 6.230.654 | -11,5% | 6.348.511 | 6.472.945 |
| TOTAL EXPENDITURE | 25.183.495 | 25.836.475 | 26.430.242 | 2,3% | 26.930.186 | 27.458.032 |

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

** - Does not include the additional EUR 15 000 000 granted for Support Assistance Fund (2022) and the EUR 20 000 000 granted under the Contribution Agreement (2023)

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

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; please refer to Annex XI for details. Other contribution agreements for the CRA single reporting platform, further actions for Support Action, SitCen, CRA-SRP and Cyber Reserve are under discussion.

Table 3: Budget outturn and cancellation of appropriations

| Budget outturn (all figures in EUR) | 2021 | 2022 | 2023 |
|---|----------------|----------------|----------------|
| Revenue actually received (+) | 23 058 211 | 39 227 392 | 25 293 935 |
| Payments made (-) | -17 989 374 | -20 396 780 | |
| Carry-over of appropriations (-) | -5 082 548 | -18 836 095 | -4 228 452 |
| Cancellation of appropriations carried over (+) | 209 385 | 248 745 | |
| Adjustment for carry-over of assigned revenue appropriations carried over (+) | 125 622 | 33 743 | 53 469 |
| Exchange rate difference (+/-) | -428 | -17.88 | |
| Total | 320 868 | 276 988 | 150 299 |

The budget 2023 outturn amounts to EUR 150 299.

With steady budget increases over the last few years of up to EUR 25.2 million in 2023 and a commitment rate of 100% (99.93% in 2022 and 99.51% in 2021) of appropriations for the year (C1 funds) having been reached by the end of the year shows the already proven capacity of the Agency to fully implement its annual appropriations.

In 2023 commitment appropriations were cancelled for the amount of EUR 560 representing 0.002% of the total budget.

The payment rate for the full budget of EUR 25.2 million reached 83,86% (in 2022 for ENISA's 'standard'

budget – 84.11 %, in 2021 – 77.40 %). The total amount carried forward to 2024 is EUR 4 064 543 or 16.14%.

No payment appropriations were cancelled during 2023.

The appropriations for 2022 carried over to 2023 were used at a rate of 99.2% (automatic carry-overs) which indicates a proven capability to estimate needs (in 2022 – 95.07%). From the total amount of EUR 18 782 626 carried forward, EUR 149 739 was cancelled (or 0.8 %). This cancellation represents 0.38 % of the total committed appropriations for 2022 of EUR 39 179 406 (fund source C1).

ANNEX 4

HUMAN RESOURCES – QUANTITATIVE

Overview of all categories of staff and its evolution Staff policy plan for 2025 - 2027

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

Statutory staff and SNEs

| Staff numbers | 2023 | | | 2024 | 2025 | 2026 | 2027 |
|------------------------------------|---|----------------------------------|------------------|-----------------------------------|------------------------------------|------------------------------------|-----------------|
| Establishment plan posts | Authorised budget | Actually filled as of 31/12/2023 | Occupancy rate % | Adopted | Envisaged staff | Envisaged staff | Envisaged staff |
| Administrators (ad) | 63 | 62 | 98% | 63 | 64 | 64 | 64 |
| Assistants (ast) | 19 | 18 | 95% | 19 | 19 | 19 | 19 |
| Assistants/secretaries (ast/sc) | | | | | | | |
| Total establishment plan posts | 82 | 80 | 98% | 82 | 83 | 83 | 83 |
| External staff numbers | Fte Corresponding to the authorised budget 2023 | Executed fte as of 31/12/2023 | Execution rate % | Adopted fte | Envisaged fte | Envisaged fte | Envisaged fte |
| Contract agents (ca) ⁴⁰ | 32 | 25 | 78% | 32 + 12 Ca Contribution agreement | 32 + 15* Ca Contribution agreement | 32 + 15* Ca Contribution agreement | 32 +Pm |
| Seconded national experts (sne) | 14 | 10 | 57% | 14 | 15 | 15 | 15 |
| Total external staff | 46 | 33 | 72% | 58 | 62 | 62 | 47 |
| Total staff⁴¹ | 128 | 113 | 88% | 140 | 145 | 145 | 130 |

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

| Human Resources | 2023 | 2024 | 2025 | 2026 | 2027 |
|----------------------------------|---------------|---------------|--------------------|---------------|---------------|
| | Envisaged FTE | Envisaged FTE | Envisaged FTE | Envisaged FTE | Envisaged FTE |
| Contract Agents (CA) | n/a | 12 | 12+3 ⁴² | 12+3* | pm |
| Seconded National Experts (SNEs) | n/a | n/a | n/a | n/a | n/a |
| TOTAL | n/a | 12 | 12+3* | 12+3* | pm |

40 - 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 using short term contracts with CAs.

41 - Refers to TAs, CAs and SNEs figures.

42 - Pending final contribution agreements to be signed; see annex XI.

Other human resources

- Structural service providers (number of persons)

| | Actually in place as of 31/12/2022 | Actually in place as of 31/12/2023 |
|-----------------------|------------------------------------|------------------------------------|
| Security | 7 | 7 |
| IT | 7 | 8 |
| Facilities management | 2 | 4 |

- Interim workers

| | Actually in place as of 31/12/2022 | Actually in place as of 31/12/2023 |
|--------|------------------------------------|------------------------------------|
| Number | 10 | 10 |

Table 2: Multi-annual staff policy plan - Years 2023-2027

| Function group and grade | 2023 | | | | 2024 | | 2025 | | 2026 | | 2027 |
|--------------------------|-------------------|-------------|----------------------------------|------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| | Authorised budget | | Actually filled as of 31/12/2023 | | Authorised | | Envisaged | | Envisaged | | 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 |
| AD 14 | | | | 1 | | | | | | | |
| AD 13 | | 2 | | 1 | | 2 | | 2 | | 2 | 2 |
| AD 12 | | 4 | | 3 | | 4 | | 4 | | 4 | 4 |
| AD 11 | | 2 | | 2 | | 3 | | 3 | | 3 | 3 |
| AD 10 | | 4 | | 3 | | 4 | | 4 | | 4 | 4 |
| AD 9 | | 11 | | 13 | | 14 | | 14 | | 14 | 14 |
| AD8 | | 25 | | 10 | | 15 | | 16 | | 16 | 16 |
| AD 7 | | 10 | | 13 | | 13 | | 13 | | 13 | 13 |
| AD 6 | | 4 | | 16 | | 7 | | 7 | | 7 | 7 |
| AD 5 | | | | | | | | | | | |
| AD TOTAL | | 63 | | 62 | | 63 | | 64 | | 64 | 64 |
| AST 11 | | | | | | | | | | | |
| AST 10 | | | | | | | | | | | |
| AST 9 | | | | | | 2 | | 1 | | 1 | 1 |
| AST 8 | | 3 | | 3 | | 1 | | 3 | | 3 | 3 |
| AST 7 | | 2 | | 0 | | 0 | | 3 | | 3 | 3 |
| AST 6 | | 8 | | 6 | | 9 | | 6 | | 6 | 6 |
| AST 5 | | 5 | | 4 | | 4 | | 4 | | 4 | 4 |
| AST 4 | | 1 | | 3 | | 2 | | 2 | | 2 | 2 |
| AST 3 | | | | 1 | | 1 | | | | | |
| AST 2 | | | | 1 | | | | | | | |
| AST 1 | | | | | | | | | | | |
| AST TOTAL | | 19 | | 18 | | 19 | | 19 | | 19 | 19 |
| AST/SC 6 | | | | | | | | | | | |
| AST/SC 5 | | | | | | | | | | | |
| AST/SC 4 | | | | | | | | | | | |
| AST/SC 3 | | | | | | | | | | | |
| AST/SC 2 | | | | | | | | | | | |
| AST/SC 1 | | | | | | | | | | | |
| AST/SC TOTAL | | | | | | | | | | | |
| TOTAL | | 82 | | 80 | | 82 | | 83 | | 83 | 83 |
| GRAND TOTAL | | 82 | | 80 | | 82 | | 83 | | 83 | 83 |

External personnel

Contract Agents

| Contract agents | FTE corresponding to the authorised budget 2023 | Executed FTE as of 31/12/2023 | FTE corresponding to the authorised budget 2024 | FTE corresponding to the envisaged budget 2025 | FTE corresponding to the envisaged budget 2026 | FTE corresponding to the envisaged budget 2027 |
|--------------------|---|-------------------------------|---|--|--|--|
| Function Group IV | 30 | 18 | 30 + 11 under contribution agreement | 30 + 11 under contribution agreement | 30 + 10 under contribution agreement | 30 |
| 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 | 25 | 43 | 43 | 42 | 32 |

Seconded National Experts

| Seconded National Experts | FTE corresponding to the authorised budget 2023 | Executed FTE as of 31/12/2023 | FTE corresponding to the authorised budget 2024 | FTE corresponding to the envisaged budget 2025 | FTE corresponding to the envisaged budget 2026 | FTE corresponding to the envisaged budget 2027 |
|---------------------------|---|-------------------------------|---|--|--|--|
| TOTAL | 14 | 8 | 14 | 15 | 15 | 15 |

Table 3: Recruitment forecasts for 2025 following retirement or mobility or new requested posts

| Job title in the agency | Type of contract (official, TA or CA) | | TA/official | | CA | |
|-------------------------|---------------------------------------|--|--|---------------------|---------------------|--|
| | Due to foreseen retirement/mobility | New post requested due to additional Tasks ⁴³ | Function group/grade of recruitment internal (brackets) and external (single grade) foreseen for publication * | Internal (brackets) | External (brackets) | Recruitment function group (i, ii, iii and iv) |
| Expert | 1 TA | n/a | n/a | 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 |

43 - Posts stemming from the required resources for the 2025 work programme (11.5 FTEs).

ANNEX 5

HUMAN RESOURCES – QUALITATIVE

A. RECRUITMENT POLICY

Implementing rules in place

| | | Yes | No | If no, which other implementing rules are in place? |
|--------------------------|----------------------------|-----|----|---|
| Engagement of CAs | Model Decision C(2019)3016 | x | | |
| Engagement of TAs | 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 TAs | Model Decision C(2015)9560 | x | | |
| Reclassification of CAs | Model Decision C(2015)9561 | x | | |

Table 1: Reclassification of TA or promotion of official

| Average seniority in the grade among reclassified staff | | | | | | | | |
|---|-----------|-----------|-----------|-----------|-----------|-----------|-----------------------------|--|
| Grades | Year 2018 | Year 2019 | Year 2020 | Year 2021 | Year 2022 | Year 2023 | Actual average over 5 years | Average over 5 years (According to decision C(2015)9563) |
| AD05 | - | - | - | - | - | - | - | 2.8 |
| AD06 | 2 | 3 | - | 1 | 1 | 1 | 3.5 | 2.8 |
| AD07 | - | - | 1 | - | 2 | 1 | 4 | 2.8 |
| AD08 | 1 | 1 | 2 | 1 | 3 | 1 | 3.9 | 3 |
| AD09 | 1 | - | - | - | - | 2 | 6.4 | 4 |
| AD10 | - | - | - | - | 2 | - | 10.5 | 4 |
| AD11 | - | - | - | - | - | - | - | 4 |
| AD12 | - | - | - | 1 | - | - | 10 | 6.7 |
| AD13 | - | - | - | - | - | - | - | 6.7 |
| AST1 | - | - | - | - | - | - | - | 3 |
| AST2 | - | - | - | - | - | - | - | 3 |
| AST3 | 1 | 1 | - | - | 1 | - | 5.2 | 3 |
| AST4 | 1 | 1 | 1 | - | - | 1 | 3.3 | 3 |
| AST5 | 1 | - | - | 1 | - | 1 | 5.3 | 4 |
| AST6 | - | - | 1 | 1 | - | - | 3.5 | 4 |
| AST7 | - | - | - | 1 | 1 | 1 | 4 | 4 |
| AST8 | - | - | - | - | - | - | - | 4 |
| AST9 | - | - | - | - | - | - | - | N/A |
| AST10 (Senior assistant) | - | - | - | - | - | - | - | 5 |
| There are currently no AST/SCs at ENISA: n/a | | | | | | | | |
| AST/SC1 | | | | | | | | 4 |
| AST/SC2 | | | | | | | | 5 |
| AST/SC3 | | | | | | | | 5.9 |
| AST/SC4 | | | | | | | | 6.7 |
| AST/SC5 | | | | | | | | 8.3 |

Table 2: Reclassification of contract staff

| Function group | Grade | Staff in activity at 31.12.2023 | Average number of years in grade of reclassified staff members | Average number of years in grade of reclassified staff members | Average number of years in grade of reclassified staff members according to decision c(2015)9561 |
|----------------|-------|---------------------------------|--|--|--|
| CA IV | 17 | 1 | - | - | Between 6 and 10 years |
| | 16 | 6 | - | - | Between 5 and 7 years |
| | 15 | 3 | 2 | 4.5 | Between 4 and 6 years |
| | 14 | 6 | 1 | 5.3 | Between 3 and 5 years |
| | 13 | 2 | - | - | Between 3 and 5 years |
| CA III | 12 | 1 | - | - | - |
| | 11 | 2 | - | - | Between 6 and 10 years |
| | 10 | 3 | - | - | Between 5 and 7 years |
| | 9 | 0 | - | - | Between 4 and 6 years |
| | 8 | 0 | - | - | Between 3 and 5 years |
| CA II | 6 | - | - | - | Between 6 and 10 years |
| | 5 | - | - | - | Between 5 and 7 years |
| | 4 | - | - | - | Between 3 and 5 years |
| CA I | 3 | 1 | - | - | n/a |
| | 2 | - | - | - | Between 6 and 10 years |
| | 1 | - | - | - | Between 3 and 5 years |

C. GENDER REPRESENTATION

Table 1: Data as at 31.12.2023 on statutory staff (only temporary agents and contract agents)

| | | Official | | TAs | | CA | | Grand total | |
|--------------------|----------------------------------|----------|---|-------|-------|-------|-------|-------------|-------|
| | | Staff | % | Staff | % | Staff | % | Staff | % |
| Female | Administrator level | - | - | 23 | 29 % | 11 | 41 % | 34 | 32 % |
| | Assistant level (AST and AST/SC) | - | - | 13 | 16 % | 4 | 16 % | 17 | 16 % |
| | Total | - | - | 36 | 45 % | 15 | 60 % | 51 | 48 % |
| Male | Administrator level | - | - | 39 | 49 % | 7 | 28 % | 46 | 44 % |
| | Assistant level (AST and AST/SC) | - | - | 5 | 6 % | 3 | 12 % | 8 | 8 % |
| | Total | - | - | 44 | 55 % | 10 | 40 % | 54 | 51 % |
| Grand total | | - | - | 80 | 100 % | 25 | 100 % | 105 | 100 % |

Table 2: Data regarding gender evolution over 5 years on middle and senior management (31.12.2023)

| | 2019 | | 31.12.2023 | |
|-----------------|--------|-----|------------|-----|
| | Number | % | Number | % |
| Female Managers | 2 | 20% | 2 | 29% |
| Male Managers | 8 | 80% | 5 | 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 last 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 coming years.

D. GEOGRAPHICAL BALANCE

Table 1: Data as at 31.12.2023 - 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 | 5 | 6% | 1 | 4% | 6 | 6% |
| BG | 2 | 3% | 0 | 0% | 2 | 2% |
| CY | 2 | 3% | 2 | 8% | 4 | 4% |
| CZ | 1 | 1% | 0 | 0% | 1 | 1% |
| DE | 1 | 1% | 0 | 0% | 1 | 1% |
| Double ⁴⁴ | 6 | 8% | 3 | 12% | 9 | 9% |
| EE | 1 | 1% | 0 | 0% | 1 | 1% |
| ES | 3 | 4% | 0 | 0% | 3 | 3% |
| FR | 6 | 8% | 1 | 4% | 7 | 7% |
| EL | 32 | 40% | 13 | 52% | 45 | 43% |
| IT | 6 | 8% | 0 | 0% | 6 | 6% |
| LT | 2 | 3% | 1 | 4% | 3 | 3% |
| LV | 2 | 3% | 0 | 0% | 2 | 2% |
| NL | 2 | 3% | 0 | 0% | 2 | 2% |
| PL | 1 | 1% | 1 | 4% | 2 | 2% |
| PT | 3 | 4% | 1 | 4% | 4 | 4% |
| RO | 5 | 6% | 1 | 4% | 6 | 6% |
| SE | 0 | 0% | 0 | 0% | 0 | 0% |
| SK | 0 | 0% | 1 | 4% | 1 | 1% |
| TOTAL | 80 | 100% | 25 | 100% | 105 | 100% |

Table 2. Evolution over 5 years of the most represented nationality in the agency

| Most represented nationality | 2019 | | 31.12.2023 | |
|------------------------------|----------------|----|-----------------|----|
| | Number | % | Number | % |
| Greek | 29 (out of 73) | 40 | 45 (out of 105) | 43 |

E. SCHOOLING

| Agreement in place with the European School of Heraklion | |
|--|-----|
| Contribution agreements signed with the Commission on type I European Schools | NO |
| Contribution agreements signed with the Commission on type II European Schools | YES |

44 - Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.)

ANNEX 6

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 an exercise in 2022 to map its current climate footprint by conducting an 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 during the 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 were undertaken during the course of 2024. The Agency expects to acquire an EMAS certificate towards the end of 2024.

- ENISA, with the assistance of an external contractor, completed a technical study for the calculation of its carbon footprint in 2022 and is working towards assessing its 2023 carbon footprint in Q4 2024.
- Several actions for the reduction of GHGs emissions were further implemented. These included the recycling of office waste in a structured manner (via dedicated recycling bins and guidelines on the proper use of the bins), the improvement of the watering system, the incorporation of provisions on GHG’s emissions into the agency’s public procurement procedures and tenders, awareness raising sessions and dedicated training to all staff about EMAS and the Agency’s greening initiatives.
- During the course of 2024 the registration and implementation of an environmental

management system (according to EMAS regulations) took place with the creation of EMS (European Management System) templates and procedures.

- An internal audit and evaluation of ENISA’s environmental performance also took place during 2024.
- In addition, the Agency proceeded to the drafting of its environmental statement for which formal approval by ENISA’s management Team is anticipated in Q4 of 2024.
- An external verification of these environmental matters is to be concluded during the course of Q4 2024.
- External communications through ENISA’s website about EMAS and the Agency’s greening initiatives are expected in Q4 2024 and Q1 2025.

Planned actions for 2025

- An assessment of the Agency’s carbon footprint for 2024.
- A call for volunteers to join members of the Agency’s renewed greening network.
- The continuation of awareness raising actions (i.e. repeat training for staff members, dedicated Q&As being made available to staff, multi-purpose cups made out of recycled materials etc.)

Additionally, the Agency aims to reduce greenhouse gas emissions in alignment with the approach taken by the Commission⁴⁵. The corporate strategy outlines objectives to decrease the number of in-person events and participation in physical gatherings, favouring hybrid or online formats instead.

45 - Communication to the Commission - Greening the Commission | European Commission (europa.eu)

ANNEX 7

BUILDING POLICY

CURRENT BUILDINGS

| Building name and type | Location | Location surface area (in m ²) | | | Rental contract | | | Host country (grant or support) | Building present value (EUR) |
|-------------------------|------------------------|--|------------------------------|-------------------------|---------------------|---------------------------|--------------|---|------------------------------|
| | | Office space (m ²) | non-office (m ²) | Total (m ²) | Rent (EUR 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 | 4 498 | 2 617 | 7 115 | | 01/01/2021 to 28/02/2030; | Lease | Rent is fully covered by Hellenic authorities | n/a |
| Brussels office | Brussels centre | 98 | | 98 | 56 496 | N/a | SLA with OIB | | n/a |
| Total | Location | 5 302 | 2 617 | 7 920 | | | | | |

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. The objective of the second implementation phase, which is currently ongoing, is to obtain accreditation for the secure room, which will enable the agency to handle EU Classified Information (EUCI) in its Brussels premises. The second phase of implementation is likely to continue into Q4 2024. Indicative resources foreseen:

| Resources (indicative) | 2025 | 2026 | 2027 |
|--|---------|---------|---------|
| Head count (FTEs) | 12–13 | 13–14 | 13–14 |
| Budget (one-off and maintenance costs) | 130 000 | 130 000 | 130 000 |

ANNEX 8

PRIVILEGES AND IMMUNITIES

| Agency privileges | Privileges granted to staff | |
|--|--|--|
| | Protocol of privileges and immunities / diplomatic status | Education/day care |
| <p>In accordance with Article 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, 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 on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered in to force on 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, 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 on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered in to force on 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> |

ANNEX 9

EVALUATIONS

In 2023, the Agency conducted a stakeholder satisfaction survey to gather feedback on the outcomes or results of ENISA's work over the previous two reporting periods (2021 and 2022). The next stakeholder satisfaction survey for the period 2023 to 2024 will be carried out in Q1 2025. This survey, as in 2023, will seek to assess the satisfaction levels of stakeholders in relation to the way the Agency implements its projects, specifically how work is organised and managed and how the feedback from external stakeholders is taken into account. The results of the stakeholder satisfaction survey should shed much important light on how stakeholders perceive the added value of ENISA's work.

On aggregate, the results of the 2023 survey demonstrated that ENISA's deliverables have a high added value with 93% of stakeholders finding significant added value in the outcomes or results of the Agency's work. Only 7% found limited added value and no stakeholder found no added value. In terms of take up, 85% of stakeholders also rated the likelihood of their taking up the results of ENISA's work to support their own tasks in the immediate to medium term, of which the operational cooperation activities 4 and 5 scored the highest in terms of immediate take up (50%) which, given the nature of these activities, is a good result.

In addition, the mandate of the Agency requires that it carries out its tasks while avoiding duplication of Member States' own activities. Therefore the result of the 2023 survey, that 83.7% of stakeholders find that ENISA deliverables do not duplicate or only somewhat duplicate Member States' own activities, is tantamount to saying that ENISA's efforts to involve stakeholders in all stages of its work and ensure that the outcomes or results are fit for purpose have been successful. However, duplication in some areas is unavoidable due to the nature of the work and the need for MSs to have their own capacities. ENISA will take action to increase efforts to focus its work even more on high added-value and low duplication areas and will introduce specific targets to its work programme to reduce duplication of the activities of Member States.

The aggregate results of the survey are among the KPI results reported under operational activities

ANNEX 10

STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

As adopted by the Management Board⁴⁶, the Agency's strategy for effective internal controls is based on international practices (COSO Framework's International Standards) as well as the relevant internal control framework of the European Commission.

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

Risk assessment is the Agency's dynamic and iterative process for identifying and assessing risks that 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 the 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 the segregation of duties.

Information is necessary for the Agency to carry out internal controls and to support the achievement of objectives. In this respect, both external and internal communication need to be considered. External communication provides the Agency's stakeholders and EU citizens with information on ENISA's policies, objectives, actions and achievements. Internal communication provides ENISA staff with the

information required to support the achievement of objectives and their awareness of 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, in 2022 ENISA conducted a thorough review of the indicators of its internal control framework 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 the assessment of enterprise risk across the Agency.

Moreover, since 2021, ENISA has been implementing its anti-fraud strategy⁴⁷, which was adopted in line with the recommendations of the European Anti-Fraud Office (OLAF).

ENISA is currently updating its anti-fraud strategy in close consultation with OLAF and aims to present it to the MB at the beginning of 2025 for endorsement.

46 - See MB Decision 12/2019 (<https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202019-12%20on%20internal%20controls%20framework.pdf>) and MB Decision 11/2022 (<https://inet/lib/mbd/MBD%202022-11%20amending%20MBD%202019-12%20on%20Internal%20Controls%20Framework.pdf>).

47 - <https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-5-on-anti-fraud-strategy>.

ANNEX 11

PLAN FOR GRANT, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS

| | SLA | Date of signature | Total amount | Duration | Counter-part | Short description | FTEs |
|---|-------------------------------|-------------------|--------------|----------------|--------------|---|----------|
| 1 | SLA with ECCC | 20/12/22 | 54 604 | 1 year | ECCC | The scope of this Service Level Agreement covers support services offered by ENISA to ECCC: data protection officer, accounting officer | 0.4 FTEs |
| 2 | SLA with eu-LISA M-CBU-23-C35 | 13/7/23 | 120 000 | Up to 31/12/23 | 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 exercises. | 2 FTEs |

Contribution agreements

| | | | | | | | |
|---|--|------------|--------------------------------------|----------------|----------|--|---------|
| 1 | Support Action fund | 21/12/2023 | Up to 20 million (80% pre-financing) | Up to 31/12/26 | DG CNECT | The purpose of this Agreement is to provide a financial contribution to implement the action 'Incident Response Support and Preparedness for Key Sectors' which is composed of three activities: 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. | 11 FTEs |
| 2 | Support Action fund (activities 5 & 6) | Pending | Up to 15 million | 2025 to 2027 | DG CNECT | EU-level cyber reserve with services from trusted private providers for incident response • Contribution to the Cyber Analysis and Situation Centre • Establishment of the Cyber Resilience Act single reporting platform • Management and maintenance of day-to-day operations of the Cyber Resilience Act single reporting platform. | TBD |
| 3 | CRA single reporting platform | Pending | Up to 400 000 | 2025 to 2026 | DG CNECT | The purpose of this Agreement is to provide the organisation with a financial contribution to conduct a feasibility study on the single reporting platform under the Cyber Resilience Act that will inform the future steps for the development of the platform. | 2 FTEs |

ANNEX 12

STRATEGY FOR COOPERATION WITH NON-EU COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

The international strategy confirms the Agency's mandate in terms of its 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 strategy 50 was adopted by the MB during its November 2021 meeting.

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.

ANNEX 13

ANNUAL COOPERATION PLAN 2025



The 2025 Annual Cooperation Plan between ENISA, the EU Agency for Cybersecurity, and CERT-EU, the Computer Emergency Response Team for EU institutions, bodies and agencies, will be annexed to the Single Programming Document 2025-2027 as a separate document.

ANNEX 14

PROCUREMENT PLAN 2025

The indicative procedures from the ENISA budget (Title 1, 2 and 3) for public contracts to be launched in 2025 are detailed as follows:

| ENISA UNIT | TITLE of Contract | TYPE of procedure | Tender launch | Contract signature | Total budget est. 4 years EUR |
|---------------------------------------|---|----------------------|---------------|--------------------|-------------------------------|
| Corporate Support services | Security guard services | Restricted procedure | Q1 2025 | 10.05.2025 | 900 000.00 |
| Corporate Support services | Mobile Voice and Data services | Open procedure | Q1 2025 | 30.05.2025 | 320 000.00 |
| Corporate Support services | SIP landline voice telephony services | Open procedure | Q1 2025 | 30.05.2025 | 80 000.00 |
| Corporate Support services | Maintenance of safety and security systems | Open procedure | Q2 2025 | 10.07.2025 | 150 000.00 |
| Executive Director's Office | Digital Communications services | Open procedure | Q3 2025 | 01.12.2025 | 400 000.00 |
| Resilience of Critical Sectors | Supporting activities in the areas of electronic identification, trust services and digital wallets | Open procedure | Q3 2025 | 20.01.2026 | 600 000.00 |

The total indicative budget reserved for procurement during 2025 is EUR 10 634 702.

NOTES



NOTES



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: 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

Brussels Office

Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu



Publications Office
of the European Union

