MANAGEMENT BOARD DECISION

DECISION No MB/2024/16

OF THE ENISA MANAGEMENT BOARD

of 14 November 2024,

on adopting the Single Programming Document (SPD) 2025-2027, the statement of estimates for 2025 and the establishment plan for 2025

THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

Having regard to

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), in particular Article 15.1.(c), Article 24.3., Article 24.4., and Article 29.7
- Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council
- Commission Opinion No. 7174 on the draft Single Programming Document for 2025 – 2027 of ENISA dated 14.10.2024
- Commission Communication C(2014) 9641 final, on the guidelines for programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies dated 16.12.2014

Whereas

(1) The Single Programming Document 2025-2027 should be adopted by the Management Board by 30 November 2024.

(2) The Single Programming Document 2025 -2027 was scrutinised by the Executive Board on 17-18 October 2024.

(3) The Single Programming Document of the Agency should be forwarded to the Member States, the European Parliament, the Council and the Commission following adoption;

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2025-2027 is adopted as set out in the Annex 1 of this decision.

Article 2

The statement of estimates of revenue and expenditure for the financial year 2025 and the establishment plan 2025 is adopted as set-out in Annex 2 and Annex 3 of this decision. They shall become final following the definitive adoption of the general budget of the Union for the financial year 2025.

Article 3

Where necessary, the Management Board shall adjust ENISAs Single Programming Document 2025-2027 and ENISA's budget and the establishment plan in accordance with the general budget of the Union for the financial year 2025.

Article 4

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

Done in Athens, 14 November 2024

On behalf of the Management Board,

[signed]

Ms Fabienne Tegeler
Chair of the Management Board of ENISA

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2025-2027

Including Multiannual planning, Work programme 2025 and Multiannual staff planning

VERSION: ADOPTED

TABLE OF CONTENTS

SECTION I. GENERAL CONTEXT 7

SECTION II. MULTI-ANNUAL PROGRAMMING 2025 – 2027 11

1. Multi-annual work programme 11
2. HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2025-2027 16
2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION 16
2.2 . OUTLOOK FOR THE YEARS 2025-2027 21
2.3 RESOURCE PROGRAMMING FOR THE YEARS 2025-2027 22
2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS 25

SECTION III. WORK PROGRAMME 2025 27

3.1 OPERATIONAL ACTIVITIES 28
3.2 CORPORATE ACTIVITIES 56

ANNEX66

I. ORGANISATION CHART AS OF 01.12.2022 66

II. RESOURCE ALLOCATION PER ACTIVITY 2025 - 2027 69

III. FINANCIAL RESOURCES 2025 - 2027 71

IV. HUMAN RESOURCES - QUANTITATIVE 72

V. HUMAN RESOURCES - QUALITATIVE 77

VI. ENVIRONMENT MANAGEMENT 82

VII. BUILDING POLICY 83

VIII. PRIVILEGES AND IMMUNITIES 83

IX. EVALUATIONS 84

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS 84

XI. PLAN FOR GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENTS 86

XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS87

XIII. ANNUAL COOPERATION PLAN 2025 87

XIV. PROCUREMENT PLAN 87

LIST OF ACRONYMS

To be updated during proof reading & editing

ABAC	Accruals-based accounting
ACER	Agency for the Cooperation of Energy Regulators
AD	Administrator
AST	Assistant
BEREC	Body of European Regulators for Electronic Communications
CA	Contract agenda
CAB	Conformity Assessment Body
Cedefop	European Centre for the Development of Vocational Training
CEF	Connecting Europe Facility
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT-EU	Computer Emergency Response Team for EU institutions, bodies and agencies
COVID-19	Coronavirus disease 2019
CSA	Cybersecurity Act
CSIRT	Computer Security Incidence Response Team
CTI	Cyber threat intelligence
CRA	Cyber Resilience Act
CSoA	Cyber Solidarity Act
CSPO	Cybersecurity Policy Observatory
EU-CyCLO-Ne	Cyber Crisis Liaison Organisation Network
DORA	Digital Operational Resilience Act (DORA)
DSP	Digital service providers
DSO	European Distribution System Operators
ECA	European Court of Auditors
EC3	European Cybercrime Centre
ECCC	European Cybersecurity Competence Centre
EUCS	EU Cloud Certification Scheme
ECCG	European Cybersecurity Certification Group
EDA	European Defence Agency
EEAS	European External Action Service
EECC	European Electronic Communications Code
EFTA	European Free Trade Association
eID	Electronic identification
eIDAS	Electronic Identification and Trust Services (eIDAS) Regulation
ENISA	European Union Agency for Cybersecurity
ENTSO	European Network of Transmission System Operators for Electricity
ETSI	European Telecommunications Standards Institute
EUCC	European Union Common Criteria scheme
EU5G	European Union certification scheme for 5G networks
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
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
MFF	Multi-annual financial framework
MoU	Memorandum of understanding
NIS	Networks and Information Systems
NISD	NIS Directive
NIS2	NIS2 Directive
NIS CG	NIS Cooperation Group

NLO	National Liaison Officers
OOTS	The Once Only Technical System
SC	Secretary
SCCG	Stakeholder Cybersecurity Certification Group
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises
SNE	Seconded national expert
SOCs	Security Operation Centres
SOP	Standard Operating Procedure
SPD	Single Programming Document
TA	Temporary agent

INTRODUCTION

FOREWORD

In today's interconnected world, the criticality of cybersecurity cannot be overstated. The European Union, home to over 500 million citizens and some of the world's most advanced economies, faces a growing number of cyber threats by malicious cyber actors. Cyber perpetrators can target everything and everyone in our hyperconnected world. The digital evolution has clearly brought immense opportunities for our economy and society but also heightened vulnerabilities and new threats, which often challenge our security.

The EU has taken bold policy steps to strengthen our cybersecurity preparedness and resilience and had developed an advanced and modern legal framework, aiming to protect our economy, society and our everyday life across Europe, becoming a global front runner in this domain. EU has also weaved a robust cybersecurity ecosystem to shield its economy and society against cyber and hybrid threats. The European Union Agency for cybersecurity (ENISA) plays a central role in this policy framework and even more critical role in supporting EU's cybersecurity ecosystem. ENISA actively contributes to EU's cybersecurity resilience and supports Europe in advancing its cybersecurity capabilities.

As the threat landscape continues to evolve, the Agency's commitment to assist EU in building a more secure digital future for all Europeans is more essential than ever. Through cooperation with private and public organizations, the different cyber communities as well as through synergies with international like-minded partners, ENISA strives to ensure a secure and trusted digital environment for all doing businesses or residing in Europe; ENISA is devoted to strengthening cybersecurity across Europe and especially in nowadays complex geopolitical context.

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

Firstly, the Agency's strategy was revised by the Management Board in 2024 to further clarify and amend its priorities and focus, including the introduction of new indicators to measure the success of its strategic objectives. The seven strategic objectives were refined and realigned to better highlight the critical success factors for each one. At the same time, the Agency streamlined its operational activities, reducing them from 10 to 8, and adjusted its organizational structure to more effectively manage these activities and step up its capacity to deliver more efficiently.

Secondly, approximately half of ENISA's operational resources, both budget and human resources, will be dedicated to enabling operational cooperation and providing effective operational cooperation through dynamic and improved situational awareness. The contribution agreement of 20 million EUR from the EU budget, which the European Commission entrusted to ENISA to manage in Autumn 2023, will allow the Agency to massively scale up and expand its support to EU Member States in 2025 and 2026. 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-programme ENISA has strengthened its capabilities and capacities in supporting EU Member States and beyond with the implementation of the NIS2 Directive, the Cyber Resilience Act and the Cyber Solidarity Act, as well as to prepare the ground for the roll-out and implementation of the EU cybersecurity certification schemes. Finally, the first ever report on the state of cybersecurity in the EU, which the NIS2 Directive requires ENISA to deliver, will enable the Agency to direct its focus to the areas which matter most for achieving its aspiration for a high common level of cybersecurity across Europe.

MISSION STATEMENT

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

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

ENISA STRATEGY[1]

Horizontal objectives:

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

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

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

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

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

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

Vertical objectives:

[1] The ENISA strategy, its strategic objectives and indicators is pending endorsement by the MB in the November 2024 meeting.

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

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

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

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

Strategic objective: "Strong cyber security capacity within EU"

The frequency and sophistication of cyberattacks is on a steady rise, while at the same time the use of digital infrastructures and technologies is increasing rapidly. The needs for cybersecurity skills, knowledge and competences exceeds the supply. EU is investing in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional and across all sectors and age groups. ENISA address capacity building across the spectrum: start by investing in youth through competence building and training, whilst providing continuous up- and reskilling opportunities to professionals, to keep up with the fast-changing nature of cybersecurity. The focus is not only on increasing the cybersecurity skillset in the Member States and contributing to the objectives of the Cybersecurity Skills Academy, but also on making sure that the different operational communities always possess the appropriate capacity to deal with the cyber threat landscape. Engaging closely with key players and multipliers in the EU is crucial to ensure adequate preparedness across sectors and borders, effectively utilising the lessons learned from well-planned exercises.

Strategic objective: "Building trust in secure digital solutions"

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

.

SECTION I. GENERAL CONTEXT

The Single Programming Document sets outs the activities that ENISA will undertake in the years 2025 to 2027 in accordance with the Agency's founding Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act)[2] and takes into account the new ENISA 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 market by 2027. NIS2 entered into force in January 2023 and reaches the transposition deadline on 17 October 2024. The NIS2 Directive introduces legal measures to enhance cybersecurity across the EU, imposing obligations on entities in 18 economic sectors, particularly regarding security requirements and incident notifications. 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 formalizes 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 the NIS2 at national level, including the implementation of the EU vulnerability database and the registry for digital entities, to support cross border collaboration, including the peer reviews, as well as to publish the report 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 prioritized from 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 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 single reporting platform for these notifications, to prepare the 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 activities.

The (CSOA) is expected to take 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 better detection, preparation, and response to significant or large-scale cybersecurity incidents: the European Cybersecurity Alert System (a pan-European Network of Cyber Hubs), the Cybersecurity Emergency Mechanism, and the European Cybersecurity Incident Review Mechanism. ENISA shall 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 with 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 upon EC request an EU scheme for the EUDI wallet; in addition, ENISA has assisted the EC in developing the Implement Act on certification and is foreseen to continue this collaboration in assisting MSs 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 of the Union (Union entities) has been adopted in 2023 and entered into force on 7 January 2024.

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

[2] Regulation (EU) 2019/881

A number of sector-specific cybersecurity initiatives, include:

o Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) entered into force on 16 January 2023.

o Commission Delegated Regulation (EU) 2022/1645 and Commission Implementing Regulation (EU) 2023/203 were adopted in 2022 in the aviation sector.

o The Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS) which 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 for the cybersecurity realm, include, 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 where the EU is making a difference in cybersecurity, as such 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 according to Art. 67 of the CSA.
NIS2 Directive	Implementation	The Commission is gathering input on the draft implementing act under the NIS2 Directive, which aims to ensure a high common level of cybersecurity across the Union. By 27th October 2024, the Commission plans to adopt 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.

Threat landscape

The ENISA Threat Landscape 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 delves 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 detailed analysis of four distinct threat actors' categories, 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 organizations in public administration (19%), transport (11%), and finance (9%) sectors.

International developments
Building on the developments of the past 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 Art.12 of the CSA. In the last years, ENISA has focused on the outreach cooperation with Ukraine, 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 aimed 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 of the Digital Europe Programme to 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 ENISA Cybersecurity Support Action implementation 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 Cybersecurity Support Action, ENISA has developed the necessary know-how and tools to deliver both ex-ante and ex-post cybersecurity services in collaboration with EU service providers, which the EU Member States have the possibility to utilise. When the Cyber Solidarity Act will enter 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.

Implementation of the EU 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 the National Cybersecurity Certification Authorities (NCCAs) across the MS. 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. When the consolidated opinion will be 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). Other schemes requests are likely to follow in line with the Union Rolling Work Programme (URWP), in particular on managed security services.

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

The adopted schemes and those under preparation will also be mapped with the requirements of the CRA to provide the means for the conformity assessment of digital products, services and processes in the digital single market, in a way that ensures compliance with the CRA requirements. 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 related to the CRA technical descriptions of products.

ENISA will also support the development of certification means 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 the 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 editions of the programme.

EU crisis management framework

The 2017 Cybersecurity Blueprint describes a framework of 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 the call from the Council for such a blueprint, given that the 2016 NIS Directive did not provide for a Union cooperation framework in case of large-scale cybersecurity incidents and crises.

The Cybersecurity Blueprint proposed a concept and a definition of large-scale cybersecurity incidents which became the basis for the definition of 'large-scale cybersecurity incident' in the NIS2 Directive, which established formally 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 level during large-scale cybersecurity incidents and crises and should enhance cooperation at operational level and support decision-making at 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 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 complex cyber threat landscape and expand the current principles them to the full crisis management lifecycle, and that the role of ENISA, along with that of the role of the Commission, the High Representative and ENISA, in line with their competences, should focus in particular on supporting horizontal coordination.”

Cyber defence policy

The Council conclusions of 22 May 2023 on the EU policy on cyber defence emphasize 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 specialized training programs, 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 cybersecurity workforce skills gap. The academy aims at fostering knowledge generation through education and training by working on a common language on cybersecurity role profiles and associated skills, namely the European cybersecurity skills framework (ECSF), and also including pilots for attestation schemes for cybersecurity competences; ensuring a better channelling and visibility of available funding opportunities for skills-related activities in order to maximise their impact; calling on stakeholders to take action by making concrete cybersecurity pledges and integrating cybersecurity skills into their national strategies; defining indicators to monitor the evolution of the market and to better address the needs on one hand, and on the other, the offer of training, as well as the better directing of funds towards cybersecurity needs. ENISA plays a valuable role in the implementation of the academy tasks outlined, all in collaboration with relevant stakeholders, namely the European Cybersecurity Competence Centre (ECCC), the National Competence Centres, the NIS CG and others. The recent Eurobaromoter survey[3] on skills confirmed the need for EU to reinforce cybersecurity skills due to the cyber skills shortage increasing, thus requiring more cybersecurity specialists and the need to increase the number of highly cybersecurity-aware staff in every company across the EU.

[3] Eurobarometer survey confirms EU must reinforce cybersecurity skills | Shaping Europe’s digital future (europa.eu)

SECTION II. MULTI-ANNUAL PROGRAMMING 2025 – 2027

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA reviewed and updated ENISA's strategy[4] in June 2024, which builds on the Cybersecurity Act (CSA), and outlines how the Agency will strive to meet the expectation of the cybersecurity ecosystem in a medium to long-term perspective, in a manner that is open, innovative, agile as well as being socially and environmentally responsible. The strategy sets out a vision of "A trusted and cyber secure Europe" in which all citizens and organisations of Europe not only benefit but are also key components in the effort to secure Europe. Most importantly, the ENISA strategy outlines three horizontal strategic objectives and four vertical strategic objectives which are derived from the CSA and set the expected medium to long-term goals for the Agency.

1. Multi-annual work programme

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

Strategic objectives		Vertical strategic objectives			
		Effective and consistent EU policies implementation for EU cybersecurity policy	**Effective Union preparedness and response to cyber incidents, threats, and cyber crises**	**Strong cyber security capacity within EU**	**Building trust in secure digital solutions**
Horizontal strategic objectives	**Empowered communities in an involved and engaged cyber ecosystem**	Uptake of ENISA recommendations to support Member States and stakeholders in implementing EU legislation	Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks	Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings)	Number of EU certification schemes developed and maintained, number EU regulations making reference to CSA, number of active Member States' NCCAs (e.g. issuing European certificates)
	Foresight on emerging and future cybersecurity opportunities and challenges	Number of identified future and emerging areas reflected in the policy initiatives and interventions	Operationalisation of the EU Cybersecurity Reserve of which administration and operation is to be entrusted fully or partly to ENISA and used by MS, EUIBAs and on a case by case basis DEP associated third countries	Number of advise and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC	Rate of satisfaction with ENISA's support to the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG)

[4] Pending approval at the MB November 2024 meeting

	Consolidated and shared cybersecurity information and knowledge support for Europe	Uptake of recommendations stemming from NIS2 Art. 18 report	EU Vulnerability Database is operationalised by ENISA and a satisfaction rate (by MS and stakeholders) with ENISA ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats	Percentage of MS that use ECSF	Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and successfully operated

ENISA Corporate Strategy

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

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

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

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

The table below highlights the responsible activity for each corporate objective from the Corporate Strategy including the key goals and means to measure the associated Key Performance Indicators (KPIs). This will be reviewed on the basis of first year results of the Corporate Strategy (including results from the 2023 Staff Satisfaction Survey) to be reported under 2023 annual activity report. In addition to these principles for resourcing the objectives have been taken into consideration when developing the budget.

STRATEGIC DIMENSION	OBJECTIVES	ACTIVITY'S TO ACHIEVE OBJECTIVES	KEY GOALS (KPIS/MEANS TO MEASURE THE KPIS)
People centric organisation	Effective workforce planning and management	Activity 11	• Agency's internal workforce needs for the year n until n+2 are defined and presented to the MB together with the first draft SPD for those years as per annual/internal procedures. • Effective FTEs used for SPD activities (as reported in AAR by end of year n) do not diverge from planned FTEs in SPD (as endorsed by MB in the beginning of year n) by more than 5% according to annual/internal procedures. • 95% of Agency's staffing posts (TA, CA, SNE) are fulfilled by the end of year according to its annual recruitment results. • Vacated staff posts are fulfilled in less than 300 days according to its annual recruitment results. • All assignments of staff are reviewed regularly every three years during the Agency's annual/internal procedures. • Aggregate loss of FTE across the Agency due to absences (excluding long-term sick leave) is less than three FTEs annually during its annual/internal process.
	Efficient talent acquisition, development and retainment	Activity 11	• 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	• 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	Activity 9 & 11	• 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	Activity 9 & 11	• Implement (replace or develop) at least five user-centered, cloud-based, corporate solutions or tools fit for purpose and in line with ENISA's IT strategy and relevant business needs by Q4 2025. • Limited disruption of continuity of services across all corporate support service areas measured by annual assessment. • To have IT support service standards as technical KPIs in place by Q2 2025 and to have them continuously monitored and observed, to support the maintenance and development of operational IT systems through an annual review. • All on-premises systems are maintained within risk levels established by the business owners and all corrective measures recommended by periodic risk assessments are implemented as found in an annual review.
	Continuous innovation and service excellence	Activity 9	• The percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have not been reviewed less than three years ago as found by an annual review. Percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have been last reviewed more than four years ago as found in an annual review.
	Developing service propositions with additional external resourcing	Activity 9 & 11	• 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	• Acquire an EMAS certificate by Q1 2024. • 50% of participants in ENISA's organised events and meetings to participate online by 2025, rising to 75% by 2030. • 50% of ENISA events and meetings to be organised as hybrid or online by 2025, rising to 75% by 2030. • Initiate and by end 2024 agree a tripartite MoU with the Hellenic Authorities and the landlord of ENISA HQ building to reduce the climate impact of the HQ building at least 40% by 2029, by installing solar panels on the

			non-classified part of the building or procure a green building for the Agency by then. • Offset all residual emissions generated through ENISA operations from 2024 onwards
	Promote and enhance ecologic sustainability across all the Agency's operations	Activity 9 & 11	• Recycle all ENISA residual waste created in its HQ and local offices by 2025. • Implement ecological sustainability and climate neutrality criteria for procuring event management and support and for facilities management and support services from external contractors by 2025. • Implement ecological sustainability and climate neutrality criteria for all ENISA tenders for corporate service contractors by 2027 and by 2029 for operational activities. • Understand best practices in sustainable IT solutions, define an agency-wide approach and include it in the IT Strategy.
	Develop efficient framework for continuous governance to safeguard high level of IT and physical security	Activity 9 & 11	• Review the Agency's IT strategy and align it with the objectives of the corporate strategy by Q3 2024. • Set in place a relevant policy for security compliance for IT and for physical security (including for required EUCI levels) for all relevant internal and external services with a high level of adherence to this KPI from 2025 onwards. • The Agency in a position to handle EUCI at the level of SECRET UE/EU SECRET and be accredited as being able to do so by Q4 2024. • 20% of the total IT budget to be allocated to information security proportional to the level of risks across various IT systems within the Agency by Q4 2024. Implement relevant security requirements and criteria for all relevant ENISA tenders for corporate services by Q1 2025.

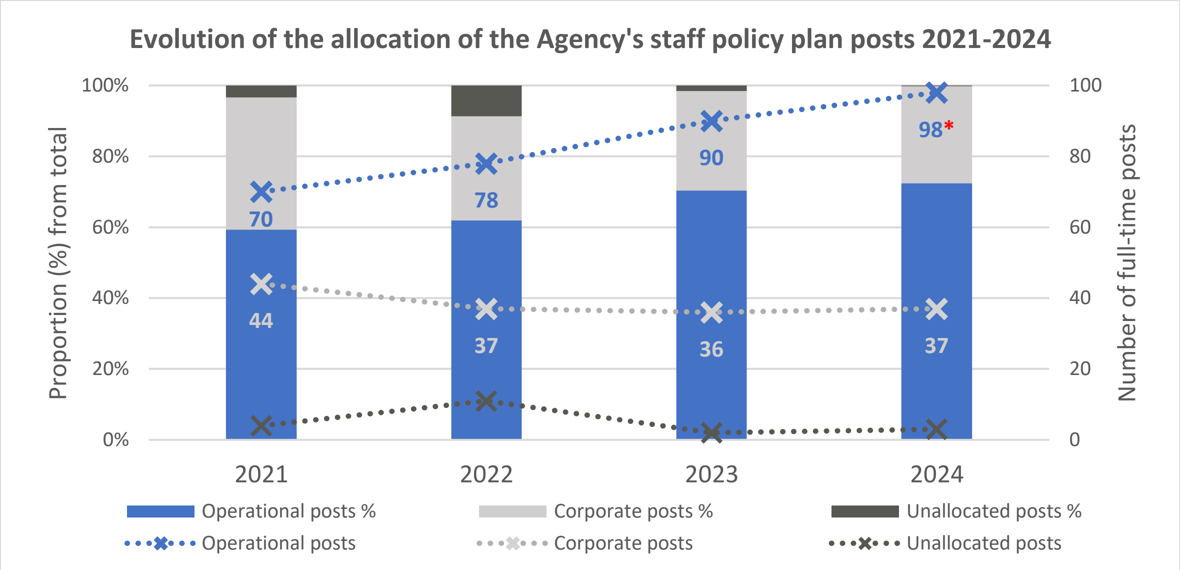
2. HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2025-2027

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

Over the past years, the Agency undertook persistent and sustained efforts to better manage, prioritize and balance the resources allocated to it, in order to adjust to the ever-increasing demand for ENISA services by Member States and stakeholders. Those actions undertaken to address the effective and efficient use of resources have included:

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 despite the increasing competition for cybersecurity talent[5] and – compared to private sector and the living standard of more economically advanced Member States – 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 4 years to rebalance the allocation of posts towards operational units and functions in expense of corporate units and functions – the latter of which have been externalised to a maximum extent possible. This follows the reorganisation of the Agency under the direction of the Management Board decision No MB/2020/9, according to which all support and corporate functions (including administrative and secretarial support etc) where concentrated to corporate units from 01.01.2020 onwards, leaving in operational units only the posts which 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 human resources to deliver 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 sustaining security (including IT and physical), legal, financial & procurement, compliance functions and other corporate support systems.



* including limited duration additional 10 CA posts financed through dedicated Contribution Agreement under Activity 6 (Activity 5b in SPD2024).

[5] 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.

2.1.2. 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, concluding 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 extent possible.

The Agency under the direction of its Management Board took steps in 2023 and 2024 to deprioritise or supress a number of outputs in the SPD. On that basis and through both restructuring and reallocating existing posts, as well as utilising previously unallocated posts, the Agency was able to allocate in total 10 FTEs to match the most critical operational and corporate needs with high or medium in 2024. It also took steps to further externalize some corporate services and functions (some level of administrative and secretarial support and technical financial assistance), which has rendered to a service provision in amount comparable to savings of 5 FTEs. Thus, through a combination of measures taken by the Management Board within SPD2024 and the Agency via 2023 annual workforce review, 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 workforce needs assessment, which was undertaken in end 2022, did not cover fully the needs arising from the CRA nor the CSoA, as the full scope of ENISA tasks foreseen nor the date of application of the proposals was not 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 under chapter 2.2. below).

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 to 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 prioritize 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 2020-2024 developed external partnerships and synergies across all operational activities, which has ensured efficient use of expertise and human resources by avoiding duplication of efforts – or through building new services – helped to increase Agency's resources. Notable examples include:

- Cooperating with the European Commission and the partner DG and 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 to the Agency's SPD: on how the Agency delivers its tasks under Activities 3, 5 and 6 (former 3, 5a and 5b in SPD2024), and what it delivers. The Agency received from the Commission an additional 15 MEUR budget in 2022-2023 [and an additional 20 MEUR budget for 2024-2026 under the Contribution Agreement signed Q4 2023, including a possibility to finance 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 in building a partnership which may be further utilised under the CSoA;

- Structured cooperation with CERT-EU entered its 4th 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 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 the cooperation even further. This cooperation has been strengthened by joint work on EUIBA

Standard Operating Procedures, which serve as a foundation for coordinated incident response and intelligence sharing with other EU agencies… revenue stream for the Agency;

- As an example of the latter, a service level agreement with **EU-LISA**[6] 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 skills gap in cybersecurity under European Cybersecurity Skills Framework as foreseen in the Commission's communication on "European Cybersecurity Skills Academy". The MoU is also foreseen to help in exploiting synergies under Activity 8 by setting up a joint cybersecurity market observatory, which should assist in fulfilling market related new ENISA tasks under CRA and in coordinating on 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 MoU with the **European Banking Authority** (EBA) as well as with **ESMA** & **EIOPA**, concerning the implementation of incident reporting under DORA and its alignment with the corresponding NIS2 requirements others, help to align ENISA's support for MS under the critical sectors of NIS2 with the activities of the other Union bodies in these sectors, including in the area of cybersecurity requirements (with ERA) and incident reporting (with EBA, ESMA, EIOPA), thus strengthening the Agency's ability to assist stakeholders in implementing or reporting on NIS2 requirements under Activity 2 and Activity 8 in SPD2024, with a potential of further additional external resourcing income with the potential use of ENISA enabled CIRAS platform for incident reporting under DORA;

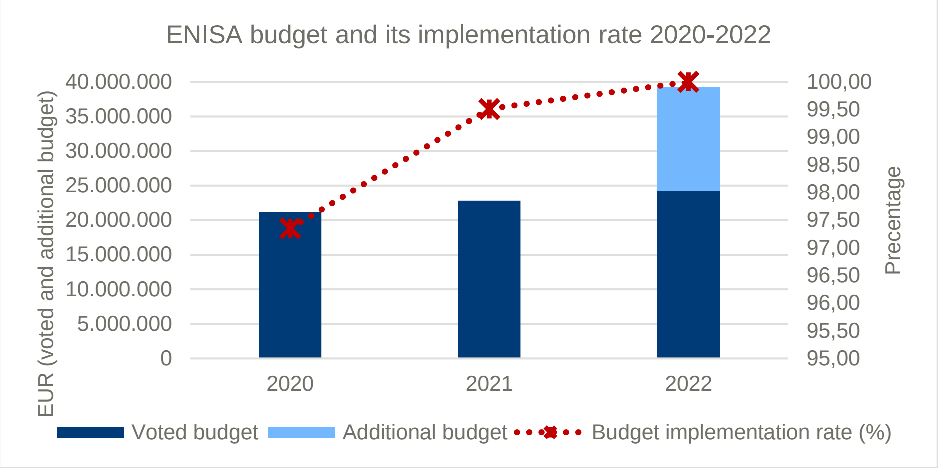
Shared services and partnerships in corporate and administrative areas. In late 2022 the Agency signed a service level agreement to create corporate synergies with the European Cybersecurity Competence Centre (ECCC), covering accounting, data protection and information security. ENISA has thus been acting as a corporate service provider for ECCC in the area of accounting and data protection with ECCC as of January 2023. The Agency has been further providing legal support services to 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 continue build up 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 – but also exploring new avenues [like for example with EIT and EIOPA, with whom the Agency in 2024 launched a joint service centre for HR, procurement and corporate cybersecurity support services]. In 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 prioritize reallocating posts to operational tasks (please see in 2.1.1 above).

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 has significantly increased its budget implementation rate to ensure that it uses all the resources to a maximum extent (please see the graph below). Those persistent efforts, which

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

included a combination of measures – such as imposing financial KPIs to 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 100% commitment rate from its voted budget. Cumulatively over 2021-2023, through increasing the budget implementation rate, the Agency has committed a total of 1.802.058,78 EUR more. An investment which would have been lost if the budget implementation rate would have remained at 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 a vast majority of the additional 15 MEUR 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 intra-muros contractors	0	0	0	5	**5**
…out of which short term interim intra-muros service providers			12		**12**
…others			0		**0**
Operational revenue in addition to Union budget (kEUR)	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 (kEUR)	0	0	200	200	**400**
Total additional revenue (kEUR)		**15 000**	**320**	**20 320**	**35 880**

Over the past three years the Agency has taken steps to use more efficiently its human and budgetary resources. Whilst its headcount in Staff Policy Plan has increased 10 FTEs from 118 in 2021 to 128 in 2023 – which has helped it to address new tasks – the Agency has used internal restructuring of post as the main tool to allocate resources to new priorities. In total 20 posts have been restructured and reallocated over the past three years in this way. This proves that the Agency is agile and able to address new service needs when those emerge.

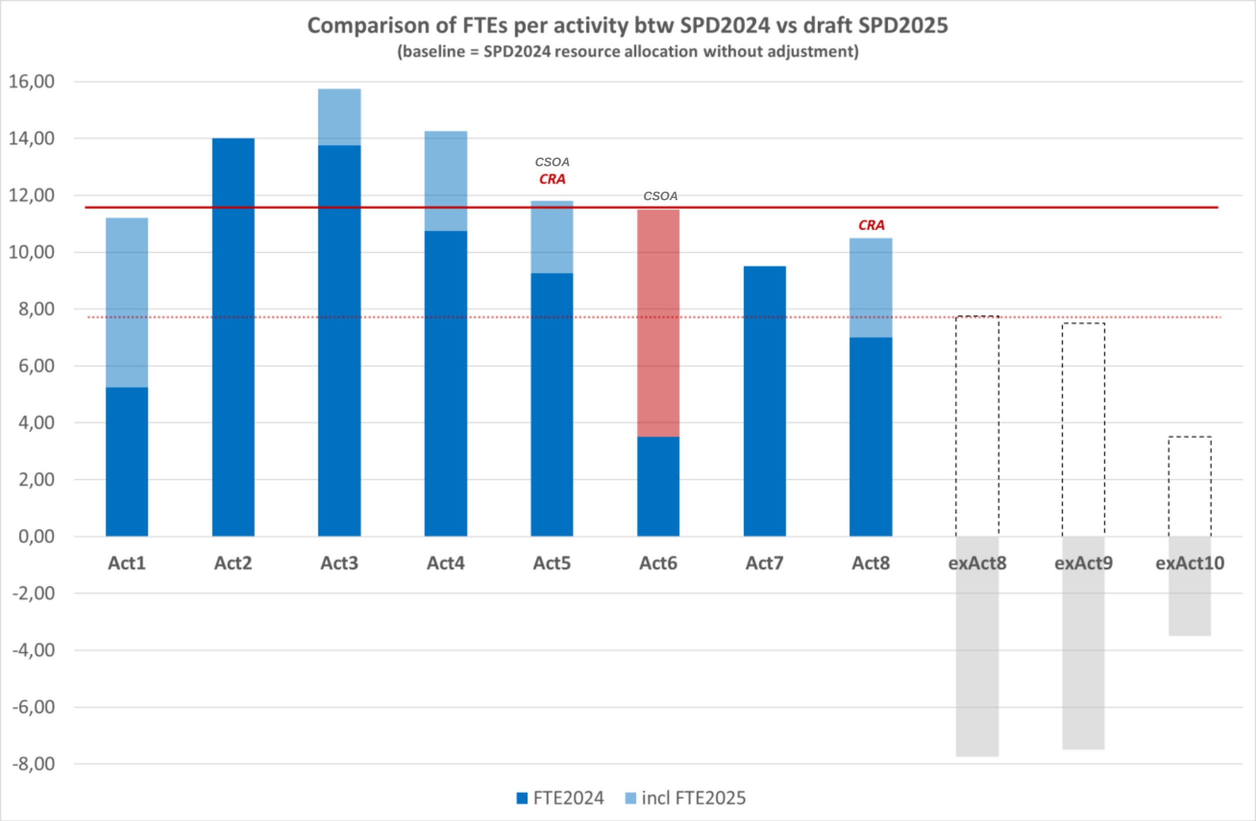
2.2. OUTLOOK FOR THE YEARS 2025-2027

The multi-annual financial framework 2021-2027 laying down the EU’s long-term budget could not foresee the cumulative effects to the rapidly deteriorating cybersecurity threat landscape – including due to 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 /…/.*”[7]

Moreover, new Union legislation, such 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 2 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 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 to a possibility that no new resources will be allocated to it. Therefore, in the 2025 draft work programme, ENISA has consolidated and restructured the operational outputs and activities. This consolidation, besides utilising better existing synergies, will also increase the budget as well as median FTE counts per activity, from slightly below 8 FTE in 2024 to almost 12 FTE. 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. Graph below shows the new FTE count per activity (using the 2024 allocation as baseline), and reallocating the FTEs linked to the outputs of the 3 supressed operational activities to the new activities. It does not include the FTE needs linked with new tasks emerging from CRA and CSoA, though Activities 5 and 8 are marked as activities which could potentially incorporate the tasks related to CRA, and Activities 5 and 6 those of CSoA.

[7] Former commissioner Thierry Breton, in his 6th of 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 are above 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 insufficient allocated resources. Therefore, unless further resources are allocated, ENISA in consultation with the MB and considering the priorities of the MS 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.

2.3 RESOURCE PROGRAMMING FOR THE YEARS 2025-2027

2.3.1. Financial resources

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

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 in the Corporate Strategy. In order to enable the achievement of the above, the Management Board has set following benchmarks, which affect the Agency's budgetary and human resource planning in 2025-2027:

- the Agency's investment into talent development is a minimum 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 of Union contribution, 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 required is detailed under each activity in the draft SPD. The total amount of budget that the Agency foresees that it requires to fulfil its mandate and by extension the demands of stakeholders amount to an additional 3.2 million EUR, when preparing the January draft SPD25-27.

2.3.2. Human resources

Though the level of ENISA's human resources should be reviewed in their entirety as regard to 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 resource estimates have not been adequate and aligned with the tasks assigned to ENISA. Thus, based on the functions that ENISA needs to develop and maintain and related internal workforce needs assessment, ENISA CRA related estimated new 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: -*reporting, management and analysis* -*developing and maintaining relevant high security systems and environment*	2	3	**-**	**5**
Chapter V (market surveillance and enforcement) incl: -*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 highest levels of confidentiality and integrity from the jobholders. All the jobholders potentially engaged for the Article 11 tasks also need to hold a valid personal security clearance at the level SECRET UE/EU SECRET. 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 brought out 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 existing resources of ENISA by deprioritising other operational activities. Preliminary lessons learned from the implementation of the Cybersecurity Support Action were presented to the Management Board during the MB meeting in November 2023, highlighting that the actual FTE allocation for ENISA Support Action 2023 was 20% to 30% higher than originally estimated (~15 FTEs) and as such adequate resourcing will need to be reflected, 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 related internal workforce needs assessment, ENISA CSOA related estimated new needs total 16 FTEs over 2025-2027. They are summarised in the table below, as well as 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: - *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) - *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 already in the current Contribution Agreement, covering the Support Action, the Commission has agreed for ENISA to engage 10 CA for limited term (until 2026) in excess to the headcount foreseen under the Staff Policy Plan. Some of these resources could be utilised in support of potential ENISA role under Cybersecurity Reserve, should the Commission ask ENISA to operate and administer it. Also, the Contribution Agreement model with additional CA's could be applied also to operationalising the Cybersecurity Reserve with appropriate scope 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 level SECRET UE/EU SECRET. Moreover, though some of the jobholders for CSOA related functions can certainly be employed at the CA level, the Agency also needs 2 TA/AD level senior officers (and already in 2025) to scope the needs of member states and third countries and steer the work, as well as additional 2 TA/AD level officers (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 brought out in table 2 above.

In sum, by the end of 2024, if the already announced legislative and political expectations towards the Agency will materialise ENISA's budgetary and human resource means shall be drawn 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.

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

Given the current constraints of its resources but also in order to fulfil its strategic and corporate objectives – including setting the pace of its staff development – ENISA will remain committed to the continuous improvement of its efficiency across its operational and corporate tasks. In the period 2025-2027 ENISA will thus further rigorously pursue all the 5 areas which were outlined in section 2.1. and which have already brought tangible benefits. Namely:

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

Within the programming period 2025-2027 ENISA will continue 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 the service packages and internal structures, ENISA aims to build partnerships with Member States (incl by exploring short- and medium-term secondments and exchanges of staff with relevant national authorities) and strengthen synergies with a number of EU institutions, agencies and bodies. This includes by proposing joint operational objectives and KPIs in the respective work programs, thus further utilising external support and mobilising external resources for the benefit of ENISA operational objectives when those are aligned with the objectives of prospective partners. The main current and possible partnerships and/or prospective cooperation frameworks across its operational activities shall include:

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

ENISA also intends to assess and analyse sustainability of existing processes, explore alternative models for providing indirect support and propose actions to ensure operational efficiency without compromising the activities of the operational units. Within the context of its Corporate Strategy, the overall operating business model of the support units would continue to be reviewed in order to ensure that the MB 2020/09 thresholds and requirements of the Corporate Strategy are met. Digitalisation of services, self-service functionalities and service optimisation will be also at the core of the future way of working and ENISA's corporate strategy to build an agile workforce. ENISA will continue to review and explore possibilities to reengineer its processes, with a view to optimising service quality and cost-effectiveness.

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 such as CERT-EU's threat-sharing frameworks, allowing for real-time data exchange and collaborative incident response. ENISA will also prioritize the creation of interoperable tools and interfaces, such as

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

SECTION III. WORK PROGRAMME 2025

This is the main body of the Work Programme describing, per operational and corporate activity, what the agency aims to deliver in the respective year towards achieving its strategy and the expected results. In total 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 service catalogue to allow management to focus efforts and resources in a highly structured and more efficient manner for obtaining specific objectives. The ENISA service catalogues are organised into individual service packages, a service package is a collection of cybersecurity products and services that span across a number of activities and contribute to the objectives of a discrete service package. A service package is a means of centralizing all services that are important to the stakeholders that use it. The Agency will continue to review and prioritize its actions in order to build and make use of internal synergies, and ensure that adequate resources are reserved across the Agency in a transparent manner.

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

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

Stakeholders and engagement level

Stakeholders' management is instrumental to the proper functioning and implementation of ENISA' work programme. On 29 March 2022 Management Team adopted the ENISA's Stakeholders Strategy. This Strategy lays down the main principles and approach towards stakeholders' engagement at Agency-wide level. The implementation of the Stakeholders Strategy is linked with the implementation of the Single Programming Document (SPD) via 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. Whilst stakeholders classified as involve / engage have a high influence and 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 performance of the activities. These metrics are inscribed 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 formulae. Where as 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 activity objectives 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
The activity seeks to bolster policy initiatives on novel/emerging technology areas by providing technical, fact-driven and tailor-made policy analyses and recommendations. ENISA will support the Union institutions and MS on new policy initiatives[8] through evidence-based inputs into the policy development process. ENISA, in coordination with the Union institutions and MS 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 the existing Union policy and law in accordance with the EU's institutional competencies in the area via "Implementation Check" model, in particular together with Activities 2 and 8. 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 MS, incuding via input fro 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 Art.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 MS needs and requirements, which can be used for programming activities 2 and 3. The added value of this activity is to support the decision makers in evidence-based policy making, in a timely manner and to inform them on developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework, by also utilizing among other sources information from 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 Article 5, Article 9 of the CSA and Articles 18 of the NIS2.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
Empowered communities in an involved and engaged cyber ecosystem Effective and consistent EU policies implementation for EU cybersecurity policy Foresight on emerging and future cybersecurity opportunities and challenges	Uptake of recommendations stemming from NIS2 Art. 18 report. Number of identified future and emerging areas reflected in the policy initiatives and interventions

ACTIVITY 1 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
1.A By end 2026 implement a policy monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, support and assistance to national and Union policymakers in cybersecurity	Art 5 CSA; Art. 9 CSA	2026	Assessment of ENISA advice and 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

[8] Initiatives on NIS2 sectors such as Space, Health, AI, data spaces, digital resilience and response to current and future crises

				is endorsed
1.B By Q3 2026 and in collaboration with Activity 2, ensure that 2/3 of policy observations within the first State of Cybersecurity in the Union report have been realized	Art 18 NIS2	2026	Assessment of MS usage of the Art. 18 report (stakeholder survey, desktop research)	2/3 of MS are using Art.18 report as input for their cybersecurity strategies
				All MS use ENISA support and tools for the work on their NIS Strategies

ACTIVITY 1 OUTPUTS

DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	TARGET 2025
1.1 Assist MS to implement, assess, review National Cybersecurity Strategies and policies. Enhance a culture of trust and cooperation among MS, also through peer reviews, 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 subgroups	Develop and pilot peer review framework, including code of conduct	Biennial (Survey), annual dialogues, and annual desktop research	NA	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		93%	>90% stakeholder satisfaction
1.3. In coordination with Activity 2, 4 and 8, develop and maintain analyses on time-sensitive observations offering technical advice to policy development.			Assessment of timeliness of advice provided during policy development		NA	>70% stakeholder satisfaction with timeliness

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

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

ACTIVITY 1 RESOURCE FORECASTS		
	Budget	FTEs
Total activity resources	Budget: €353.037[9]	FTE[10]: 10

[9] *of which €59.000 centralised to missions and large-scale events budget*
[10] Target FTEs

Activity 2 Cybersecurity and resilience of critical sectors[11]

OVERVIEW OF ACTIVITY

The activity supports Member States and EU Institutions with the implementation of the NIS2.. The objectives of this activity is the rapid and harmonized implementation of the 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 cybersecurity of cross-border electricity flows. This activity includes an annual policy implementation check, which relies on direct information from companies in the NIS sectors.

Under this activity ENISA provides support to the NIS Cooperation Group workstreams, and the implementation of the NIS CG work program. In this period the focus is on supporting the NIS2 transposition, the NIS2 implementing acts, and the implementation of new tasks under the NIS2, like the EU registry for digital infrastructure entities. ENISA's goal here is 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/approach for risk management, security measures and incident reporting in the EU.

Secondly, ENISA supports MS and the Commission with 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 Posture[12], the Union coordinated supply chain risk assessments (under the NIS2), and the Union coordinated preparedness tests (aka resilience stress tests, under the Cyber Solidarity Act). After supporting the MS and Commission with developing the necessary frameworks, methodologies and scenarios, in 2026 ENISA will also support the MS and the Commission with carrying out a Union coordinated resilience preparedness test and a Union coordinated supply chain risk assessment. 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 organizing industry events to facilitate public-private dialogue on cybersecurity. Besides supporting the four highly critical sectors telecoms, energy-electricity, finance, and the internet infrastructure (aka core internet), ENISA also supports sectors with low to medium level of maturity, like 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 of the NIS sectors, producing the annual NIS investments report, the annual NIS 360 and sectorial cyber risk posture briefs, which give an overview of the posture of different NIS sectors. This output provides important sectorial input to the State of Cybersecurity in the Union report (Activity 1).

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

The legal basis for this activity is Article 5 and Article 6 (1)(b) of CSA.

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

ACTIVITY 2 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
2.A By [2026] pilot and by [end 2027] implement common frameworks and joint tools for NIS2 in the areas of (a) risk management, (b) security measures and (c) incident reporting for all EU sectors, and in line with industry good	CSA Article 5, Article 6 and NIS2	Frameworks' development 2025	Framework's development	#2 frameworks developed
		Frameworks pilot by 2026	Pilot program implementation (# of sectors piloting the	#20MS to adopt/use/endorse the frameworks

[11] Critical sectors as terminology is used in this context to cover ALL sectors in scope of the NIS2.
[12] st09364-en22.pdf (europa.eu)

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

ACTIVITY 2 OUTPUTS

DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	TARGET 2025
2.1 Support Member States with the 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 to adopt/use/endorse the frameworks
			EU register for digital entities is used by all MS	Annual (Report)	n/a	20 MS to use the registry
			Alignment between DORA and NISD2	Satisfaction survey	n/a	>80%
2.2 Support Member States with union toolboxes, union coordinated risk evaluations, and union 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 chain	Annual (Internal count)	n/a	#1 coordinated risk assessment for 1 domain/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	Annual (Internal count)	21	24

			services/ workflow delivered to NIS sectors according to the maturity of the sector			
2.4 Perform an annual policy implementation check	MS and EU institutions, both horizontal and sectorial stakeholders, use the NIS investments, the NIS360 and the cyber posture briefs as reference documents for policy making.	DG CNECT, NIS CG, Sectorial EU ISACS, sectorial EU agencies	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	#5 requests stemming from the NIS2 implementation in MS

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: €468.024[13]	FTE[14]: 12

[13] *of which €137.000 centralised to missions and large-scale events budget*

[14] 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 trainings, designing and executing awareness raising programs on cybersecurity risks and good practices, and by facilitating gamified Capture the Flag (CTF) competitions at national and EU level.

Secondly this activity contributes in Agency's reporting duties on the current State of Cybersecurity in the Union (NIS 2 Article 18) by providing insights on cybersecurity capabilities of private and public stakeholders and on 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 from 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 programs using ENISA's services through a pricing model.

Furthermore, the Agency, in collaboration with relevant EUIBAs and Members States operational communities, will conduct a limited number of targeted exercises and trainings 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 trainings (such as Team Europe trainings) and educational programmes in cooperation with National Competence Centers (NCCs) and other relevant stakeholders.

The plan is to gradually transfer knowledge and empower MSs, in particular NCCs, national operational communities, and ECCC, and to organize and financially support CTF trainings 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 TREX service package and supports the INDEX, SITAW and NIS service packages.

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

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
Empowered communities in an involved and engaged cyber ecosystem	Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, trainings)
Strong cyber security capacity within EU	Percentage of MS that use European Cybersecurity Skills Framework

ACTIVITY 3 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
3.A Maintain and regularly update the European Cybersecurity Skills Framework (ECSF).	EU Communication on Cyber Security Skills Academy Article 10 and 6	2027	Number of MS endorsing the 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 Article 4, 6, 7(5), 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 Article 4, 6, 7(5), 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	Review and update ECSF in line with the CyberSkills Academy Communication Measure and report on the skills gap including developing indicators to be used for INDEX and Article 18a Promote the adoption of ECSF in MS, in training organisations and academia and ensure its regular update.	AHWG on Cybersecurity Skills, ECCC WG 5 on Skills	Stakeholder satisfaction	Biennial (Survey)	91%	95%
			Number of MS endorsing ECSF	Annual	N/A	10
			Number of Training Organisations endorsing ECSF in their training programs	Annual	N/A	15
3.2 Organise targeted exercises and support stakeholders to plan, execute their own exercises	Organise a set of limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders Develop, deploy and promote exercises tools and frameworks that enable stakeholders, in particular NIS2 sectors, to independently execute their own cybersecurity exercises Develop a community of "train the planners" that leverage the tools, platforms and frameworks developed by ENISA	NLO Network (as necessary) CSIRTs Network (as applicable) EU-CyCLONe members (as applicable) NIS Cooperation Group (as applicable) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as applicable) CERT.EU	Number of people impacted directly and/or indirectly by exercises organized by ENISA	Annual (Report)	N/A	>7.000
			Number of sectorial authorities, including EUIBAS, using ENISAs exercise solutions and frameworks	Annual	N/A	5
			Number of MS participate in the community of "train the planners"	Annual	N/A	10
3.3 Organise targeted trainings and awareness programs and support	Develop, deploy and promote trainings and awareness raising tools,	NLO Network (as necessary)	Number of participants in ENISA online based trainings	Annual (Report)	3800	4000 (depending on

stakeholders to plan, execute their own trainings / programs	frameworks and content that enable stakeholders, in particular NIS2 sectors, to independently execute their own training or awareness raising programs Develop a community of “train the trainers” that leverage the tools, platforms and frameworks developed by ENISA Harmonize training activities sponsored by Cyber Security Support Action	CSIRTs Network (as applicable) EU-CyCLONe members (as applicable) NIS Cooperation Group (as necessary) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as necessary)				Support Action contribution)
			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	10000
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)	3000	20000

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: €796.409[15]	FTE[16]: 12
Other supplementary contribution	~€120.000 from Service Level Agreement with EU-LISA to provide support on exercises	**Other supplementary contribution**

[15] *of which €105.000 centralised to missions and large-scale events budget*
[16] 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 efficient functioning of EU operational networks and cyber crisis management mechanisms, including the revision of the Blueprint. Under the mandate of NIS2, activity 4 provides expertise, organizational 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 the structured cooperation with CERT-EU and as such to identify and act upon synergies between the Agency and Member States' work and the work of the IICB and CERT-EU.

Thirdly, the 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 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 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 delivering of the tasks mandated by the Cyber Solidarity Act within the Cybersecurity Incident Review Mechanism (at the request of the commission or of national authorities -the EU-CyCLONe or the CSIRTs network-, ENISA will be responsible for the review of specific significant or large-scale cybersecurity incident and should deliver a report that includes lessons learned, and where appropriate, recommendations to improve Union's cyber response..

Fourthly, the activity also maintains IT systems and platforms for all ENISA operational activities and develops a comprehensive knowledge and stakeholder management system.The activity facilitates synergies with national cybersecurity communities (including civilian, law enforcement, cyber diplomacy, and cyber defence) and EU actors, such as CERT-EU, EC3, and EEAS, to exchange knowledge, best practices, provide advice, and issue guidance.

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

This activity supports SITAW, INDEX and NIS service packages.

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

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
Empowered communities in an involved and engaged cyber ecosystem Effective Union preparedness and response to cyber incidents, threats, and cyber crises Consolidated and shared cybersecurity information and knowledge support for Europe	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 and a satisfaction rate (by MS and stakeholders) with ENISA ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats

ACTIVITY 4 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
By [end 2026] strengthen the interaction and trust within and between key EU operational and cybersecurity communities (CSIRTs Network, EU-CyCLONe, HWPCI and NIS Cooperation Group).	Article 7, 10, 15, 16 NIS2 Article 6, 7 CSA Article 16 CRA Article 11 CSOA	2026	Assessment of High level of operational interaction across CSIRTs Network, EU-CyCLONe, HWPCI and NIS Cooperation Group.	>60% of stakeholders agree that ENISA has enabled the functioning of supported the building of trust within the network

			ENISA is judged as a key enabler of trust within and between CSIRTs Network, CyCLONe, HWPCI and NIS Cooperation Group.	>60% of stakeholders agree that ENISA has enabled interaction and trust between the networks and communities
Review and implement both the ENISA stakeholder strategy and ENISA international strategy	Article 12 CSA	2026	Coherence of ENISA International Engagement with the Agency's strategy.	Updated international strategy
			Comprehensive knowledge management and stakeholder management system is established.	Establish framework for knowledge management and stakeholder management
Develop and maintain relevant operational IT systems and platforms to support all operational communities and enhance synergies.	Article 7, 10, 12, 15, 16 NIS2 Article 7 CSA Article 16 CRA	2026	Relevant IT systems are maintained and new mandatory platforms are developed.	IT Operations are consolidated and synergy plan designed (2025) and implemented (2026).

ACTIVITY 4 OUTPUTS						
DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	TARGET 2025[17]
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

[17] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023

			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 ENISA Cyber Partnership programme aiming at information exchange 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 program	Annual (report)	4	6
			Percentage of RFI answered by members of partnership program	Annual (report)	N/A	65%
4.3 Implement the ENISA international strategy and outreach	EU values recognised by international stakeholders	MT, EEAS, COM and (MB as required)	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)
	International cooperation support ENISA objectives		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.	CSIRTs Network.	Stakeholder satisfaction	Biennial (survey)	N/A	66% by 2027
	CRA Single Reporting Platform is being developed					
4.5.Develop and maintain IT systems and platforms for operational activities.	Consolidation of operational IT with view to support ENISA operations.	CSIRTs Network and CyCLONe members, HWPCI and NIS Cooperation Group and Business owners for ENISA Operational IT systems.	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			IT architecture for external operational IT services	Biennial update	N/A	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 the 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 FORECASTS		
	Budget	FTEs
Total activity resources	Budget: 1.652.091[18]	FTE[19]: 15

[18] *of which €115.000 centralised to missions and large-scale events budget*
[19] Target FTEs

Activity 5 Provide effective operational cooperation through situational awareness

OVERVIEW OF ACTIVITY

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

ENISA delivers on this activity by collecting and analysing security events, cyber incidents, vulnerability and threats based on its own monitoring , shared by external stakeholders due to legal obligations[20] or voluntary shared, aggregating and analysing reports, ensuring information flow between the CSIRTs Network, EU-CyCLONe, and other technical, operational and political decision makers at Union level and including cooperation finalized to increase situational awareness with other Union entities services such as relevant Commission services and in particular DG CNECT, CERT-EU, Europol/EC3, and EEAS including EU INTCEN. This activity activly benefits from ENISA's Cyber Partnership Programme managed under Activity 4 and the Agency international cooperation frameworks.

Secondly the activity includes the preparation of the regular in-depth EU Cybersecurity Technical Situation Report in accordance with CSA art7(6), also known as the EU Joint Cyber Assessment Report (EU-JCAR), regular weekly OSINT reports, Joint Rapid Report together with CERT-EU and other ad-hoc reports as needed. Under this activity the Agency preapres **threat landscapes** and provides topic-specific, as well as general, assessments on the expected societal, legal, economic, technological and regulatory impact, with targeted recommendations to Member States and Union institutions, bodies, offices and agencies. Under this activities, a semi-annual report in accordance to NIS 2 Art23(9)[21] is prepared and the work related to the Cyber Solidarity Act – Incident Review Mechanism (Art18*) is undertaken

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

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

Finally under this activity the work underpinning the establishment of the Single Reporting Platform as established under the Cyber Resilience Act.In doing so, the Agency will take into account **incident reports** frameworks implemented under Article 23 of NIS2 and other relevant EU legislation to ensure alignment and future proof architecture for reporting simplification at EU level.

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

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

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

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

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
Empowered communities in an involved and engaged cyber ecosystem Effective Union preparedness and response to cyber incidents, threats, and cyber crises Consolidated and shared cybersecurity information and knowledge support for Europe	EU Vulnerability Database is operationalised by ENISA and a satisfaction rate (by MS and stakeholders) with ENISA ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and successfully operated

ACTIVITY 5 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
By [end 2027] build a common situational awareness between Member States based	Article 7 of CSA Article 23(9) of NIS2	2025 - 2027	Content of JCAR is contributed and	Produce at least one comprehensive joint analysis

[20] NIS2, CRA and Regulation 2023/2841

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

on shared accurate data and underpinned by validated joint analysis	Article 18 of CSOA		validated by Member States	report every quarter, contributed and validated by at least 75% of l Member States (EU-JCAR).
			ENISA Data repository is open to and includes also information directly provided by Member States	Data repository is accessible by MS.
				Percentage of information in the data repository validated or provided by MSs is above 75% and 100% or significant event impacting EU MSs
			Establish and test processes and procedure for the Incident Review Mechanism under Art 18 of CSOA	Process for IRM is established and endorsed by MSs
Provide regularly general as well as specific threat landscapes and threat analysis, based on observed and data driven trends in incidents and vulnerabilities	CSA Art 9 Article 7 of CSA Article 23(9) of NIS2 Article 18 of CSOA Article 14-17 CRA	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).
			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 is included by Q4 2026
			Ability of ENISA to produce	80% of Member States scores

			accurate threat analysis based on Incidents, Vulnerabilities and Threat information based on Agency own monitoring , shared by external stakeholders due to legal obligations[22], or voluntary shared,	quality of threat analysis provided by ENISA above 4 (1-5)
				80% of Member States scores ability of ENISA to use information available to produce threat analysis and recommendation above 4 (1-5)
			CRA SRP is established and operational	CRA SRP is used to carry on tasks under CRA by end of 2026

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 to 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[23]	Establishment of a Threat Information Management Platform. Production of briefings, reports, and summaries of incidents, threats, and vulnerabilities Increased understanding and timely access to information regarding latest threats, incidents and vulnerabilities	CSIRT Network, EU CyCLONe, Union entities, National Authorities within MSs subscribed to the products	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			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, threat and risk analysis[24]	CSIRT Network, EU CyCLONe, Union entities, HWPCI, Management Board	Stakeholder satisfaction	Biennial (survey)	84%	>90%

[22] NIS2, CRA and Regulation 2023/2841
[23] Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1
[24] Including JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and CNECT Situation Centre

	Recipients receive accurate and timely assessment of threat actors and associated risk 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 the cyber threat landscapes	Mapping threats Generate recommendations for stakeholders to take up	NLO, AG and Cybersecurity Threat Landscape AhWG CSIRTs Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Number of downloads of ETL	Annual (report)		>5% increase year on year
5.4 Analyse and report on incidents as required by Art 5(6) of CSA as well as other sectorial legislations (e.g. DORA, eIDAS Art. 10, etc.)	Analysing incidents Generate 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 operationalize 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 process expected for 2025 are defined Implementation work is started.	Survey	N/A	80% of the stakeholder agree on the established process and score them >4

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

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

ACTIVITY 5 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources from direct annual budget	*Budget: 1.566.118*[25]	*FTE*[26]*: 13*[27]

[25] *of which €90.000 centralised to missions and large-scale events budget*
[26] Target FTEs, Current Staff 12 plus foreseen 2 FTE for CRA SRP and 1 FTE for Incident Review Mechanism
[27] Including 2 FTE – Contract Agents are hired through the Contribution Agreement signed with Commission in 2023 under Cybersecurity Support Action and Situation Center.

Other supplementary contribution	Budget: TBD (outputs 5.1 and 5.2) [28] and TBD[29] for CRA Platform	2[30]
Other supplementary contributions on-going	Budget: (outputs 5.1 and outputs 5.2) forecast €223.000 from existing contribution agreement signed in 2023	2[31]

[28]. 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 action, situation center and CRA single reporting platform implementation., please refer to annex XI for further details regarding contribution agreements, final text pending. The amount indicated refers to years 2025 to 2027.

[29] Allocation depends on the final text of the Contribution Agreements to be signed with Commission in 2024.

[30] FTE allocation depends on the final text of the Contribution Agreement to be signed with Commission in 2024.

[31] 2 FTE – Contract Agents are hired through the Contribution Agreement signed with Commission in 2023 under Cybersecurity Support Action and Situation Center.

Activity 6: Provide services for operational assistance and support

OVERVIEW OF ACTIVITY

The activity contributes to further develop preparedness and response capabilities at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity through the implementation and delivery of ex-ante and ex-post services. It implements the Cybersecurity Support Action, through which the Agency provides services such as: pentest, threathunting, risk monitoring and assessment, customized exercise, trainings and support the Member States with incident response.

The Agency will leverage upon the lessons learned and the mechanisms that have been put in place during the first year of the Cybersecurity Support Action in 2023. This will refocus the service catalogue an the processes/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 are agreed with single point of contact within each EU Members States and final beneficiary entities.

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

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

This activity will be adjusted when the Cyber Solidarity Act will enter 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 conducting of mapping of the services needed by the users of the Reserve, including the availability of such services from legal entities established and controlled by Member States.

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

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

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
Empowered communities in an involved and engaged cyber ecosystem Effective Union preparedness and response to cyber incidents, threats, and cyber crises	Operationalisation of the EU Cybersecurity Reserve of which administration and operation is to be entrusted fully or partly to ENISA and used by MS, EUIBAs and on a case by case basis DEP associated third countries

ACTIVITY 6 OBJECTIVES

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

ACTIVITY 6 OUTPUTS

DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	TARGET 2025

6.1 Provide pentest and threat hunting services towards selected entities within EU Member States[32]	Pentest and Threat Hunting services are delivered timely and accurately to MSs	MSs, CNECT, Beneficiaries	% of MSs requesting the service Satisfaction score	Annual	N/A	50% >4
6.2 Provide customized Exercise and Training for selected entities within EU Member States	Customize Exercise and Training services are delivered timely and accurately to MSs.	MSs, CNECT, Beneficiaries	% 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 provide specific risk assessment and threat landscape as requested by MSs	MSs, CNECT, Beneficiaries	% of MSs requesting the service Satisfaction score		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, Beneficiaries	% of MSs requesting the service Support was provided timely Satisfaction Score		N/A	50% >4

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	FTEs: 4
Other supplementary contribution	Budget: TBD [33]	FTEs: TBD
Other supplementary contributions on-going	Budget: forecast €9.773.866,89 from existing contribution agreement signed in 2023	9 FTEs financed from existing Contribution Agreement signed in 2023)

[32] Beneficiaries of the Act5 services are specified in the [Contribution Agreement]

[33] 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 action, situation center and CRA single reporting platform implementation., please refer to annex XI for further details regarding contribution agreements, final text pending. The amount indicated refers to years 2025 to 2027.

Activity 7 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

This 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 Commissionor on the basis of the Union Rolling Work Program (URWP) or, in duly justified cases, at the request of the Commission or the European Cybersecurity Certification Group (ECCG). This also includes in particular the activities related to the ID Wallet certification (support to national schemes and development of EU scheme) as a priority, and other schems under development (EUCS, 5G), as well as the activities in view of the upcoming request in line with the URWP , such as the one related tomanaged security services following entry into force of the CSA amendment. Actions also include supporting the maintainance and review, as well as evaluating adopted European cybersecurity certification schemes, in particular the adopted EUCC, as well as capacity building for National Cybersecurity Certification Authorities (NCCAs)and supporting the peer review mechanism in line with the CSA and related implementing regulation. In addition, in this activity, ENISA assists the Commission with regard to the European Cybersecurity Certification Group (ECCG) and existing ECCG sub-groups (EUCC review and maintenance; peer review; cryptographic mechanisms) as well as with co-chairing and providing secretariat to the Stakeholder Cybersecurity Certification Group (SCCG) .

ENISA has developed one candidate scheme based on an EC request from 2019, in accordance with Art 49.2, which was adopted as Implementing Regulation, the EUCC. ENISA is currently developing 2 other candidate schemes also based on EC requests, the EUCS and the EU5G, in accordance with Art 49.2. The URWP was adopted in Feb 2024, and the recent request received for the development of an EUDI wallet candidate scheme is in line with Art 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 also explored the possibility of the certification of AI, which is also highlighted in the URWP but for which no candidate scheme request 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 legislations, in particular the Cyber Resilience Act. Other relevant legislations include NIS2, DGA EUDI Wallet, AI Act, Chips Act, Data Act. .

.

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

The legal basis for this activity is Article 8 and Title III Cybersecurity certification framework, of the CSA.

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

ACTIVITY 7 OBJECTIVES

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

for drafting new cybersecurity certification schemas			Certification and pending formal COM request, Managed Security Services)	
			ECCG endorsement of draft certification schemes	Positive ECCG endorsement
			SCCG opinion on draft certification schemes (satisfaction survey)	More than 60%
Ensure the maintenance of existing schemas and support their roll-out	CSA, Art. 49	2027	Number of schemas maintained with ENISA active involvement	1 (EUCC) + EUCS pending final approval
			Satisfaction by ECCG on ENISA supporting efforts for documents for maintenance	75%
			Number of certificates issued and published under an EU certification scheme; high utilisation rate in the market.	Proportionate[34] 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[35]
7.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes	Scheme meets stakeholder requirements, notably of the Member States and the Commission Take up of schemes by stakeholders Timely delivery by ENISA of all schemes requested in	Ad hoc working groups on certification ECCG European Commission	Stakeholder satisfaction	Biennial (survey)	82%	75%
			Number of opinions of stakeholders managed	Annual (report)	n/a	100 opinion items per scheme
			Number of people/organizations engaged in the	Annual (report)	N/A	At least 20 ad hoc Working Group Member from third-party

[34] ENISA monitors the certificates issued under SOG-IS and transition to EU CC will have to be proportional to the number of certificates issued.
[35] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023

	cooperation with the Commission Statutory Bodies and ad hocWorking Groups actively involved		preparation of certification schemes			Experts; at least 15 Member States joining ad hoc Working Groups
7.2 Implementing and maintaining of the established schemes including evaluation of adopted schemes, participation in peer reviews etc. monitoring the dependencies and vulnerabilities of ICT products and services	Review of schemes to improve efficiency and effectiveness Take up of schemes by stakeholders	ECCG European Commission	Stakeholder satisfaction	Biennial	82%	75%
			ECCG satisfaction of ENISA efforts on schemes adopted	Triennial (survey)	N/A	75%
			Satisfaction of ENISAs role in NCCA peer reviews	Triennial (survey)	n/a	75%
7.3 Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks		ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			Feedback from statutory bodies including NCCAs on ENISAs role	Annual (survey)	N/A	75%
7.4 Developing and maintaining the necessary provisions and tools and services concerning the Union's cybersecurity certification framework (incl. certification website, support the Commission in relation to the core stakeholders service platform of CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework etc.)	Supporting in transparency and trust of ICT products, services and processes Stakeholders engagement promotion of certification	ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			Users satisfaction concerning the certification website services	Annual (survey)	N/A	75%
			Usage of certification website	Annual (report)	N/A	75%

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. 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: 697.089*[36]	*FTE*[37]*: 10*

[36] *of which €127.000 centralised to missions and large-scale events budget*
[37] 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 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 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 adoption of relevant codes of conduct. As such, this activity also seeks to lay the ground for an effective role of ENISA in the CRA notably in terms of market analysis, preparation of market sweeps and 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 for risk management as well as performing regular analysis of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein, as well as incurred incidents. The activity aims at strengthening and reinforcing ties with the private sector and promoter collaboration among the cybersecurity market players, in order to improve visibility and uptake of trustworthy and secure ICT solutions in the digital single market.

In parallel the activity aims to provide advice to EU Member States (MS), EU institutes, bodies and agencies (EUIBAs) on research needs and priorities in the field of cybersecurity, thereby contributing to the EU strategic research and innovation agenda, notably the ECCC.

To prepare this strategic advice, ENISA will take full account of past and ongoing research, development and technology assessment activities, outputs of other statutory bodies of the cybersecurity landscape such as the NIS Cooperation Group, ECCG, CSIRTs Network, EU-CyCloNe and scan the horizon for emerging and future technological, societal and economic trends that may have an impact on cybersecurity. In this respect, lessons learned and trends from reported incidents and vulnerabilities will also be utilised.

ENISA will 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 different quadrants of the community. The ecosystem of the ECCC and the National Coordination Centres (NCCs) will be involved in these consultations. A strong collaboration and mapping of relevant requirements of the market authorities as defined in the CRA will also take place in the context of this activity.

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

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

The legal basis for this activity is Article 8 and 11 and Title III of the CSA, as well as the CRA, the eIDAS2 Regulation, the AI Act (Art. 67) and the Data Governance Act (Art. 29).

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

ACTIVITY 8 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
By [end 2026] implement a 'market' monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, reports on the trustworthiness of critical products and services with digital elements under CRA	CRA (final text pending)	2026	Timeliness of ENISA reports	Reports delivered on time
			Acceptance of ENISA reports by MS	2/3 of MS endorsing ENISA reports
			Validity of ENISA framework	All MS validating and endorsing

				ENISA framework
Provide continuous comprehensive support to MS market supervisory authorities and to the COM for implementing CRA requirements.	CRA (final text pending)	2026	MS and COM stakeholder satisfaction survey	More than 70%
Create a technology & innovation radar, to understand the level of impact that new technologies have on cybersecurity	CSA Art. 9 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
			EU cybersecurity R&I impact assessment	5% increase over reference data

ACTIVITY 8 OUTPUTS

DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	Target 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, MS 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 MS (NCCs and market authorities)	Annual	N/A	> 60%
			ECCC Strategic Agenda and Action Plan alignment	Annual (survey with ECCC GB)	N/A	> 60%
8.2. Market analysis on 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 / industry	Ad hoc working groups cybersecurity market analysis ECCG (as necessary) SCCG Advisory Group NLO (as necessary) MS Market authorities	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Cybersecurity market analysis; cybersecurity product and services	Annual (report)	N/A	All reports produced as planned (Y out of Y reports)

			Endorsement by MS of report on emerging trends regarding cybersecurity risks in products with digital elements	Biennial (report)	N/A	27 MS 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-years 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 (incl. 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 Centre's.

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: 697.887*[38]	*FTE*[39]*: 10*

[38] *of which €134.200 centralised to missions and large-scale events budget*
[39] 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

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

Under this activity ENISA seeks to deliver against key objectives of the Agency's Corporate Strategy (service-centric and sustainable organisation), including by establishing a thorough quality assessment framework, ensuring proper and functioning internal controls and compliance checks, as well as maintaining a high level of cybersecurity across all Agency's corporate and operational activities. In terms of resource management, the Budget Management Committee coordinates the Agency's adherence to financial management principles. In the area of IT systems and services, the IT Management Committee coordinates and monitors the comprehensive application of the Agency's IT strategy and adherence to applicable policies and procedures.

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

ACTIVITY 9 ANNUAL OBJECTIVES

DESCRIPTION	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	LATEST RESULT	TARGET
9.A Enhance corporate performance and strategic planning	Ensure efficient corporate services	Proportion of SPD KPIs meeting targets	Annual	13 metrics were unchanged, 21 underperformed and 58 outperformed	>80 of indicators outperformed
	Continuous innovation and service excellence	Results of Internal control framework assessment	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 continuous governance to safeguard high level of IT	Agency IT strategy aligned with corporate strategy	Annual	N/A	70% implementation (ITMC reporting)
		Proportion of total IT budget allocated to information security proportional to the level of risks identified across IT systems within Agency		N/A	20%

ACTIVITY 9 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025**
9.1 Coordinate the implementation of the Agency's performance management framework, including Agency wide budget management and IT management processes, environmental management and regulatory compliance	Unified day to day practices across the agency upon implementing SPD Annual risk assessment and internal controls assessment performed and reported Legal and regulatory compliance are monitored; issues and areas of improvement identified. Outcomes are included in the Annual risk assessment and internal controls assessment Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy; under ITMC Streamlined budget management across the Agency; under BMC A plan to reduce CO2 emissions at ENISA's HQ	MT, ITMC & BMC External and internal audits Statutory bodies	Number of high risks identified in annual risk assessment	Annual	3	<= 3
			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
			Percentage of identified internal controls deficiencies addressed within timelines		N/A	100% for critical, 80% for major, 60% for moderate
			Timely follow-up and resolution of internal and external audits (in particular from IAS and ECA) recommendations and findings			Monitoring audit action plans Results of corrective actions taken during year N-1 are reported in the current year AAR

			Number of identified regulatory breaches		3	<=3
			Percentage of revised and up to date corporate rules (MBD, EDD, policies, processes)		N/A	50% corporate rules which have not been reviewed less than 4 years ago; 60% corporate rules which have not been reviewed less than 5 years ago. Provide or confirm motivation for non-revision, as baseline requirement
			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	>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 Regulation on a high common level of cybersecurity within Union entities Timely identification and response to cybersecurity risks Continuous monitoring of IT systems cybersecurity and timely identification of issues and areas of improvement (first level and second level controls)	MT and relevant committees External and internal audits Statutory bodies	Percentage of identified high risk mitigation measures addressed within timelines	annual	NA	90%
			Annual risk assessment (RA) and risk treatment plan with the relevant Business Owners	annual	NA	Implement annual risk assessment follow up actions.
			Implement action plan for the implementation of the cybersecurity risk management measures in line with the Regulation (EU) 2023/2841	annual	NA	Report on the level of accomplishment of action plan

			Address all potential cybersecurity incidents	annual	NA	Respond to >90% of tickets submitted to ServiceNow
			Cybersecurity trainings for staff and managers	annual	NA	At least two trainings per year
9.3 Provide support services in the EU Agencies network and in key areas of the Agency's expertise and chair EUAN in 2025	Cybersecurity advisory in 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	NA	>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/accessible within ENISA	Annual	29%	55%
			Response timeliness to external parties (internal reporting)	Annual	NA	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: 743.000*	*FTE: 14*[40]
Other supplementary contribution	Budget: 54.604 SLA with ECCC, see annex XI for additional information	FTE: 0

[40] Including ED, COO, advisor and accounting officer

Activity 10: Reputation and Trust

OVERVIEW OF ACTIVITY

This activity seeks to meet requirements set out in Art 4(1) of the CSA that sets an objective for the Agency to: “be a centre of expertise on cybersecurity by virtue of its **independence**, the scientific and technical **quality of the advice and assistance it delivers**, the information it provides, the **transparency of its operating procedures**, the **methods of operation**, and its **diligence in carrying out its tasks**”. This objective requires that a transparent and proactive approach is taken to maximise the quality and value provided to stakeholders. It also includes contribution to efficiency gains, by optimising the way it engages with stakeholders and offering on demand driven services in addition to the essential services to increase the Agency’s outreach.

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

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

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

ACTIVITY 10 ANNUAL OBJECTIVES

DESCRIPTION	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	LATEST RESULT	TARGET
10.a Protect and grow the Agency’s brand	Ensure efficient corporate services	Level of trust in ENISA (as per Biannual Stakeholder Survey)	Biennial	95%	95%
		ENISA brand management	Annual	N/A	Target set in crisis communications playbook by 2025
10.b Improve outreach of ENISA’s o 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 Engaged communities Increased impact of ENISA activities Relevant and easily accessible information is provided to stakeholders Successful EUAN leadership, communications and EUAN yearly meetings	Management Team and agency stakeholders	Number & types of activities at each engagement level (stakeholder strategy implementation)	Annual (Internal report)	N/A	Stakeholder strategy under review
			Number of social media engagement	Annual (Media monitoring)	75k	>80k
			Stakeholder satisfaction with ENISA outreach	Biennial (survey)	N/A	>80%
			Number of total ENISA website visits	Annual (website analytics)	2.03 million	>2.5 million
			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 the operation and organisation of ENISA statutory bodies Support effectiveness of implementation of work programme (validation of operational outputs) Providing administrative support for the day to day working of the Management board decisions and recommendations from NLO & AG	Statutory bodies, Management Team and Committees	Number of feedback instantiations received per NLO consultation	Annual (Internal report)	N/A	>6
			Number of feedback instantiations received per AG consultation	Annual (Internal report)	N/A	>8
			Satisfaction of statutory bodies with ENISA 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: 760.000*	*FTE:8.5*

Activity 11 Effective and efficient corporate services

OVERVIEW OF ACTIVITY

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

ENISA aims to develop its human resources to align with the Agency’s goals and needs, by attracting, retaining, and nurturing talent while enhancing its reputation as an agile, knowledge-driven organization where staff can grow, stay motivated, and remain engaged. A key priority is competency development, positioning ENISA as an "employer of choice" and a rewarding workplace for all.

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

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

ACTIVITY 11 ANNUAL OBJECTIVES

DESCRIPTION	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	LATEST RESULT	TARGET
11.a Enhance people centric services by implementing the Corporate and HR strategy	Effective workforce planning and management	Implementation of Strategic Workforce Planning and Review decisions	Annual	Fully implemented	Fully implemented

	Efficient talent acquisition, development and retainment	Implementation of the Corporate and HR strategy		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 Introduce digital solutions that maximise synergies and collaboration in the Agency Developing service propositions with additional external resourcing Promote and enhance ecologic sustainability across all Agency's operations Develop efficient framework for ENISA continuous governance to safeguard high level of IT and physical security	Implement best practices in sustainable IT solutions	Annual	N/A	IT strategy updated accordingly
		Limited disruption of continuity of corporate services	Annual	N/A	BCP for corporate IT, facilities, financial and HR services in 2025
		Handling EUCI at the level of SECRET UE/EU SECRET	Annual	N/A	Operational for the first full year, in 2025

ACTIVITY 11 OUTPUTS

DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	TARGET 2025[41]
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. Implementation of the ED decision on annual workforce review [adopted in April 2024]	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 of the implementation of approved Recruitment plan		n/a	>90%
			Percentage of the implementation		n/a	>90%

[41] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023

			of approved Procurement Plan			
			Percentage of procurement procedures launched via e-tool (PPMT)		100%	>90%
			Percentage of 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%
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. and 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, safesecure and streamlined ways of working and introducing self-service functionalities	Service such as access management, meeting room facilities, equipment renewal, cloud-based solutions and data availability are efficient.	Management Team IT Management Committee	Critical systems uptime//downtime	Annual	100 %	99 %
			Staff satisfaction with IT resolution		84 %	85 %

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

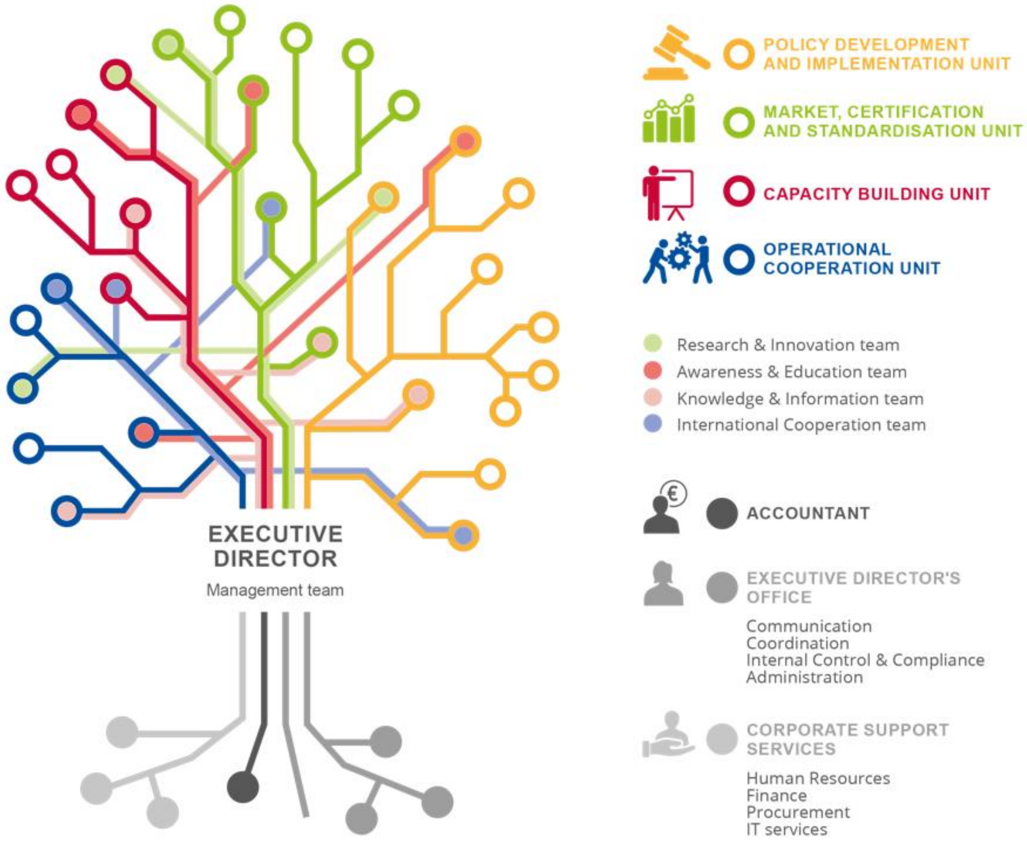
Involve / Engage: Private Sector and International Organisations

ACTIVITY 11 RESOURCE FORECASTS

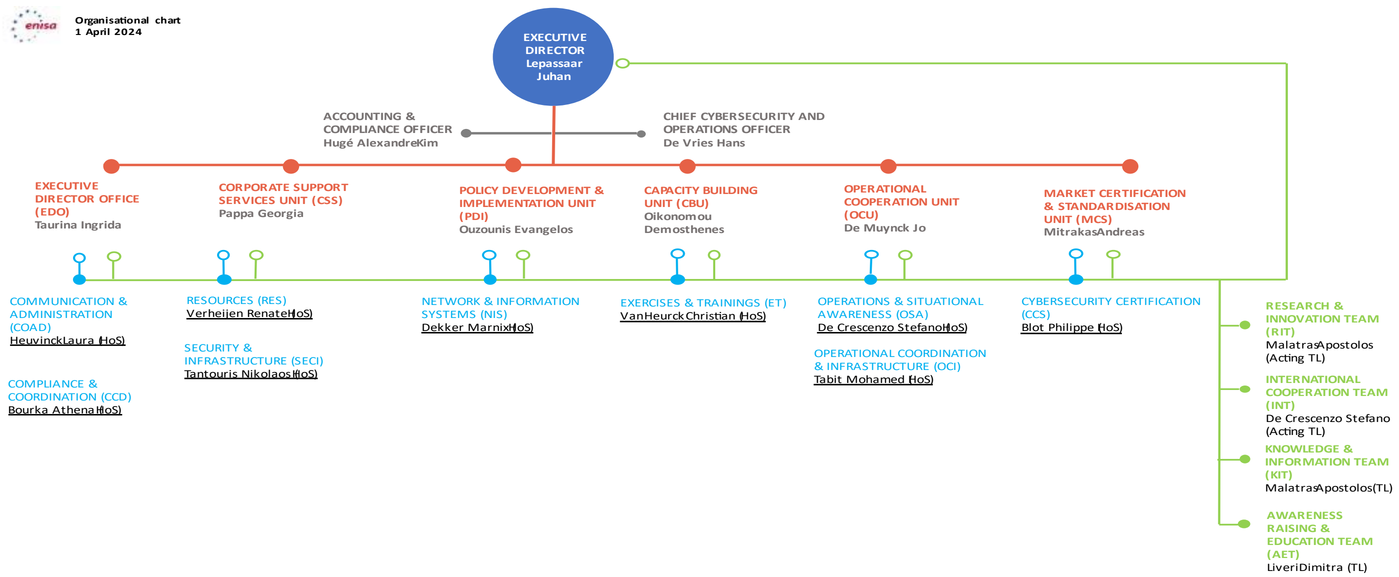
	Budget	FTEs
Total activity resources	*Budget: 4.631.348*	*FTE: 21.25*

ANNEX

I. ORGANISATION CHART AS OF 31.12.2023


EXECUTIVE DIRECTOR
Management team
POLICY DEVELOPMENT AND IMPLEMENTATION UNIT
MARKET, CERTIFICATION AND STANDARDISATION UNIT
CAPACITY BUILDING UNIT
OPERATIONAL COOPERATION UNIT
Research & Innovation team
Awareness & Education team
Knowledge & Information team
International Cooperation team
ACCOUNTANT
EXECUTIVE DIRECTOR'S OFFICE
Communication
Coordination
Internal Control & Compliance
Administration
CORPORATE SUPPORT SERVICES
Human Resources
Finance
Procurement
IT services

Administrative Organigramme



Organisational chart
1 April 2024

EXECUTIVE DIRECTOR
Lepassaar Juhan

ACCOUNTING & COMPLIANCE OFFICER
Hugé AlexandreKim

CHIEF CYBERSECURITY AND OPERATIONS OFFICER
De Vries Hans

EXECUTIVE DIRECTOR OFFICE (EDO)
Taurina Ingrida

- COMMUNICATION & ADMINISTRATION (COAD)
  HeuvinckLaura (HoS)
- COMPLIANCE & COORDINATION (CCD)
  Bourka Athena(HoS)

CORPORATE SUPPORT SERVICES UNIT (CSS)
Pappa Georgia

- RESOURCES (RES)
  Verheijen Renate(HoS)
- SECURITY & INFRASTRUCTURE (SECI)
  Tantouris Nikolaos(HoS)

POLICY DEVELOPMENT & IMPLEMENTATION UNIT (PDI)
Ouzounis Evangelos

- NETWORK & INFORMATION SYSTEMS (NIS)
  Dekker Marnix(HoS)

CAPACITY BUILDING UNIT (CBU)
Oikonomou Demosthenes

- EXERCISES & TRAININGS (ET)
  VanHeurck Christian (HoS)

OPERATIONAL COOPERATION UNIT (OCU)
De Muynck Jo

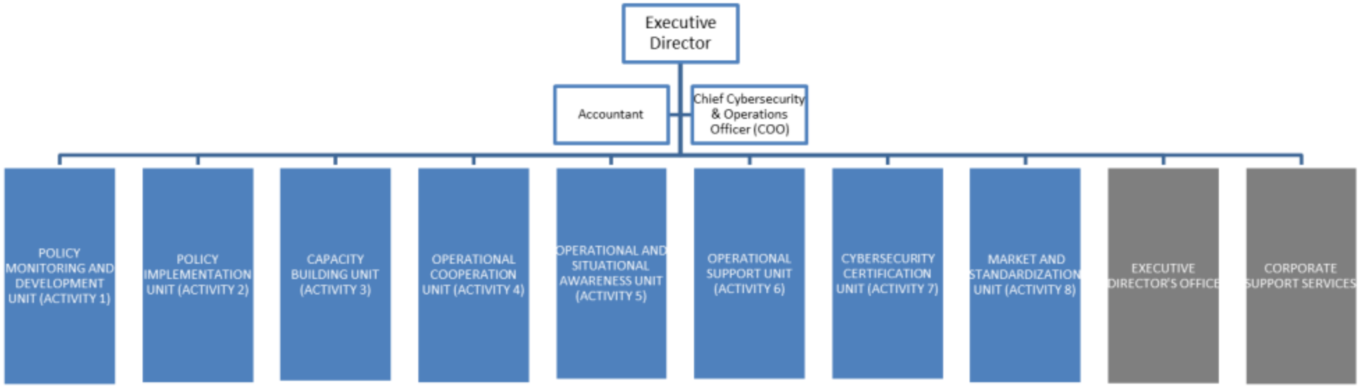
- OPERATIONS & SITUATIONAL AWARENESS (OSA)
  De Crescenzo Stefano(HoS)
- OPERATIONAL COORDINATION & INFRASTRUCTURE (OCI)
  Tabit Mohamed (HoS)

MARKET CERTIFICATION & STANDARDISATION UNIT (MCS)
MitrakasAndreas

- CYBERSECURITY CERTIFICATION (CCS)
  Blot Philippe (HoS)

- RESEARCH & INNOVATION TEAM (RIT)
  MalatrasApostolos (Acting TL)
- INTERNATIONAL COOPERATION TEAM (INT)
  De Crescenzo Stefano (Acting TL)
- KNOWLEDGE & INFORMATION TEAM (KIT)
  MalatrasApostolos(TL)
- AWARENESS RAISING & EDUCATION TEAM (AET)
  LiveriDimitra (TL)

ENISA new organigramme 2025


Executive Director
Accountant
Chief Cybersecurity & Operations Officer (COO)
POLICY MONITORING AND DEVELOPMENT UNIT (ACTIVITY 1)
POLICY IMPLEMENTATION UNIT (ACTIVITY 2)
CAPACITY BUILDING UNIT (ACTIVITY 3)
OPERATIONAL COOPERATION UNIT (ACTIVITY 4)
OPERATIONAL AND SITUATIONAL AWARENESS UNIT (ACTIVITY 5)
OPERATIONAL SUPPORT UNIT (ACTIVITY 6)
CYBERSECURITY CERTIFICATION UNIT (ACTIVITY 7)
MARKET AND STANDARDIZATION UNIT (ACTIVITY 8)
EXECUTIVE DIRECTOR'S OFFICE
CORPORATE SUPPORT SERVICES

II. RESOURCE ALLOCATION PER ACTIVITY 2025 - 2027

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

The following assumptions are used in the simplified ABB methodology:

- Budget granted to ENISA through the Contribution Agreement signed in 2023 is not included in the calculations as activities (as well as budget) defined in the mentioned agreement span through 2024-2026.
- 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.
- Budget allocation of each activity includes Direct and Indirect budget attributed to each activity.
- Direct Budget is the cost estimate of each of the 8 operational activities as indicated under Section 3.1 of the SPD 2025-2027 (carried out under Articles 5-12) in terms of goods and services to be procured.
- Budget for operational missions and large scale operational events is allocated to operational activities (Activities 1-8) based on the direct FTEs under each activity.
- Indirect Budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs, attributable to each activity. The indirect budget is allocated to activities based on different drivers. Main driver for costs allocation was number of foreseen direct FTEs for each operational activity in 2025.
- In order to estimate full costs of operational activities, both corporate activities (Activities 9 to 11) should be distributed accordingly to all operational activities based on respective drivers.

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (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	15,27
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 where budget of EUR 20 million has been granted as well as 12 FTEs for implementation of agreed activities during 2024-2026.

III. FINANCIAL RESOURCES 2025 - 2027

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

Revenues	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**

REVENUES	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	3,06%	25.716.933	26.213.532	26.719.532
- of which assigned revenues deriving from previous years' surpluses	*320.868*		*150.299*	*0*	*0*
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	883.404	-19,25%	713.309	716.654	738.500
*- of which EEA/EFTA (excl. Switzerland) ***	*883.404*	*-19,25%*	*713.309*	*716.654*	*738.500*
- 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

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 CRA single reporting platform, further actions for Support Action, SitCen and CRA-SRP, Cyber Reserve and SitCen are under discussion.

Table 3: Budget outturn and cancellation of appropriations

Budget outturn	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**

Budget 2023 outturn amounts to EUR 150 299.

With steady budget increase over the last years up to EUR 25,2 million in 2023 a commitment rate of 100,00 % (99,93 % in 2022 and 99,51 % in 2021) of appropriations of the year (C1 funds) at year end has been reached which shows the already proven capacity of the Agency to fully implement its annual appropriations.

In 2023 commitment appropriations were cancelled for an 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 ‘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 of 2022 carried over to 2023 were utilized at a rate of 99,20 % (automatic carry-overs) which indicates a proven capability of estimation of needs (in 2022 – 95,07 %). From the total amount of EUR 18 782 626 carried forward, the amount of EUR 149 739 was cancelled (or 0,80 %). This cancellation represents 0,38 % of the total committed appropriations 2022 of EUR 39 179 406 (fund source C1).

IV. 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 SNE

STAFF	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	**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)[42]	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 STAFF[43]	**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[44]	12+3*	pm
Seconded National Experts (SNE)	n/a	n/a	n/a	n/a	n/a
TOTAL	n/a	12	12+3*	12+3*	pm

Other Human Resources

- Structural service providers

	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

[42] Article 38.2 of the ENISA Financial Rules allows the opportunity to “offset the effects of part-time work”. ENISA will explore this option in 2025 and may use this option in the future to offset long-term absences and part-time work with short term contracts of CA.

[43] Refers to TAs, CAs and SNEs figures

[44] *Pending final contribution agreements to be signed see annex XI

- 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 contribution agreement	30 + 11 contribution agreement	30 + 10 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 2025 following retirement / mobility or new requested posts

JOB TITLE IN THE AGENCY	TYPE OF CONTRACT (OFFICIAL, TA OR CA)		TA/OFFICIAL **Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication ***		CA **Recruitment Function Group (I, II, III and IV)**
	Due to foreseen retirement/ mobility	**New post requested due to additional tasks**[45]	**Internal (brackets)**	**External (brackets)**	
Expert	1 TA	n/a	n/a	n/a	n/a
Officer		n/a	n/a	n/a	n/a
Assistant		n/a	n/a	n/a	n/a

[45] Posts stemming from the required resources for 2025 work programme (11.5 FTEs)

V. HUMAN RESOURCES - QUALITATIVE

A. Recruitment policy

Implementing rules in place:

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

B. Appraisal and reclassification/promotions

Implementing rules in place:

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

Table 1: **Reclassification of TA/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 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	HOW MANY STAFF MEMBERS WERE RECLASSIFIED IN YEAR 2023	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 on 31.12.2023 statutory staff (only temporary agents and contract agents)

		OFFICIAL		TEMPORARY		CONTRACT AGENTS		GRAND TOTAL	
		Staff	**%**	**Staff**	**%**	**Staff**	**%**	**Staff**	**%**
Female	Administrator level	-	-	23	29%	11	44%	34	32%
	Assistant level (AST & AST/SC)	-	-	13	16%	4	16%	17	16%
	Total	-	-	**36**	**45%**	**15**	**60%**	**51**	**49%**
Male	Administrator level	-	-	39	49%	7	28%	46	44%
	Assistant level (AST & 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 OF THE MIDDLE AND SENIOR MANAGEMENT (31.12.2023)**	**2019**		**31.12.2023**	
	Number	**%**	**Number**	**%**
Female Managers	2	20%	2[46]	29%
Male Managers	8	80%	5[47]	71%

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

D. Geographical Balance

Table 1: Data on 31.12.2023 - statutory staff only

[46] This category comprises the ED and Heads of Unit level (Team Leaders not included)
[47] This category comprises the ED and Heads of Unit level (Team Leaders not included)

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 *48	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%

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

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 EC on type I European schools	**No**
Contribution agreements signed with the EC on type II European schools	**Yes**

VI. ENVIRONMENT MANAGEMENT

The Management Board of ENISA established – within the Agency's SPD for 2022-2024 – a goal for the Agency to achieve climate neutrality (defined as zero CO2, CH4 and N2O emissions) across all its operations, by 2030. As a first step, the agency undertook already an exercise in 2022 to map its current climate footprint by conducting audit of past ENISA emissions for which 2019 and 2021 were used as reference years.
ENISA further strengthened its environmental management and carried out an overarching audit in course of 2023, on the CO2 impact of all the operations of the agency in 2023.

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

- ENISA with the assistance of an external contractor completed a technical study for the assessment of the carbon footprint calculation for 2022 and works towards assessing its 2023 carbon footprint calculation in Q4 2024.
- Several actions for the reduction of GHGs emissions were further implemented that included recycling of office waste in a structured manner (via dedicated recycling bins and guidelines on the proper use of the bins), advancement of the watering system, incorporation of GHG emissions provisions to the agency's public procurement procedures and tenders, awareness raising sessions and dedicated trainings to all staff about EMAS and the greening initiatives of the agency.
- In course of 2024 the registration and implementation of an environmental management system (according to the EMAS regulation) also took place with the creation of EMS (European Management System) templates and procedures.
- An internal audit and environmental performance evaluation took also place in course of 2024.
- The agency also proceeded to the drafting of its environmental statement for which the formal approval by ENISA's management Team is also anticipated in Q4 of 2024.
- An external verification to be concluded in course of Q4 2024.
- Externally communicate via ENISA's website about EMAS and the greening initiatives of the agency (Q4 2024 and Q1 2025).

Planned actions for 2025

- The assessment of the carbon footprint calculation of the agency for 2024.
- A call for volunteers to renew the greening network members of the agency.

- Continue the awareness raising actions (i.e repeat trainings to the staff and dedicated Q&As, make available to the staff multi-purpose cups made out of recycling materials etc.)

Additionally, the Agency aims to reduce greenhouse gas emissions in alignment with the approach taken by the Commission[49]. The corporate strategy outlines objectives to decrease the number of in-person events and participation in physical gatherings, favoring hybrid or online formats instead.

VII. BUILDING POLICY

Current buildings:

Building Name and type	Location	Location SURFACE AREA(in m²)			RENTAL CONTRACT			Host country (grant or support)	Building present value(€)
		Office space (m2)	non-office (m2)	Total (m2)	Rent (euro per year)	Duration	Type		
Heraklion Office	Heraklion	706		706		01/01/2021 to 28/02/2030;	Lease	Rent is fully covered by Hellenic Authorities	N/A
Athens Office	Chalandri	4498	2617	7115		01/01/2021 to 28/02/2030;	Lease	Rent is fully covered by Hellenic Authorities	N/A
Brussels office	Brussel centre	98		98	56.496	N/A	SLA with OIB		N/A
Total	Location	5302	2617	7920					

Brussels office

The office is being used on a daily basis by Brussels based staff, which is a significant benefit for the operational activities of the Agency as they are able to communicate readily with the CERT EU Team situated on the same floor. 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 & maintenance costs)	**130.000**	**130.000**	**130.000**

VIII. PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff

[49] Communication to the Commission - Greening the Commission | European Commission (europa.eu)

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

IX. EVALUATIONS

In 2023, the agency conducted stakeholder satisfaction survey to gather feedback on the outcomes/results of ENISA work over the past two reporting periods (2021 and 2022). The next stakeholder satisfaction survey for the period 2023 to 2024 will be executed in Q1 2025. The survey like 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 demonstrate high added value of ENISA's deliverables with 93 % of stakeholders finding significant added value in the outcome / results of ENISA's work. Only 7 % find limited added value and no stakeholder finds no added value. In terms of take up, 85 % of stakeholders also rate the likelihood of taking up the results of ENISA work in support of their 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 the agency carry out its tasks while avoiding the duplication of Member State activities, therefore the result of 2023 that 83,7 % of stakeholders find that ENISA deliverables do not duplicate or only somewhat duplicate Member State activities is tantamount to ENISA's effort to involve stakeholders in all stages of its work and ensure that the outcomes / results are fit for purpose. However, duplication in some areas is unavoidable due to the nature of the work and the need for MS to have their own capacities, as such ENISA will take action to increase efforts to focus its work even more on high added-value / low duplication areas and specifically introduced targets in the work programme to reduce duplication of MS activities.

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

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

As adopted by the Management Board[50], the Agency's strategy for effective internal controls is based on international practices (COSO Framework's international Standards), as well the relevant internal control framework of the European Commission.

[50] 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)

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

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

The Control Activities ensure the mitigation of risks related to the achievement of policy, operational and internal control objectives. They are performed at all levels of the organisation, at various stages of business processes, and across the technology environment. They may be preventive or detective and encompass a range of manual and automated activities as well as segregation of duties.

Information is necessary for the Agency to carry out internal controls and to support the achievement of objectives. In this respect, it is needed to consider both external and internal communication. External communication provides the Agency's stakeholders and globally the EU citizens with information on ENISA's policy, objectives, actions and achievements. Internal communication provides ENISA staff with the information required to support the achievement of objectives and the awareness for day-to-day controls.

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

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

Moreover, since 2021 ENISA has been implementing its anti-fraud strategy[51], 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 in the beginning of 2025 for endorsement.

[51] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-5-on-anti-fraud-strategy

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

	SLA	Date of signature	Total amount	Duration	Counterpart	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	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 mil (80% prefinancing)	up to 31/12/26	DG CNECT	The purpose of this Agreement is to provide a financial contribution toimplement 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.	est. 11 FTEs
2	Support Action fund (activities 5 & 6)	Pending	Up to. 15 mil	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. • The establishment of the Cyber Resilience Act single reporting platform. • Management, and maintenance of day-to-day operations of the 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 financial contribution to conduct a feasibility study on single reporting platform under the Cyber Resilience Act that will inform the future steps of the platform development.	2 FTEs

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

The international strategy confirms the Agency's mandate in terms of its and focus on the EU and EU actors, while also allowing increased flexibility to engage with international partners in line with the strategic objectives outlined in the ENISA Strategy for a Trusted and Cyber Secure Europe of July 2020 and in support of the EU's international priorities. The Agency's international strategy[52] was adopted by the MB during the 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.

XIII. ANNUAL COOPERATION PLAN 2025

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

XIV. PROCUREMENT PLAN 2025

The indicative procedures from 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
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

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

Corporate Support services	SIP Landline Voice Telephony services	Open procedure	Q1 2025	30.05.2025	€ 80,000.00
Corporate Support services	Maintenance of safety & security systems	Open procedure	Q2 2025	10.07.2025	€ 150,000.00
Executive Directors Office	Digital Communications services	Open procedure	Q3 2025	01.12.2025	€ 400,000.00
Resilience of Critical Sectors	Supporting activities in the area 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 € 10 634 702.

XX-00-00-000-XX-X

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

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

Annex I of the MB Decision No 16/2024

Statement of Estimates 2025 (Budget 2025)

European Union Agency for Cybersecurity

CONTENTS

1. General introduction
2. Justification of main headings
3. Statement of Revenue 2025
4. Statement of Expenditure 2025

1. GENERAL INTRODUCTION

Explanatory statement

Legal Basis:

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

Reference acts

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

2. JUSTIFICATION OF MAIN HEADINGS

2.1 Revenue in 2025

The 2025 total revenue amounts to € 26430242 and consists of a subsidy of € 25716933 from the General Budget of the European Union and EFTA countries' contributions € 883404

Subsidy from the Greek Government for the rent of the offices of ENISA in Greece is no longer available as rent is directly covered by Greece

On 21 December 2023 the Contribution Agreement between DG CONNECT and ENISA was signed with the purpose to provide ENISA with financial contribution to implement the ‘Preparedness and Incident Response Support for Key Sectors’ action under the Digital Europe Programme (DEP) which grants ENISA a total of € 20000000 for implementation of agreed actions during the period 2024-2026. Amount of € 16000000 has been received in February 2024 as the first instalment.

Contribution Agreement for CRA single reporting platform is currently at draft stage with the indicated amount of € 400000. Other contribution agreements are pending.

ENISA has signed a few SLAs with other EU Agencies for provision of services where revenue is expected to reach € 169804.

2.2 Expenditure in 2025

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

Title 1 - Staff

The estimate of Title 1 costs is based on the Establishment Plan for 2025, which contains 83 Temporary Agent posts.

Total expenditure under Title 1 amounts to € 15.271.440

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to € 4.159.348

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of
Work Programme 2025 and amounts to € 6.999.454

Title 4 - Externally funded activities

Expenditure under Title 4 amounts to p.m.

3. STATEMENT OF REVENUE 2025

Title	Heading	Voted Appropriations 2023 €	Voted Appropriations 2024 €	Amended Budget 2024 €	Draft Appropriations 2025 €	Remarks - budget 2025
1	**EUROPEAN COMMUNITIES SUBSIDY**	24.475.757	24.953.071	24.953.071	25.716.933	Total subsidy of the European Communities
2	**THIRD COUNTRIES CONTRIBUTION**	707.738	883.404	883.404	713.309	Contributions from Third Countries.
3	**OTHER CONTRIBUTIONS**	0	0	16.000.000	p.m.	Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA under the Digital Europe Programme (DEP). Contribution Agreement for CRA single reporting platform currently at draft stage.
4	**ADMINISTRATIVE OPERATIONS**	0	0	p.m.	p.m.	Other expected income from other operations including under SLAs with other EU Agencies.
	GRAND TOTAL	**25.183.495**	**25.836.475**	**41.836.475**	**26.430.242**	

Article Item	Heading	Voted Appropriations 2023 €	Voted Appropriations 2024 €	Amended Appropriations 2024 €	Draft Appropriations 2025 €	Remarks - budget 2025
1	**EUROPEAN COMMUNITIES SUBSIDY**					
10	**EUROPEAN COMMUNITIES SUBSIDY**					
100	***European Communities subsidy***	24.475.757	24.953.071	24.953.071	25.716.933	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security.
100	***European Communities subsidy - Expansion of Activities 3, 4, 5***	n/a	n/a	n/a	n/a	*As per Letter of intent between DG CONNECT and ENISA on the provision of support to Member States to further mitigate the risks of large scale cybersecurity incidents in the short term, dated 20 July 2022, ref. Ares(2022)5473716 - 29/07/2022*
	CHAPTER 10	24.475.757	24.953.071	24.953.071	25.716.933	
	TITLE 1	**24.475.757**	**24.953.071**	**24.953.071**	**25.716.933**	
2	**THIRD COUNTRIES CONTRIBUTION**					
20	**THIRD COUNTRIES CONTRIBUTION**					
200	***Third Countries contribution***	707.738	883.404	883.404	713.309	Contributions from Associated Countries.
	CHAPTER 2 0	707.738	883.404	883.404	713.309	
	TITLE 2	**707.738**	**883.404**	**883.404**	**713.309**	
3	**OTHER CONTRIBUTIONS**					
30	**OTHER CONTRIBUTIONS**					
300	***External funding under Contribution Agreement***	n/a	n/a	16.000.000	p.m.	Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA under the Digital Europe Programme (DEP). Contribution Agreement for CRA single reporting platform currently at draft stage.
	CHAPTER 30	n/a	n/a	16.000.000	p.m.	
	TITLE 3	**n/a**	**n/a**	**16.000.000**	**p.m.**	
4	**ADMINISTRATIVE OPERATIONS**					
40	**ADMINISTRATIVE OPERATIONS**					
400	***Administrative Operations***	0	p.m.	p.m.	p.m.	Revenue from administrative operations including SLAs with other EU Agencies. Estimated amount for the year shall be € 169804 *
	CHAPTER 40	0	0	p.m.	p.m.	* Assigned revenue may be included in the estimate of revenue and expenditure only for the amounts that are certain at the date of the establishment of the estimate (Art. 20(7) of the FFR)
	TITLE 4	**0**	**0**	**p.m.**	**p.m.**	
	GRAND TOTAL	**25.183.495**	**25.836.475**	**41.836.475**	**26.430.242**	

4. STATEMENT OF EXPENDITURE 2025

Title	Heading	Voted Appropriations 2023 €	Voted Appropriations 2024 €	Amended Appropriations 2024 €	Draft Appropriations 2025 €	Remarks - budget 2025
1	**STAFF**	12.719.412	14.739.106	14.739.106	15.271.440	Total funding for covering personnel costs.
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**	3.519.470	3.666.898	3.666.898	4.159.348	Total funding for covering general administrative costs.
3	**OPERATIONAL EXPENDITURE**	8.944.613	7.430.471	7.430.471	6.999.454	Total funding for operational expenditures.
4	**EXTERNALLY FUNDED ACTIVITIES**	n/a	n/a	16.000.000	p.m.	Total external funding such as contribution agreements and SLAs.

		GRAND TOTAL	**25.183.495**	**25.836.475**	**41.836.475**	**26.430.242**	
1	**STAFF**						
11	**STAFF IN ACTIVE EMPLOYMENT**						
110	***Staff holding a post provided for in the establishment plan***						
1100	Basic salaries		8.551.219	9.877.711	9.877.711	10.314.300	Staff Regulations applicable to officials of the European Communities and in particular Articles 62 and 66 thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of permanent officials and Temporary Agents (TA).
		Article 1 1 0	8.551.219	9.877.711	9.877.711	10.314.300	
111	***Other staff***						
1110	Contract Agents		1.967.658	2.507.984	2.507.984	2.428.441	Conditions of employment of other servants of the European Communities and in particular Article 3 and Title III thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of Contract Agents (CA).
1113	Seconded National Experts (SNEs)		501.116	672.621	672.621	814.031	This appropriation is intended to cover basic salaries and all benefits of SNEs.
		Article 1 1 1	2.468.774	3.180.605	3.180.605	3.242.472	
		CHAPTER 11	**11.019.993**	**13.058.316**	**13.058.316**	**13.556.771**	
12	**RECRUITMENT/DEPARTURE EXPENDITURE**						
120	***Expenditure related to recruitment***						
1201	Recruitment and Departure expenditure		404.684	517.889	517.889	508.469	This appropriation is intended to cover the travel expenses of staff (including members of their families), the installation allowances for staff obliged to change residence after taking up their duty, the removal costs of staff obliged to change residence after taking up duty, the costs of daily subsistance allowances as per Staff Regulations applicable to officials of the European Communities (SR) and in particular Articles 20 and 71 thereof and Articles 5, 6, 7, 9, 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants. This appropriation is intended to cover expenditure related to recruitment, e.g. incurred for interviewing candidates, external selection committee members, screening applications and other related costs.
		Article 1 2 0	404.684	517.889	517.889	508.469	
		CHAPTER 1 2	**404.684**	**517.889**	**517.889**	**508.469**	

13	**SOCIO-MEDICAL SERVICES AND TRAINING**						
132	***Staff Development***						
1320	Staff Development		232.215	447.501	447.501	450.000	This appropriation is intended to cover the costs of language and other training needs as well as teambuilding and other staff development activities.
		Article 1 3 2	232.215	447.501	447.501	450.000	
133	***Staff Welfare***						
1332	Staff Welfare		691.520	307.000	307.000	238.200	This appropriation is intended to cover staff welfare measures such as the subsidy for the functioning of the School of European Education of Heraklion and other expenditure relevant to schooling & education of children of the Agency staff, health related activities to promote well-being of staff, other activities related to internal events, other welfare measures. This appropriation is also intended to cover the costs of annual medical visits and inspections, occupational doctor services as well as pre-recruitment medical costs and other costs related to medical services.
		Article 1 3 3	691.520	307.000	307.000	238.200	
		CHAPTER 1 3	**923.735**	**754.501**	**754.501**	**688.200**	
14	**TEMPORARY ASSISTANCE**						
142	***Temporary Assistance***						
1420	External Temporary Staffing		371.000	408.400	408.400	518.000	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
		Article 1 4 2	371.000	408.400	408.400	518.000	
		CHAPTER 1 4	**371.000**	**408.400**	**408.400**	**518.000**	
		Total Title 1	**12.719.412**	**14.739.106**	**14.739.106**	**15.271.440**	
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**						
20	**BUILDINGS AND ASSOCIATED COSTS**						
200	**Buildings and associated costs**						
2001	Building costs		1.357.750	1.000.719	1.000.719	1.081.300	This appropriation is intended to cover various building related costs including the payment of rent for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces, utilities and insurance of the premises of the Agency, cleaning and maintenance of the premises used by the Agency, fitting-out of the premises and repairs in the buildings, costs of building surveillance as well as purchases and maintenance cost of equipment related to security and safety of the building and the staff, expenditure of acquiring technical equipment, as well as maintenance and services related to it, and other costs such as for example market survey costs for rent of buildings, costs of moving to and/or establishing new premises of the Agency and other handling costs.
		Article 2 0 0	1.357.750	1.000.719	1.000.719	1.081.300	
		CHAPTER 2 0	**1.357.750**	**1.000.719**	**1.000.719**	**1.081.300**	
22	**CURRENT CORPORATE AND ADMINISTRATIVE EXPENDITURE**						

222	***Consultancy and other outsourced services***						
2220	Consultancy and other outsourced services (incl. legal services)		379.650	438.125	438.125	612.000	This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. in HR area, financial, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy and/or other administrative support services provided by third parties including EC management costs.
		Article 2 2 2	379.650	438.125	438.125	612.000	
223	***Corporate and Administrative Expenditures***						
2230	Corporate and Administrative Expenditures		93.000	78.000	78.000	75.000	This appropriation is intended to cover corporate and administrative expenditure such as the costs of purchasing, leasing, and repairs of furniture, the costs of maintenance and repairs of transport equipment as well as insurance and fuel, the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions, the costs of office stationery and the purchase of office kitchen consumables, post office and special courrier costs, bank charges, interest paid and other financial and banking costs and other costs of corporate administrative nature.
		Article 2 2 3	93.000	78.000	78.000	75.000	
		CHAPTER 2 2	**472.650**	**516.125**	**516.125**	**687.000**	
23	**ICT**						
231	***Core and Corporate ICT expenditure***						
2312	Core and corporate ICT costs		1.689.070	2.150.054	2.150.054	2.391.048	This appropriation is intended to cover core and corporate ICT costs including recurrent corporate ICT costs (including support and consulting services) as well as new investments and one-off projects for hardware, software, services and maintenance as well as ENISA website and portals support and corporate cybersecurity aspects.
		Article 2 3 1	1.689.070	2.150.054	2.150.054	2.391.048	
		CHAPTER 2 3	**1.689.070**	**2.150.054**	**2.150.054**	**2.391.048**	
		Total Title 2	**3.519.470**	**3.666.898**	**3.666.898**	**4.159.348**	
3	**OPERATIONAL EXPENDITURE**						
30	**ACTIVITIES RELATED TO OUTREACH AND MEETINGS**						
300	***Outreach, meetings and representation expenses***						
3001	Outreach, meetings, translations and representation expenses		438.600	387.000	387.000	768.800	This appropriation is intended to cover costs of outreach activities (communications, stakeholders' management, publication and translations), meetings of statutory bodies (i.e. MB, AG, NLOs, and meetings with other stakeholders) and other representation costs. It also covers mission costs for the ED, COO, ACOO as well as missions related to the implementation of Activities 9-11 as defined in the SPD 2025-2027 mainly covering horizontal tasks and other administrative services.
3002	Operational missions		n/a	n/a	n/a	512.200	This appropriation is intended to cover costs of operational missions related to the implementation of Activities 1-8 as defined in the SPD 2025-2027 related to performing operational tasks.
3003	Large scale operational events		n/a	n/a	n/a	255.000	This appropriation is intended to cover costs of large scale operational events (>50 participants) related to the implementation of Activities 1-8 as defined in the SPD 2025-2027 related to performing operational tasks.
		Article 3 0 0	438.600	387.000	387.000	1.536.000	
		CHAPTER 3 0	**438.600**	**387.000**	**387.000**	**1.536.000**	
36	**CORE OPERATIONAL ACTIVITIES**						
361	***Activity 1***						
3610	Activity 1 - Support for policy monitoring and development		n/a	n/a	n/a	294.037	This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT).
		Article 3 6 1	n/a	n/a	n/a	294.037	
362	***Activity 2***						
3620	Activity 2 - Supporting implementation of Union policy and law		n/a	n/a	n/a	331.024	This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT).
		Article 3 6 2	n/a	n/a	n/a	331.024	
363	***Activity 3***						
3630	Activity 3 - Capacity building		n/a	n/a	n/a	691.409	This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs).
		Article 3 6 3	n/a	n/a	n/a	691.409	
364	***Activity 4***						

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

37	CORE OPERATIONAL ACTIVITIES					
371	***Activity 1 - Providing assistance on policy development***					
3710	Activity 1 - Providing assistance on policy development	330.262	357.135	357.135	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 1	330.262	357.135	357.135	n/a	
372	***Activity 2 - Supporting implementation of Union policy and law***					
3720	Activity 2 - Supporting implementation of Union policy and law	773.404	720.268	720.268	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 2	773.404	720.268	720.268	n/a	
373	***Activity 3 - Capacity building***					
3730	Activity 3 - Capacity building	1.709.239	1.236.591	1.236.591	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 3	1.709.239	1.236.591	1.236.591	n/a	
374	***Activity 4 - Enabling operational cooperation***					
3740	Activity 4 - Enabling operational cooperation	2.122.530	1.776.494	1.776.494	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 4	2.122.530	1.776.494	1.776.494	n/a	
375	***Activity 5 - Contribute to cooperative response at Union and Member States level***					
3750	Activity 5 - Contribute to cooperative response at Union and Member States level	913.512	867.459	867.459	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 5	913.512	867.459	867.459	n/a	
376	***Activity 6 - Development and maintenance of EU cybersecurity certification framework***					
3760	Activity 6 - Development and maintenance of EU cybersecurity certification framework	804.578	571.896	571.896	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 6	804.578	571.896	571.896	n/a	
377	***Activity 7 - Supporting European cybersecurity market and industry***					
3770	Activity 7 - Supporting European cybersecurity market and industry	356.027	266.666	266.666	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 7	356.027	266.666	266.666	n/a	
378	***Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities***					
3780	Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities	811.881	711.646	711.646	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 8	811.881	711.646	711.646	n/a	
379	***Activity 9 - Outreach and education***					
3790	Activity 9 - Outreach and education	489.209	409.315	409.315	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 9	489.209	409.315	409.315	n/a	
370	***Activity 10 - Advise on Research and Innovation Needs and priorities***					
3700	Activity 10 - Advise on Research and Innovation Needs and priorities	195.371	126.000	126.000	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
	Article 3 7 0	195.371	126.000	126.000	n/a	
	CHAPTER 3 7	**8.506.013**	**7.043.471**	**7.043.471**	**n/a**	
38	CORE OPERATIONAL ACTIVITIES - ASSISTANCE FUNDS					
380	***Supplement to Activities 3, 4 and 5 - Providing assistance to Member States***					
3800	Supplement to Activities 3, 4 and 5 - Providing assistance to Member States by providing “ex-ante” and “ex-post” services	n/a	n/a	n/a	n/a	This appropriation is intended to cover direct operational costs relevant to the activities implemented according to Letter of Intent (including operational ICT and mission costs).
	Article 3 8 0	n/a	n/a	n/a	n/a	
	CHAPTER 3 8	**n/a**	**n/a**	**n/a**	**n/a**	
	TITLE 3	**8.944.613**	**7.430.471**	**7.430.471**	**6.999.454**	
4	**EXTERNALLY FUNDED ACTIVITIES ***					* The appropriations corresponding to assigned revenue shall be made available automatically, both as commitment appropriations and as payment appropriations, when the revenue has been received by the Union body (Art. 21(2) of the FFR)
40	**ACTIVITIES RELATED TO EXTERNALLY FUNDED PROJECTS**					
400	***Implementation of externally EU funded projects***					

4000	Activities related to the Contribution Agreement under DEP	n/a	n/a	16.000.000	p.m.	This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement of 21/12/2023 between DG CONNECT and ENISA with the purpose to implement the ‘Preparedness and Incident Response Support for Key Sectors’ action under the Digital Europe Programme (DEP). This Contribution Agreement covers Support Action ex-ante/ex-post and SitCen (2024-2026).
4001	Operational activities related to the implementation of SLAs	n/a	n/a	p.m.	p.m.	This appropriation is intended to cover costs of implementation of operational activities under the SLAs between ENISA and other EU Agencies.
4002	Administrative activities related to the implementation of SLAs	n/a	n/a	p.m.	p.m.	This appropriation is intended to cover costs of implementation of administrative activities under the SLAs between ENISA and other EU Agencies.
4003	Activities related to the Contribution Agreement for CRA	n/a	n/a	p.m.	p.m.	This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for CRA single reporting platform which is currently in draft stage with estimated amount of EUR 400 000. This Contribution Agreement covers CRA feasibility study (2024-2026).
4004	Activities related to the Contribution Agreement for Support Action, SitCen, and CRA-SRP	n/a	n/a	p.m.	p.m.	This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for Support Action, SitCen and CRA-SRP which is currently in draft stage. This Contribution Agreement covers Support Action incident response services (2025-2027), CRA SRP initial implementation (2025-2027) and SitCen.
4005	Activities related to the Contribution Agreement for Cyber Reserve and SitCen	n/a	n/a	p.m.	p.m.	This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for Cyber Reserve and SitCen which is currently in draft stage. This Contribution Agreement covers Cyber Reserve and SitCen (might span multiple years).
4006	Activities related to the Contribution Agreement for CRA SRP	n/a	n/a	p.m.	p.m.	This appropriation is intended to cover costs of implementation of activities under the Contribution Agreement for CRA SRP which is currently in draft stage. This Contribution Agreement covers CRA SRP operation (might span multiple years).
	Article 4 0 0	n/a	n/a	16.000.000	p.m.	
	CHAPTER 4 0	**n/a**	**n/a**	**16.000.000**	**p.m.**	
	TITLE 4	**n/a**	**n/a**	**16.000.000**	**p.m.**	
	GRAND TOTAL	**25.183.495**	**25.836.475**	**41.836.475**	**26.430.242**	

European Union Agency
for Cybersecurity

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

Adopted Establishment plan 2025

Category and grade	Establishment plan in voted EU Budget 2024		Establishment plan 2025[1]	
	Off.	TA	Off.	TA
AD 16				
AD 15		1		1
AD 14				
AD 13		2		2
AD 12		4		4
AD 11		3		3
AD 10		4		4
AD 9		14		14
AD 8		15		16
AD 7		13		13
AD 6		7		7
AD 5				
Total AD		63		64
AST 11				
AST 10				
AST 9		2		1
AST 8		1		3
AST 7		0		3
AST 6		9		6
AST 5		4		4
AST 4		2		2
AST 3		1		
AST 2				
AST 1				
Total AST		19		19
AST/SC1				
AST/SC2				
AST/SC3				
AST/SC4				
AST/SC5				
AST/SC6				

[1] Request for modification to establishment plan 2025 will be submitted in January for MB approval via written procedure.

Total AST/SC				
TOTAL		82		83