European Union Agency for Cybersecurity
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711 | e-mail: info@enisa.europa.eu
www.enisa.europa.eu

DECISION No MB/2024/01
OF THE MANAGEMENT BOARD
OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

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

THE MANAGEMENT BOARD OF ENISA,

Having regard to

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

Whereas:

1. The Management Board should produce, on the basis of the draft drawn by the Executive Director, a statement of estimates of revenue and expenditure for the following year which will be forwarded by the Management Board to the Commission by 31 January 2024;
2. The Management Board should endorse the draft programming document by 31 January 2024;
3. The Executive Board has endorsed the draft single programming document 2025-2027 at its meeting held on 24 January 2024.
4. The Agency should send the draft programming document to the Commission, the European Parliament and the Council no later than 31 January 2024;

HAS DECIDED TO ADOPT THE FOLLOWING DECISION

Article 1

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

Article 2

The Statement of estimates of revenue and expenditure for the financial year 2025 and the Establishment plan 2025 are endorsed as set-out in Annex 2 and Annex 3 of this decision.

.

Article 3

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

Done by written procedure on 20 January 2024.

On behalf of the Management Board,

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

ANNEX 1: DRAFT V.1

DOCUMENT HISTORY

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

Date	Version	Modification	Author
December 2023	V.01	MB for consultation	ENISA
January 2024	V.1	Adopted by MB	ENISA

TABLE OF CONTENTS

LIST OF ACRONYMS

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
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
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

Foreword, to be reviewed during the course of 2024, will rest on the following premises:

- Renewed ENISA strategic focus (to be set in 2024);
- ETL2024
- Need to prepare the Agency to the new upcoming tasks of CRA [and CSOA];

Main conclusions of the State of Cybersecurity in the Union report [to be adopted 2024].

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 bodies 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.

STRATEGY

EMPOWERING COMMUNITIES

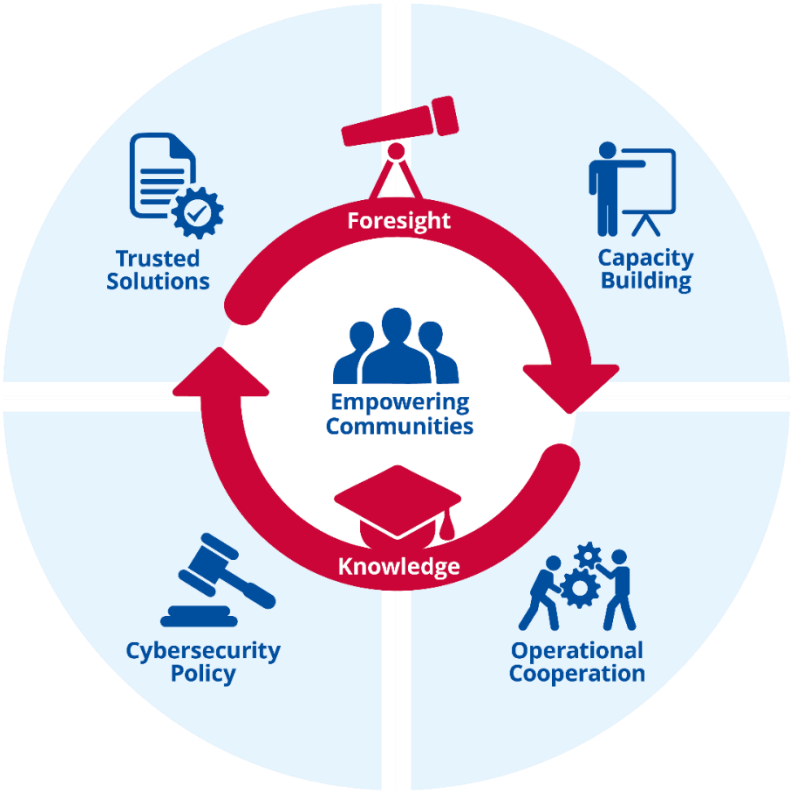
Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It strives to ensure complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

CYBERSECURITY POLICY

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity must therefore be embedded across all domains of EU policies. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

OPERATIONAL COOPERATION

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



massive (large-scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in

cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

TRUSTED SOLUTIONS

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust on digital solutions and the wider digital environment.

FORESIGHT

Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

KNOWLEDGE

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge is clearly needed. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

SECTION I. GENERAL CONTEXT

The present document provides a preliminary draft work programme for 2025. The multi-annual section including the strategic objectives stemming from the review of the ENISA strategy will be updated during the course of 2024 in preperation for its final adoption by 30 November 2024.

The 2025-2027 single programming document will undergo significant changes during the course of 2024 due to foreseen review of the ENISA strategy. Previous versions of the single programming document were tailored to the CSA and the ENISA strategy that are both under review.Therefore in anticipation of these reviews and based on lesson learned from the past three years and acknowledge the feedback from the Management Board in the 2022 Annual Activity Report the agency has on this basis put forward some prelimary adjustments that also take into account legislative changes. NIS2 was adopted and published in December 2022 and comes into force on 17th October 2024. Although some adjustments were made at the time, the current draft of the work programme has fully taken this significant legislation into consideration. Another signficant changes stems from the the CRA that is foreseen to be adopted by the end of 2023 and will come into force within the scope of the 2025-2027 programming period. This will require further adjustments and changes in this draft work programme.

In addition the European Commission has indicated the support action funded via the Digital European Programme will continue beyond 2024. Therefore existing capabilities can be fostered to achieve greater impact by aligning and consolidating existing tasks. Finally, the Management Boards decisions on reprioritising resources to the most pertinent tasks need to be reflected in the 2025-2027 single programming document.

[GENERAL CONTEXT TO BE UPDATED IN THE COURSE OF 2024]

SECTION II. MULTI-ANNUAL PROGRAMMING 2025 – 2027

[The multi-annual section including the strategic objectives stemming from the review of the ENISA strategy will be updated during the course of 2024 in preperation for its final adoption by 30 November 2024].

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA adopted a strategy for the Agency in June 2020, 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 seven 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[1], against the respective articles of the CSA [including references to tasks stemming from NIS2, CRA and CSoA]. It furthermore integrates the activities of the Work Programme showing how the progress in the achievement of the objectives is monitored. The ENISA strategy and thus the objectives will be reviewed during 2024 and thus any changes will be reflected in the following section during the course of 2024.

[1] The ENISA strategy entered into force on the 31 July 2020 and the Management Board shall launch a review procedure, as from 1st July 2024.

STRATEGIC OBJECTIVE	ACTIONS TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	INDICATOR
SO1 **Empowered and engaged communities across the cybersecurity ecosystem**	Activities 1 to 8	Art.5 to Art.12	Empowered ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure An EU-wide, state of the art body of knowledge on cybersecurity concepts and practices, that builds cooperation amongst key actors in cybersecurity, promotes lessons learned, EU expertise and creates new synergies	The % gap between demand and supply of cybersecurity skilled professionals General level of cybersecurity awareness and cyber hygiene among citizens and entities[2]
SO2 **Cybersecurity as an integral part of EU policies**	Activities 1 & 2	Art.5	Cybersecurity aspects are considered and embedded across EU and national policies	Uptake of policy recommendations adopted within the biennial report on the state of cybersecurity in the Union . Effectiveness of EU relevant policy initiatives taking cybersecurity into consideration Union level cybersecurity risk assessment and cyber threat landscape [adopted in accordance of NIS2 Art. 18(1)a] Alignment of MS national cybersecurity strategies [in accordance with NIS2 Article 7]
			Consistent implementation of Union policy and law in the area of cybersecurity, also in crucial vertical sectors EU cybersecurity policy implementation reflects sectorial specificities and needs Wider adoption and implementation of good practices	Level of maturity of cybersecurity capabilities and resources across the Union at sector level[3]
SO3 **Effective cooperation amongst operational actors within the Union in case of massive[4] cyber incidents**	Activities 4, 5 & 6	Art.7	All communities (EU Institutions and MS) use streamlined and coherent set of SOPs for cyber crises management Efficient, tools and methodologies for effective cyber crisis management	Level of cooperation and availability, (disruptions) and utilisation and trust of Union level networks, tools and databases.

[2] Article 18(1)c in NIS2
[3] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e
[4] large scale and cross-border

STRATEGIC OBJECTIVE	ACTIONS TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	INDICATOR
			Member States and institutions cooperating effectively during large scale cross border incidents or crises Public informed on a regular basis of important cybersecurity developments Stakeholders aware of current cybersecurity situation	Risk level due to cyber threats is understood by the cybersecurity communities at Union level and decision makers are able to prioritize actions to manage the risk Union level cybersecurity risk assessment and cyber threat landscape [adopted in accordance of Article 18(1)a]
			Improve MS capabilities to respond to cyber threats and incidents	Level of preparedness and response to large-scale cross-border incidents
SO4 **Cutting-edge competences and capabilities in cybersecurity across the Union**	Activities 3	Art.6 and Art.7(5)	Enhanced capabilities across the community Increased cooperation between communities	Aggregated assessment of the level of cybersecurity capabilities in the public and private sectors across the Union[5]. Aggregated assessment of the level of maturity of national cybersecurity capabilities and resources as well as the extent to which MS national cybersecurity strategies are aligned[6]
		Art.10 & Art.12	Greater understanding of cybersecurity risks and practices Stronger European cybersecurity through higher global resilience.	The % gap between demand and supply of cybersecurity skilled professionals General level of cybersecurity awareness and cyber hygiene among citizens and entities
SO5 **High level of trust in secure digital solutions**	Activities 7 & 8	Art.8	Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework versus schemes' requests and schemes' adopted Smooth transition to the EU cybersecurity certification framework Certified ICT products, services and processes are preferred by consumers / industry and where relevant, Operators of Essential Services or Digital Service	Citizens trust in ICT certified and non-certified solutions in the EU market

[5] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)b
[6] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e

STRATEGIC OBJECTIVE	ACTIONS TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	INDICATOR
			Providers under NIS1, and entities in scope of NIS2.	
			Contribution towards understanding market dynamics A more competitive European cybersecurity industry, SMEs and start-ups	Monitor metrics such as number of certificates issued under an EU scheme; number of companies interested in EU certification; growth observed in the number of CABs / or EU certification functions thereof recorded in the MS.
SO6 **Foresight on emerging and future cybersecurity challenges**	Activity 1 & 8	Art.11 & Art. 9	Research and development of cybersecurity technology reflecting the needs and priorities of the Union. Funding the development of cybersecurity technologies that meet the Union's ambition to become more resilient, autonomous and competitive.	Overall EU investment in R&I activities addressing emerging cybersecurity challenges
SO7 **Efficient and effective cybersecurity information and knowledge management for Europe**	Activity 1 & 5	Art.9	Decisions about cybersecurity take into consideration information and knowledge concerning the current and evolving cybersecurity threat landscape Stakeholders receive relevant and timely information for policy and decision making	Union level cybersecurity risk assessment and cyber threat landscape [adopted in accordance of Article 18(1)a]

The strategy of ENISA also establishes a set of values which guide the execution of its mandate and its functioning, namely:

Community Mind-Set ENISA works with communities, respecting their competencies and expertise, and fosters synergies and trust to best achieve its mission.

Excellence ENISA aims for state-of-the-art expertise in its work, upholds the highest quality standards of operation and evaluates its performance to strive for continuous improvement through innovation and foresight.

Integrity/ethics ENISA upholds ethical principles and EU relevant rules and obligations in its services and working environment ensuring fairness and inclusiveness.

Respect ENISA respects fundamental European rights and values covering all its services and working environment, as well as the expectations of its stakeholders.

Responsibility ENISA assumes responsibility thus ensuring integration of the social and environmental dimensions into practices and procedures.

Transparency ENISA adopts procedures, structures and processes that are open, factual and independent, thus limiting bias, ambiguity, fraud and obscurity.

Those values are built on the ethos of the CSA, and in particular the objectives set out in Articles 3(4) and 4(1), and have been encapsulating into two corporate objectives, which form the baseline from which the multiannual activities of the SPD will be delivered.

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 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.

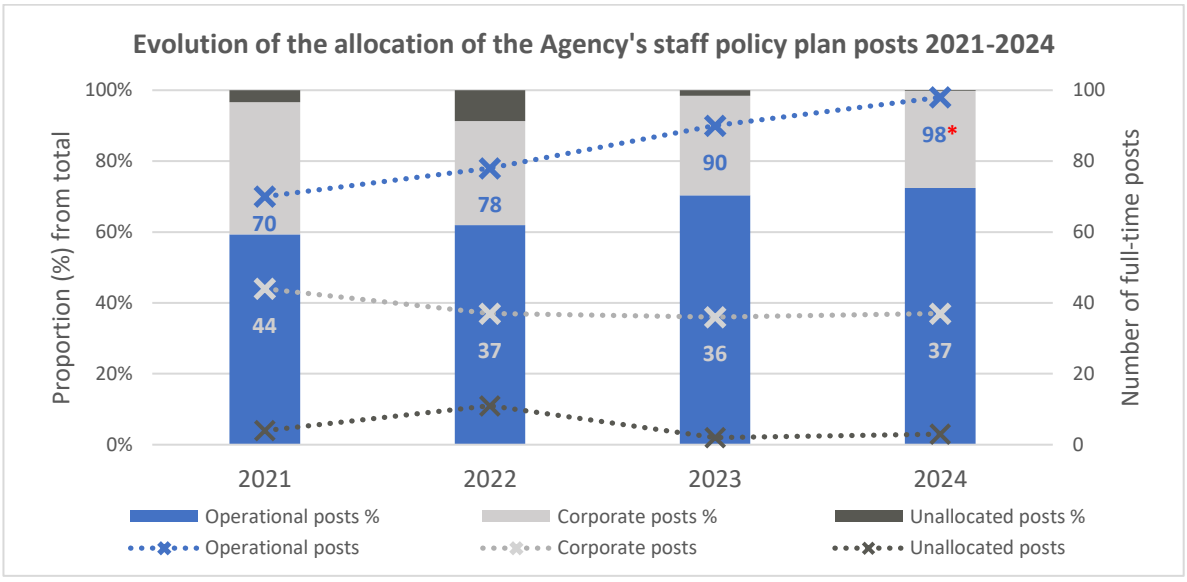
2. HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2025-2027

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[7] 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). Though the rebalancing has **increased human resources to deliver operational tasks** (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).

[7] 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 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 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 priority with the view of 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 CRA nor 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 CRA and 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 (DG CNECT),** in delivering services to increase the preparedness of Member State's critical entities and ensure capacities to assist in incident response if requested, has had a huge impact 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's cooperation, including in the Commission's Cyber Situation and Analysis Centre, gave the Agency 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 10 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 a game-changer 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 Commission's proposed Cyber Solidarity Act (CSOA) initiative];

- 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**). Structured cooperation with CERT-EU also covers Activity 3, through jointly developing and deploying exercises and trainings for EUIBAs, and in view of the resource constraints, also enabling the Agency to develop cost-based trainings and exercises

services for EUIBAs, to address increased demand and building an additional potential revenue stream for the Agency;

- As an example of the latter, a service level agreement with **EU-LISA**[8] 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;

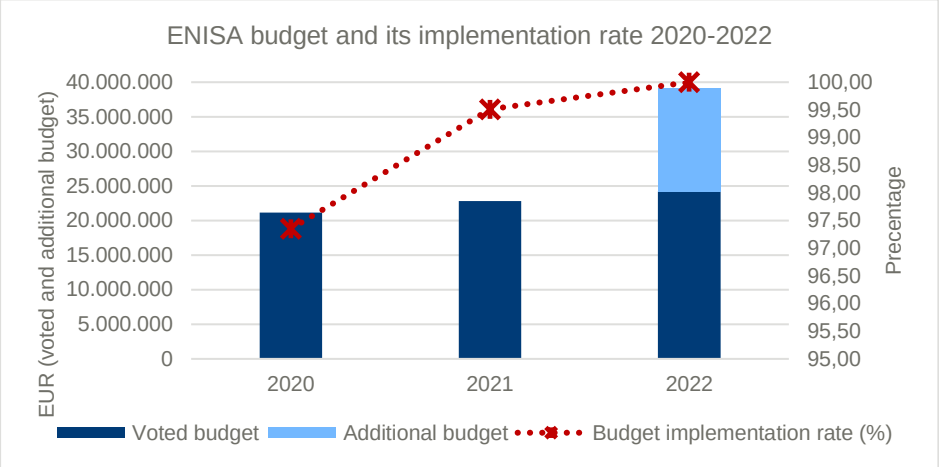
Shared services and partnerships in corporate and administrative areas. In late 2022 the Agency signed a service level agreement to create corporate synergies with the European Cybersecurity Competence Centre (**ECCC**), covering accounting, data protection and information security. ENISA has thus been 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 the period 2023-2024 ENISA, in collaboration with CERT-EU and interested EU Agencies, developed a pilot on the Cybersecurity Regulation 2023/2841. The pilot consists of a mapping exercise and a risk assessment methodology for EU Agencies. On the basis of this work, ENISA and CERT-EU will explore the options to work on guidance and for the joint provision of a shared service for EU Agencies on risk assessment that could be provided by ENISA via CERT-EU. This concept is developed in close cooperation with CERT-EU and another six EU agencies that volunteered to join this initiative. All these cooperation formats have delivered efficiency gains and/or further external income, which has enabled the Agency to prioritise its rebalancing of allocating posts to favour 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 percentage points, 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 included a combination of measures – such as imposing financial KPIs to all budget managers, better budgetary

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

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 is on the verge of executing a minimum 99% commitment rate more 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 is estimated at a minimum 96% for the voted budget and 95% 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	10	**10**
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**

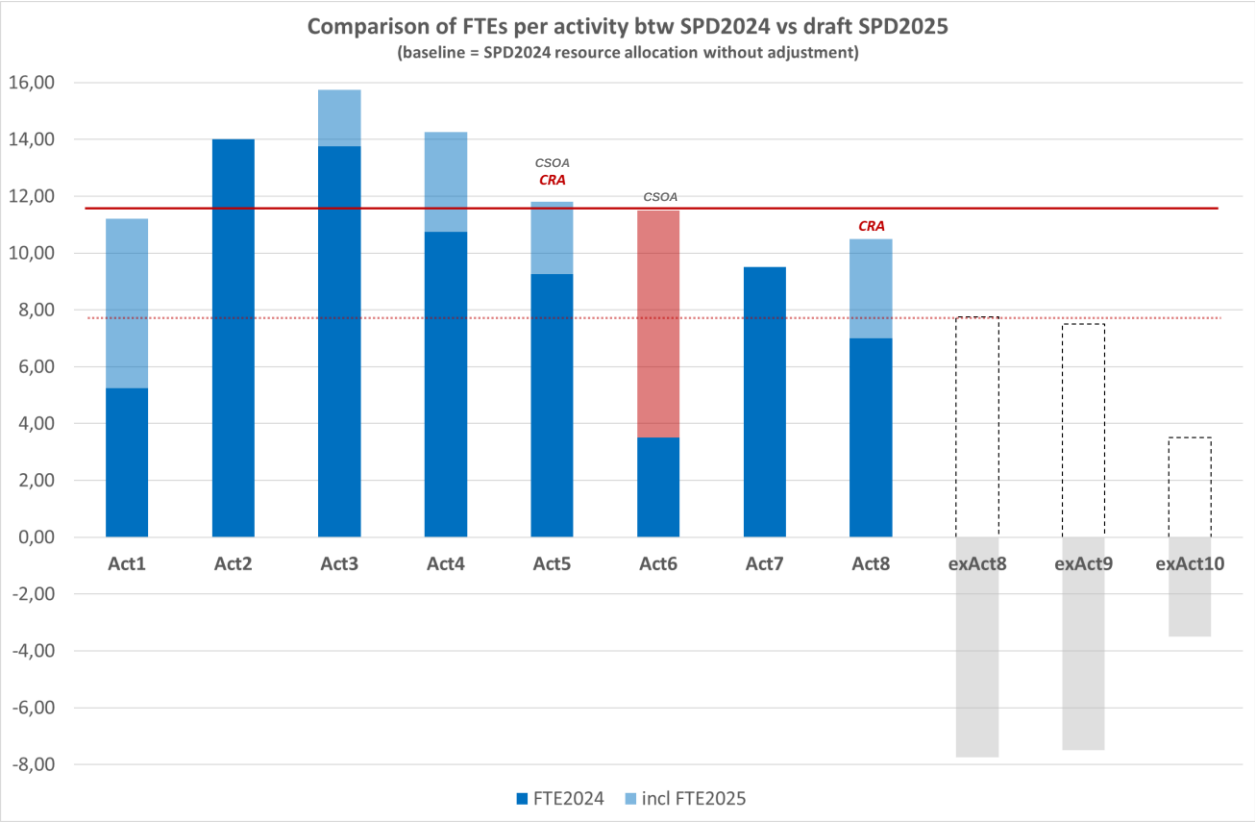
Over the past three years the Agency has taken steps to use more efficiently its human and budgetary resources. Whilst its headcount in Staff Policy Plan has increased 10 FTEs from 118 in 2021 to 128 in 2023 – which has helped it to address new tasks – the Agency has used internal restructuring of post 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 Russian war of aggression. The Union's attack surface has increased which has also brought new challenges to manage supply-chain security. The current 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***."

Moreover, new Union legislation, such the Cyber Resilience Act (CRA), and legislative initiatives such as the Cyber Solidarity Act (CSOA), will bring new tasks to the Agency which demand strenuous resourcing between 2025-2027. Though the initial financial statements accompanying those two proposals do 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 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, with the 2025 draft work programme, ENISA proposes to consolidate and restructure 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.



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 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 26.3 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, as detailed in the operational and corporate activities.

2.3.1. 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 **Cyber Resilience Act** (CRA) that was agreed late in 2023, the Commission estimated that ENISA would need about 4,5 FTEs to fulfil these new tasks. However, both legislators have noted that the Commission's initial resource estimations did not seem adequate and aligned with the seriousness of the tasks put on 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 11 (vulnerability notification) incl: *-notification handling, 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. Thus, overall, the work related to CRA can only 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** [proposal], the Commission again estimates that new assignments need about 7 FTEs to be implemented and again 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. Thus, 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 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, 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.

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)
Training and exercises (TREX)
Situational Awareness (SITAW)
Certification (CERTI)
Cybersecurity index (INDEX)

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 strategic objectives, indicators and targets for measuring the activity objectives and indicators at the output level to measure the performance of the outputs. Many of the proposed indicators have been taken from the cybersecurity index pilot run by ENISA in 2022 and will eventually be superseded by the NIS2 directive indicators to monitor high level progress towards general objectives.

Indicators will be reviewed and adjusted during the course of 2024 stemming from updates from the ENISA Strategy that will be reviewed in 2024.

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 cybersecurity advice and recommendations. ENISA will support the EC and MS on new policy initiatives[9] through evidence-based inputs into the policy development process. ENISA, in coordination with the EC and Member States 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 the Cybersecurity Policy Assessment (CSPA) service.

This activity delivers on ENISA's strategic objectives SO7 (efficient and effective cybersecurity knowledge management for Europe) and supports SO6 (foresight on emerging and future cybersecurity challenges). In particular, work under this Activity shall provide strategic long-term analysis, guidance, foresight and advice on current emerging and future cybersecurity challenges and opportunities. In terms of knowledge management, ENISA will work towards consolidating data, information and indicators concerning the status of cybersecurity across MS and the EU. 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 activity leads ENISA's efforts towards delivering the cybersecurity index (INDEX) service package, while in parallel contributing to the delivery of the NIS, TREX and situational awareness (SITAW) service packages and by providing input that can be used for future certification schemes (CERTI service package) and by providing findings and recommendations for the service packages offered to critical NISD sectors (Activity 2).

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. Given the cross-cutting nature of cybersecurity across the policy landscape, the activity will provide an up-to-date risk- based analysis of cybersecurity not only in the areas of critical infrastructure and sectors, but also by providing advice across the field in an integrated and holistic manner.

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
SO2. Cybersecurity as an integral part of EU policies SO6. Foresight on emerging and future cybersecurity challenges SO7. Efficient and effective cybersecurity information and knowledge management for Europe	1. Uptake of policy recommendations adopted within the biennial report on the state of cybersecurity in the Union10. 2. Effectiveness of EU relevant policy initiatives taking cybersecurity into consideration 3. Union level cybersecurity risk assessment and cyber threat landscape [adopted in accordance of NIS2 Art. 18(1)a] 4. Alignment of MS national cybersecurity strategies11

ACTIVITY 1 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
1. A Improve the effectiveness and consistency of EU cybersecurity policies	Art.5 CSA	2026	Assessment of ENISA advice and its influence on EU policy (stakeholder centric survey)	75% stakeholder satisfaction from ENISA's advice and influence (among EU policy makers)
1.B Increase the level of alignment and cooperation within and between Member States as well as sectors, EU institutions, bodies and agencies	Art.6 CSA Art.9 CSA	2025	Number of MS that use ENISA support and tools on the	All MS that have reviewed their NCSS use

[9] Initiatives on NIS2 sectors such as Space, AI, Telecoms, 5G, Data Governance Act/big data, data spaces, digital resilience and response to current and future crises
[10] As part of the report of the state of cybersecurity in the Union ENISA shall include policy recommendations with a view to addressing shortcomings and increasing the level of cybersecurity across the union [Art 18(2) of NIS2]
[11] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e

			implementation review and update of their NCSS.	ENISA support and tools.
1.C Knowledge and uptake of future challenges and opportunities by MS and Union actors.	Art.9 CSA	2025	Cybersecurity index indicator "emerging technology threats are considered by national risk assessments" Level of the acceptance of the report of the state of cybersecurity in the Union	European Parliament positive adoption] >70% take-up of the report by MS and Union actors All MS have considered at least 1/3 of the mapped emerging technology threats in assessing risk at national level
1.D Increase understanding of the state of cybersecurity	Art.9 CSA	2025	Use of Cybersecurity index by MS	All MS give input to cybersecurity index 2/3 of MS are using the index to inform their national cybersecurity strategies

ACTIVITY 1 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[12]**
1.1 Advise the EC and Member States in reviewing the effectiveness of current cybersecurity policy frameworks	Stakeholders will use evidence to understand how implemented policies have affected the targeted entities	DG CONNECT NIS CG NLOs	Stakeholder satisfaction[13]	Biennial (Survey)	93%	>90%
			Number of contributions to policy development activities (reports, papers, opinions, participation in workshops etc.)	Annual (Internal report)	21	30
1.2 Assist MS to develop, implement and assess National Cybersecurity Strategies	Increase the level of preparedness and cooperation	NLO subgroup on National	Stakeholder satisfaction	Biennial (Survey)	91%	90%

[12] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023
[13] Stakeholder satisfaction conducted every two years to measure the take up of results / outcome, added value, duplication of ENISA work etc by stakeholders

	Prepare capabilities to respond to cybersecurity incidents Increase skill sets Align cybersecurity competencies Improved national cybersecurity strategies	Cybersecurity Strategies				
			Maturity of national cybersecurity strategies, ISACs, SOCs etc	Annual (Report)	N/A	N/A
1.3 Advise the EC and MS on new policy development, as well as carrying out preparatory work	Stakeholders will use ENISA's advice to develop effective and consistent EU cybersecurity policies	DG CONNECT and other DGs or EUIBAs depending on policy file owner.	Stakeholder satisfaction	Biennial (Survey)	93%	>90%
			Number of EU policies supported by ENISA	Annual (Internal report	7	5
			Number of contributions to policy development activities (reports, papers, opinions, participation in workshops etc.)	Annual (Internal report)	21	30
1.4 Monitor and analyse new and emerging policy areas	Stakeholders are informed in a timely manner about gaps, overlaps and inconsistencies across EU policy initiatives under development	NLOs NIS CG DG CONNECT and other DGs or EUIBAs depending on policy file owner	Stakeholder satisfaction	Biennial (Survey)	93%	>90%
1.5 Develop and maintain EU cybersecurity index and State of Cybersecurity in the Union report	Measuring maturity Stakeholders can better prepare for future challenges based on indication of maturity	NISD CG, NLO, CSIRTs Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Uptake of the cybersecurity index	Biennial (survey)	N/A	27 MS representatives 60% satisfaction rate Agreement by all validating bodies
1.6 Foresight on emerging and future cybersecurity challenges and recommendations	Identifying future challenges and opportunities Generate	Foresight AhWG, NLO and AG	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023

	recommendations for stakeholders to take up		Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357[14]	±5% compared to 2023
			The influence of foresight on the development of ENISA work programme	Biennial (ENISA SPD)	N/A	>2 emerging areas identified
			Uptake of reports generated in activity 1	Annual (report)	N/A	±5% compared to 2023

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: DG CNECT, other DGs and Agencies, NIS Cooperation Group and relevant work streams, ENISA National Liaison Officers, Foresight ahWG, CTL ahWG, Index NLO subgroup

Involve / Engage: Operators of essential services and digital service providers under NIS1 and overall entities in scope of NIS2 and industry associations/representatives, National Competent Authorities, other formally established groups

ACTIVITY 1 RESOURCE FORECASTS

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 1.1	INDEX, SITAW, NIS, CERTI	0,95	310.650	0	16.350	0,2	0	1,15	327.000
Output 1.2	TREX, INDEX	2,00	70.000	0,00	0	0,00	0	2,00	70000
Output 1.3	NIS, CERTI	2	8.000	0,25	7.000	0,10	0	2,35	15.000
Output 1.4	NIS, CERTI	0,75	22.500	0,25	22.500	0,00	0	1	45.000
Output 1.5	INDEX	2,5	175.000	0	0	0	0	2,5	175.000
Output 1.6	INDEX	0.75	100.000	0.75	100.000	0	0	1,5	200.000
Total activity resources	Budget: €832.000				FTE: 10,50				

[14] Results includes ENISA threat landscapes which will no longer be managed within this activity, hence baseline in future iterations will be adjusted

Activity 2 Supporting implementation of Union policy and law

OVERVIEW OF ACTIVITY

Activity 2 supports Member States and EU Institutions with the *implementation* of EU cybersecurity policy, and in particular with technical advice on the implementation of the NIS2, as well as the cybersecurity aspects of other legislation, such as DORA. The objectives of this activity are the rapid and harmonized implementation of the NIS2, the increase of maturity of NIS sectors, and the alignment of the implementation of horizontal and sectorial EU cybersecurity policy.

Under this activity ENISA provides support to the NIS Cooperation Group, its workstreams, and the implementation of its 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. Secondly, under this activity ENISA follows up on the 5G toolbox, supports the Union risk evaluations processes (Nevers, Council Cyber risk posture[15]), supports their follows up, delivers a methodology for Union risk evaluations and the building of sectorial risk scenarios, delivers sectorial situational awareness, and runs a yearly NIS360 for assessing maturity and criticality of sectors across the board.

Besides the horizontal outputs, which address sector-agnostic cross-cutting issues, this activity has a sectorial output, which addresses sector-specific issues, with a focus on increasing cybersecurity in the NIS sectors, via targeted service bundles ('sustain', 'build', 'involve', 'prepare'). Currently, we focus our limited resources on low-medium maturity and/or high criticality sectors like telecoms, digital infrastructures (e.g. core internet), energy-electricity, health, and rail. Very limited preparatory work is ongoing in a few sectors, like gas, public administrations and space. This sectorial output also provides relevant sectorial input to other SPD activities, such as cyber exercises (Activity 3), situational awareness (Activity 5), knowledge and information (Activity 1), and awareness raising (Activity 3), allowing these activities to better target sectorial stakeholders.

Besides NIS2 implementation, Activity 2 also provides support to MS and EU institutions on the implementation of DORA, which is 'lex specialis' in the finance sector, with the goal of aligning the NIS2 and DORA implementation. The Agency also supports cybersecurity aspects of policy implementation in the areas of digital identity (eID) and EU Digital Identity Wallets (EUDIW), Network Code on Cybersecurity of cross-border electricity flows, Data Governance Act (DGA) and covers holistically data protection and privacy issues.

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
SO2. Cybersecurity as an integral part of EU policies	Level of maturity of cybersecurity capabilities and resources across the Union at sector level[16]

ACTIVITY 2 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
2.A Effective implementation of the NISD	CSA Article 5 and NIS2	First target: end 2024 and then continuously	Cybersecurity index area "**Policy**" – indicator 2.3 Implementation of cybersecurity related directives	>75% of MS have implemented NIS 2 by end of 2025
2.B Improve maturity of NIS sectors	CSA Article 5 and NIS2	2026	Average maturity of critical sectors Average maturity of less critical sectors – source NIS sector 360.	1 immature NIS1 sector increases maturity score 1 mature NIS1 sector increases maturity score
2.C Improve alignment between NIS2 and sectorial policies	CSA Article 5	2026	Level of alignment between main NIS2 provisions (incident reporting and	75% of respondents say NIS2 and DORA

[15] st09364-en22.pdf (europa.eu)
[16] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e

			security measures) and DORA provisions in survey of JC-DOR and NISCG	are aligned on these topics

ACTIVITY 2 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[17]**
2.1 Support Member States and the EC in the implementation of the NIS CG work program and the NIS directive	Member States will use ENISA advise to implement the NIS Directive.	DG CNECT, NIS CG	Stakeholder satisfaction[18]	Biennial (Survey)	94%	>90%
			EU register for digital entities is used by all MS	Biennial (Survey)	n/a	Used by all MS
			CVD guidance is implemented by MS and all MS are on the CVD map	Biennial (Survey)	n/a	Used by all MS
2.2 Support Member States with union-wide risk evaluations scenarios, union toolboxes and follow up	Support Union-wide risk evaluations and risk scenarios Follow-up of previous union-wide risk assessments (5G, Nevers) Sectorial situational awareness reporting	DG CNECT, NIS CG	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of stakeholders involved in the NIS360	Annual (Internal count)	n/a	120
			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 DGs, sectorial EU agencies	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)	Annual (Internal count)	3	4
			Number and frequency of services delivered to NIS sectors	Annual (Internal count)	21	24

[17] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023
[18] Results / outcome taken up, added value, duplication of existing work etc and effectiveness of ENISA guidance to help MS implement their tasks and deliver the NIS CG work program

			according to the maturity of the sector			

STAKEHOLDERS AND ENGAGEMENT LEVELS
Partners: CNECT, NIS CG, National competent authorities, Sectorial DGs, Sectorial EU agencies, National competent authorities **Involve / Engage:** NLOs, Operators of essential services and digital service providers under NIS1 and overall entities in scope of NIS2 and industry associations/representatives

ACTIVITY 2 RESOURCE FORECASTS

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**		**FTE**	**EUR**
Output 2.1	NIS, SITAW	4,00	183.268	0.25	39.500	0,25	-	4,50	222.768
Output 2.2	NIS, SITAW, TREX	3,75	167.500	0,25		0,25	-	4,25	167.500
Output 2.3	NIS, SITAW, CERTI, TREX	3,00	330.000	0,50		-	-	3,50	330.000
Total activity resources		Budget: €720.268				FTE: 12.25			

Activity 3 Capacity Building

OVERVIEW OF ACTIVITY

This activity seeks to improve and develop the capabilities of Member States, Union Institutions, bodies, and agencies, as well as various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the Union. This is achieved through the development of frameworks (Risk management, strategies, etc.) that are based on lessons learnt from MSs through the implementation and development of their National Cyber Security Strategies. In parellel, the activity seeks to raise the overall awareness of cybersecurity risks and practices. in cooperation with Member States, Union institutions, bodies, offices and agencies and EU's international partners, it aims to build an empowered European community, with an allied global community which can counter risks in line with the values of the Union. Under this activity the Agency will be organising regular outreach campaigns, providing guidance on best practices and support coordination across MS on awareness and education. Moreover, the Agency will facilitate the exchange of best practices and information on cybersecurity in education between MS.

Actions to support this activity includes the organisation of large scale exercises, sectorial exercises, Capture the Flag (CTF) competitions, trainings and Attack Defence (AD) competitions., in addition the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem including cross-border, and assist in reviewing and developing national and Union level cybersecurity strategies.

The Agency will run awareness campaigns and best practices promotion activities with the aim to enhance behavioural change with regards to cyber hygiene and cyber capacity. At the same time will promote the adoption of the Cybersecurity Skills Framework by public and private actors. In addition, the tasks stemming from the EC Communication on the Cybersecurity Skills Academy are undertaken within this Activity focusing mostly on preparing the development of indicators and KPIs to measure the progress towards closing the cyber talent gap and collect associated data. The Agency will collaborate with all relevant actors while undertaking these tasks. Moreover, the Agency will facilitate the exchange of best practices and information on cybersecurity in education between MS. 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 service package TREX.
The legal basis for this activity is Articles 6, 7(5), 10 of the CSA.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO4: Cutting-edge competences and capabilities in cybersecurity across the Union SO1. Empowered and engaged communities across the ecosystem	1. Aggregated assessment of the level of cybersecurity capabilities in the public and private sectors across the Union[19]. 2. Aggregated assessment of the level of maturity of national cybersecurity capabilities and resources 3. The gap between demand and supply of cybersecurity skilled professionals 4. General level of cybersecurity awareness and cyber hygiene among citizens and entities

ACTIVITY 3 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
3.A Increase the supply of skilled professionals to meet market demand	Article 10 and 6 EU priority on skills shortage EC Communication on Cybersecurity Skills Academy	2025	Increase in cybersecurity indicator "cybersecurity graduates in higher education" Number of professionals trained under cybersecurity skills academy Number of higher education institutions providing	"cybersecurity graduates in higher education" At least 200 000 professionals trained by 2025 TBD

[19] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)b

			education/courses in cybersecurity	
3.B Prepare and test capabilities to respond to cybersecurity incidents	Art.6 CSA	2025	Proportion of beneficiaries who take part in relevant ENISA exercises and trainings Added-value of ENISA exercises and trainings	All MS participate in Cyber Europe 2026 >80% of EU Agencies have participated in JASPER exercises over 3 years 90% participants see positive added value
3.C Increase skill sets and align cybersecurity competencies	Art.6 CSA	2025	Assessment of average level of cybersecurity technical competences of participants in European cybersecurity challenge finals Number of participants that take part in national competitions improving cybersecurity skills and capabilities Level of alignment of cybersecurity competences across the Union	A relevant metric is in the process of being developed in the ENISA security index. More than 10.000 participants take part in the annual CTF competitions that are organised prior to the ECSC final MS national competence frameworks are aligned with European Cybersecurity Skills framework
3.D Increase awareness of cybersecurity risks and improve cyber-secure behaviour	Article 10	2025	Cybersecurity indicator “SME awareness training ” Number of cybersecurity incidents with human error as root course Cybersecurity index indicators “National culture of cybersecurity”	1% - 2% increase of Cybersecurity indicator “SME awareness training ” increases year by year Number of cybersecurity incidents in critical sectors with human error as root course

				decreases year by year in relative percentages 1% - 2% increase of Cybersecurity index "National culture of cybersecurity"

ACTIVITY 3 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[20]**
3.1 Support the implementation and uptake of EU cybersecurity skills framework	Promoting cybersecurity skills courses Greater number of participants in cybersecurity courses	AHWG on Cybersecurity Skills, ECCC WG on Skills	Stakeholder satisfaction	Biennial (survey)		1% increase (from previous year – decrease in duplication)
			Number of cybersecurity programmes (courses) and participation rates	Annual (cyberhead platform)		1-2% increase
			Total number of students enrolled in the first year of the academic programmes		5 205	1-2% increase
			Student gender distribution (% female: % male)		19% female 81% male	
			Total number of cybersecurity programmes		122	>2 programmes
			Number of postgraduate programmes		5%	
			Number of master's degree programmes		80%	
			Number of bachelor's degree programmes		15%	
			Number of entities included in ECSF registry (i.e. # of MS adopted ECSF, #of ECSF implementations/pledges), # of users of the EC Cybersecurity	Annual (register of activities)	N/A	30% of MS to adopt ECSF, At least 15 orgisations to have endorsed ECSF

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

			Skills Academy pledgers)			
3.2 Organise large scale biennial exercises and sectorial exercises	Increase the level of preparedness and cooperation Prepare and test capabilities to respond to cybersecurity incidents Stakeholder test and improve capabilities and increase capacity	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)	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Evaluation of capacity building actions by participants in exercises and trainings	Annual (Report)	40% high usefulness 53.5% medium usefulness 6.5% low usefulness	>50% high usefulness
			Number of participants in trainings and organized by ENISA	Annual (Report)		>500 (incl online exercises)
3.3 Organise trainings and other activities to support and develop maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS cooperation group (NIS CG), EU-CyCLONe and work streams, information sharing and analysis centers (ISACs) and other communities	Increase the level of preparedness Prepare capabilities to respond to cybersecurity incidents Increase skill sets Stakeholders improve capabilities and skill set	NLO Network (as necessary) 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)	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Number of participants in trainings and challenges organized by ENISA	Annual (Report)	N/A	>1.000 (incl online trainings)
3.4 Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)	Align cybersecurity competencies Increase skill sets	ECSC Steering Committee (NLO Subgroup)	Stakeholder satisfaction	Biennial (Survey)	91%	90%
3.5 Develop activities to enhance behavioural change by essential entities[21]	Targeted awareness campaigns to improve behaviour Take up of best practices by stakeholders	Awareness Raising AHWG, NISD WS	Stakeholder satisfaction	Biennial (survey)	91 %	>1% increase (from previous year – decrease in duplication)
			Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics	Annual (report)		>5% increase

[21] Defined by NIS 2

			Total social media impressions		27 278 491	
			Total social media engagement		19 301	
			Total video views		6 602 355	
			Total website visits		300 530	
			Total participation at events		40	
			Number of download of materials and overall utilisation of AR tools (i.e. AR-in-a-Box and SME tool)	Annual (ENISA website)	N/A	>4000 per semester
3.6 Implement the Cybersecurity in Education roadmap22	Influence education to include cybersecurity Greater awareness and interest in cybersecurity as a career path	AR AHWG	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)
				# of cybersecurity activities addressing secondary and primary level of education	N/A	TBD

STAKEHOLDERS AND ENGAGEMENT LEVELS

Involve / Engage: Cybersecurity professionals, Private industry sectors (operators of essential services such as health, transport etc. or generally entities in scope of NIS2), EU Institutions and bodies, CSIRTs Network and related operational communities, European ISACs, EU-CyCLONe members, NISD Cooperation Group, Blueprint stakeholders, SOCs, including National and Cross-border SOCs. : ECSM Coordination Group, National Competent Authorities through the NIS Cooperation Group Work Streams, AHWG on Awareness Raising and Education, AHWG on Skills, EEAS, DG NEAR, DG CONNECT

ACTIVITY 3 RESOURCE FORECASTS

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 3.1	INDEX, TREX, NIS	1,5	70.000	1	30.000	0	0	2,50	100.000
Output 3.2[23]	TREX, NIS	3,35	500.000	0,00	0	0,00	0	3,35	500.000
Output 3.3	TREX	4,30	546.591	0,00	0	0,00	0	4,30	546.591

[22] Roadmap developed by ENISA during the course of 2022

Output 3.4	TREX	2.3	120.000	0,00	0	0,50	0	2,8	120.000
Output 3.5	NIS	1,75	50.000	0,6	50.000	0	0	2,35	100.000
Output 3.6	INDEX	0,5	60.000	0,5	30.000	0	0	1	90.000
Total activity resources	Budget: €1.456.591				FTE: 16.3[24]				
Other supplementary contribution	~€120.000 from Service Level Agreement with EU-LISA to provide support on exercises								

[24] Does not include 1.5 FTEs unallocated from previous output 9.2 from SPD24-26

Activity 4 Enabling operational cooperation

OVERVIEW OF ACTIVITY

The 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. ENISA, as mandated by the NIS2, provides the organizational support and tools for both the technical(EU CSIRTs Network) and operational layer (EU CyCLONe - Cyber Crises Liaison Organisation Network) of Union operational cooperation networks.

Under this activity ENISA is supporting operational communities through helping to develop and maintain secure and highly available networks / IT platforms and communication channels in particular ensuring maintenance, deployment and uptake of the MeliCERTes platform[25] and the EU Vulnerability Database. As such, this activity could also frame prepare some of ENISA's proposed tasks in coordinating information and notification about vulnerabilities at the Union level as outlined in the Commission's legislative initiative on CRA. In parellel the activity maintains IT systems and platofrms for all operational activities.

In addition, actions include facilitating synergies with and between the different national cybersecurity communities (including the civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors - notably CERT-EU, EC3, EEAS - with the view to exchange know how, best practices, provide advice and issue guidance.

This activity also manages the ENISA Cyber Partnership Programme and the use of 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[26].

This activity contributes to the Situational Awareness, INDEX and NIS service packages. Finally, this activity will also seek to contribute to the Unions efforts to cooperate with third countries and international organisations on cybersecurity.

The legal basis for this activity is Article 7,12 & 42 of the CSA and Articles 12, 15 and 16 of NIS2.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO3: Effective cooperation amongst operational actors within the Union in case of massive cyber incidents	Level of cooperation and availability, (disruptions) and utilisation and trust of Union level networks, tools and databases.

ACTIVITY 4 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
4.A. Enable trust and effective cooperation and operations of CSIRTs Network and EU-CyCLONe members.	Article 7 & NIS2	2025	Satisfaction with scalable ENISA support Maturity of operational communities	80% of satisfaction of stakeholders Average overall level of maturity increases year by year
4.B. Ensure a high level of coordination of the Vulnerability Disclosure Services within the Union.	Article 7 & NIS2	2026	EU vulnerability database usage and added-value	EU Vulnerability Disclosure Services are

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

				gradually available (Numbering Services in place) and aligned with national mechanisms . EU vulnerability database functional and aligned with national mechanisms
4.C. Robust and secure tools/ platforms are established, and actively utilised to facilitate seamless operational collaboration at the Union level.	Article 7 & NIS2	2025	Continuous operations and use of secure communication tools and platforms for EU-CyCLONE and CNW including the use of regular checks and controls.	No significant disruption or incidents in the working of operational tools and platforms recorded against standard checks and controls Beneficiaries use the tools
4.D Information exchange to augment Union common situational awareness through cooperation with private sector and non-EU entities	Article 7	2026	Cyber Partnership programme is established Information coming from private sector partners and non-EU entities are part of operational cycle of situational awareness production	90 % of selected entities are enrolled into the ENISA Cyber Partnership programme 90% of the participating entities are actively contributing by exchanging information
4.E Foster EU cybersecurity values and priorities	Article 42 of the CSA	2025	Ability to support the Union external objectives Coherence of ENISA International Engagement with the Agency's strategy	ENISA is seen as key contributor to foster EU cybersecurity values and priorities where engaged ENISA activities are judged aligned with its

				International Strategy

ACTIVITY 4 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[27]**
4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs Network and EU-CyCLONe members.	Enhanced Information Sharing and cooperation among the CSIRTs Network and EU-CyCLONe members.	CSIRTs Network and EU-CyCLONe members.	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	
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	Establishment and operationalisation of the Cyber Partnership Programme ENISA Situational Awareness leverage private sector partnership to augment context and understanding of threats, vulnerabilities and incidents	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)	N/A 6	10/4
			Percentage of RFI answered by members of partnership program	Annual (report)	N/A	80%
4.3 Implement the ENISA international strategy and outreach	EU values recognised by international stakeholders International cooperation support ENISA objectives	MT, EEAS, COM and (MB as required)	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)
			Staff satisfaction with international coordination	Annual (survey)	N/A	>80%
4.4 Support coordinated vulnerability disclosure and maintain the EU Vulnerability Database	ENISA provides numbering services for Common Vulnerabilities and Exposures with a view to	CSIRTs Network and NIS Cooperation Group.	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			Continuous use and durability of platforms	Annual (report)		

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

	gradually establishing EU Vulnerability Database.		(including prior to and during large-scale cyber incidents)			
4.5.Develop and maintain IT systems and platforms for operational activities.	Usage of the available tools	CSIRTs Network and CyCLONe members.	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			Number of users, both new and recurring, and usage per platform/tool/ SOP provided by ENISA	Annual (report)		>5% increase
			CSIRTs active users % increase year on year		19%	
			CSIRTs number of exchanges/i nteractions % increase year on year		104%	
			EU-CyCLONe active users % increase year on year		2%	
			EU-CyCLONe number of exchanges/i nteractions % increase year on year		548%	

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

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

ACTIVITY 4 RESOURCE FORECASTS									
OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 4.1	NIS, SITAW	3,1	279.000	0,2	15.500	0,2	15.500	3,5	310.000
Output 4.2	SITAW	1,25	37.000	0	0	0	0	1,25	37.000
Output 4.3	SITAW, TREX	1	-	0,75	20.000	0	0	1,75	20.000
Output 4.4	NIS, SITAW	3,5	266.474	0	0	0	0	3,5	266.474
Output 4.5	SITAW, NIS	3,5	974.676	0	278.988	0	0	3,5	1.253.664
Total activity resources	Budget: 1.887.138				FTE: 13,5				

Additional required resources for 2025

Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 4.4	NIS, SITAW		43.526						43.526
Output 4.5	SITAW, NIS		321.336						321.336
Remarks	By the end of 2024, first parts of the EU vulnerability disclosure database will be operational. This is a new system/service for the operational tools that need extra budgeting for the proper deployment and operations of two environments (pre-production and production). In particular, extra budget is needed for its further design, installation, deployment, testing, support and maintenance of the two environments with proper security levels. Activity 4 will be hosting the Operational IT. The transition of the majority of these services to the cloud necessitates a dedicated budget to facilitate smooth migration.								

Activity 5 Provide effective operational cooperation and situational awareness

OVERVIEW OF ACTIVITY

The activity contributes to developing cooperative preparedness and response at Union and Member States level to large-scale cross-border incidents or crises related to cybersecurity through maintaining and contributing to the Union common situational awareness. ENISA is delivering this activity by collecting and analysing information based on its own capabilities, aggregating and analysing reports, ensuring information flow between the CSIRTs Network, EU-CyCLONe, the Inter-Institutional Cyber Crisis Task Force and other technical, operational and political decision makers at Union level and including cooperation with other EUIBAs services such as CERT-EU, EC3, EEAS including EU INTCEN, DG CONNECT Cyber Coordination Taskforce Unit. This activity also manages the ENISA Cyber Partnership Programme and the use of information exchange with security vendors and non-EU cybersecurity entities.

The activity includes the development of regular in-depth EU Cybersecurity Technical Situation Report in accordance with CSA art7(6), also known as Joint Cyber Assessment Report (EU-JCAR), regular weekly OSINT reports, Joint Rapid Report together with CERT-EU and other ad-hoc reports as needed.

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, facilitating technical handling of incidents, supporting cross-border information sharing and analyzing vulnerabilities, including through the EU Vulnerability Database (under development in Output 4.2).

This activity implements the structured cooperation with CERT-EU (please see Annex XIII Annual Cooperation Plan 2025) including general oversight over the cooperation, provides primary point of contact for the Cyber Crisis Task Force, and implement the agreements between ENISA and DG CONNECT for the contribution to the Commission Situation Center.

Under this activity the Agency will map **threat landscapes** and provide 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.

Finally under this activity a new task to fullfil Article 11 of the proposed CRA will be undertaken.

In doing so, the Agency will take into account **incident reports** submitted to it under Article 23 of NIS2 and other relevant EU legislation.

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

The activity leads the service package on situational awareness (SITAW) and contributes to the INDEX and NIS service packages.

The legal basis for this activity is Article 5 (6) 7 & 9 of the CSA and Article 23(9) of the NIS2.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO3: Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents SO6. Foresight on emerging and future cybersecurity challenges SO7. Efficient and effective cybersecurity information and knowledge management for Europe	Risk level due to cyber threats is understood by the cybersecurity communities at Union level and decision makers are able to prioritize actions to manage the risk Union level cybersecurity risk assessment and cyber threat landscape [adopted in accordance of Article 18(1)a]

ACTIVITY 5 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
5.A Threat and information are disseminated in a timely and accurate manner and/or available on-demand	Article 7	2025	Recipients are timely and accurately informed about the latest threat, vulnerabilities and incidents Usefulness of situational reports	At least 80% of recipients found the information being communicated in timely and accurately based on the level of confidence of the information. At least 80% of recipients found the reports useful
5.B Improved common situational awareness through joint assessment, threat and risk analysis	Article 7	2025	Stakeholders ability to make informed decisions based on	100% quarterly JCAR reports have been issued on time

			joint situational reports Usefulness and timeliness of joint situational reports	At least 80% of recipients find the reports useful
5.C Information exchange to augment Union common situational awareness through cooperation with private sector and non-EU entities	Article 7	2026	Cyber Partnership programme is established Information coming from private sector partners and non-EU entities are part of operational cycle of situational awareness production	90 % of selected entities are enrolled into the ENISA Cyber Partnership programme 90% of the participating entities are actively contributing by exchanging information

ACTIVITY 5 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[28]**
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[29]	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, , EUIBAs, National Authorities within MSs subscribed to the products	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Timeliness and Accuracy of reports	Annual (survey)	N/A	
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[30]	CSIRT Network, EU CyCLONe, EUIBAs, HWPCI, Management Board	Stakeholder satisfaction	Biennial (survey)	84%	>90%

[28] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023
[29] Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1
[30] 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 and relevant EUIBAs	Annual (report)	N/A	
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 recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357[31]	±5% compared to 2023
			Uptake of reports generated in activity 5	Annual (report)	N/A	±5% compared to 2023
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
			EU incident reporting maturity	Annual (report)	N/A	EU Average >50%
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)		±5% compared to 2023

[31] Results includes ENISA threat landscapes which will no longer be managed within this activity, hence baseline in future iterations will be adjusted

5.5 Assist in developing the EU vulnerability notification under CRA	TBD	TBD	TBD			TBD

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) ECATS, Foresight ahWG, CTL ahWG

Involve / Engage: Other type of CSIRTs and PSIRTs

ACTIVITY 5 RESOURCE FORECASTS

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 5.1	INDEX, SITAW, NIS	4	839.311 + 450.000	0	0	0	0	4	839.391 + 450.000
Output 5.2	INDEX, SITAW, NIS	4		0	0	0	0	4	
Output 5.3	INDEX, SITAW, NIS	2	190.000	0	0	0	0	2	190.000
Output 5.4	INDEX, SITAW, NIS	1,5	152.000		0	0	0	1,5	150.000
Total activity resources	*Budget: 1.179.391*					*FTE: 11,5*			
Other supplementary contribution	**Budget: 450.000 (outputs 5.1 and 5.2)** [32] (+2 FTEs from Contribution Agreement)								

Additional required resources for 2025

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 5.1	INDEX, SITAW, NIS		91.068						91.068
Output 5.5 NEW	INDEX, SITAW, NIS	3	1.000.000					3	1.000.000
Remarks	Additional requested resources needed for new tasks expected under the CRA for vulnerability notification and CSOA								

[32] allocation of 450.000 and 2 FTEs CA from Contribution Agreement related to Cybersecurity Support Action, refer to annex XI for further information and activity 6

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 pentest, threathunting, risk monitoring and assessment, customized exercise, 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 5a.

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 intended for 2025 through 2026[33]

The legal basis for this activity is Article 6 and 7 of the CSA. The activity contributes to the SITAW, NIS, INDEX, TREX service packages.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO3: Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents	Level of preparedness and response to large-scale cross-border incidents

ACTIVITY 6 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
6.A Enhanced preparedness and effective incident response	Article 7	2025	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	>4[34]

ACTIVITY 6 OUTPUTS

DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	TARGET 2025[35]
6.1 Provide pentest and threat hunting services towards selected entities within EU Member States[36]	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[37]	Customize Exercise and Training	MSs, CNECT, Beneficiaries	% of MSs requesting the service		N/A	50%

[33] Information on FTE calculation and Budget amount are estimates based on DEP 2024 and are final determination of the Contribution Agreement between Commission (DG CONNECT) and ENISA
[34] Target response to qualitative survey regarding ENISAs ability to support MS with a scale of 1 to 5, with 5 being the highest rating
[35] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023
[36] Beneficiaries of the Act5B services are specified in the [Contribution Agreement]
[37] Beneficiaries of the Act5B services are specified in the [Contribution Agreement]

	services are delivered timely and accurately to MSs.		Satisfaction score			>4
6.3 Support risk monitoring and assessment for selected entities within EU Member States[38]	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[39]	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

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)[40]		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 6.1	SITAW, NIS, INDEX, TREX	3.5[41] (+8 FTEs from Contribution Agreement)	14,55m[42]						14,55m
Output 6.2	SITAW, NIS, INDEX, TREX								
Output 6.3	SITAW, NIS, INDEX, TREX								
Output 6.4	SITAW, NIS, INDEX, TREX								

[38] Beneficiaries of the Act5B services are specific in the [Contribution Agreement]
[39] Beneficiaries of the activity 6 services are specific in the [Contribution Agreement]
[40] Cyber Support Action Programme
[41] This activity is resources through the use of 10 Contract Agents to be absorbed as direct cost of the programme and financed through Commission contribution agreement. The actual resources count will be available once the Contribution Agreement between Commission (DG CONNECT) and ENISA is in place. The FTE represent the contribution of ENISA based on the current establishment plan.
[42] This is based on the Digital Europe Programme 2024 earmarked 15m euros based on information available as of dec 2023. In addition 450.000 allocated to activity 5

Total activity resources (supplementary contribution)	Budget: 14.550.000[43]	FTE: 3.5[44] (+8 FTEs from Contribution Agreement)

Additional required resources for 2025

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Outputs 6.1 to 6.4	SITAW, NIS, INDEX, TREX	2	0	0	0	0	0	2	0
Remarks	Additional FTEs required as its foreseen that this area of work will be intensified and scaled up - also in view of the upcoming Cyber Solidarity Act								

[43] Minus 450.000 and 2 FTEs CA allocated to activity 5, please refer to annex XI for further details regarding contribution agreement
[44] Currently 3.5 FTEs have been allocated from ENISA resources however additional 2 FTEs required due to expected scaling up and intensity of actions

Activity 7 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

This activity encompasses actions that seek to establish and support the EU cybersecurity certification framework by preparing and reviewing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the Union Rolling Work Program. Actions also include maintaining and evaluating adopted cybersecurity certification schemes and participating in peer reviews. In addition, in this activity, ENISA assists the Commission with regard to the European Cybersecurity Certification Group (ECCG), co-chairing and providing secretariat to the Stakeholder Cybersecurity Certification Group (SCCG); 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 aspects of certification along the lines of legislation adopted notably, NIS2, DGA as well as legal instruments in the legislative process that include CRA, EUDI Wallet, AI Act, Chips Act, Data Act, amendment of CSA regarding managed security services certification etc.

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
SO5 High level of trust in secure digital solutions	Citizens trust in ICT certified and non-certified solutions in the EU market

ACTIVITY 7 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
7.A Improve the certification requirements concerning security posture management of certified products, services, processes and gradually of managed security services	Article 8 and Title III	2025	Monitor the take up of technical standards and technical specifications and use lessons learned to support EU policy and legislation (document monitoring)	Applicable standards cybersecurity requirements have been considered by ENISA to promulgate better cybersecurity certification schemes
7.B Efficient and effective implementation of the European cybersecurity certification framework	Article 8 and Title III	2025	Number of stakeholders (public and private) in the internal market, implementing the cybersecurity certification framework for their digital solutions	60% of European cybersecurity certification frameword is timely implemented across all relevant stakeholders
7.C Increase use and uptake of European cybersecurity certification	Article 8 and Title III	2025	Number of schemes and additional requests addressed to ENISA by the Commission Number of schemes and additional requests processed by ENISA	All validated requests are processed by ENISA

			Uptake of certified digital solutions (products, services, processes and gradually managed security services) using certification schemes under the CSA framework as well as other directly applicable instruments i.e. CRA, EUDIW etc.	High number[45] of private and public entities and/or market sectors relevant to a given scheme taking up certification after the entry into force of the implementing act
6.D Increase trust in ICT products, services and processes	Article 8 and Title III	2025	Number of certificates issued and published under an EU certification scheme; high utilisation rate in the market.	Proportionate[46] number of certificates issued migrating to a new scheme

ACTIVITY 7 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[47]**
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 cooperation with the Commission Statutory Bodies and ad hocWorking Groups actively involved	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 preparation of certification schemes	Annual (report)	N/A	At least 20 ad hoc Working Group Member from third-party 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	ECCG European Commission	Stakeholder satisfaction	Biennial	82%	75%
			ENISA response to consolidated monitoring	Triennial (survey)	N/A	75%

[45] Number cannot be quantified as yet but will be monitored and the target adjusted after the transition period
[46] ENISA monitors the certificates issued under SOG-IS and transition to EU CC will have to be proportional to the number of certificates issued.
[47] Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023

	Take up of schemes by stakeholders		and maintenance requirements of schemes adopted			
			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

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 7.1	CERTI, NIS	4,65	416732	0,7	0	0,5	0	5,85	416.732
Output 7.2	CERTI	1,9	53 000	0	0	0	0	1,9	53.000
Output 7.3	CERTI	0,5	0	0	0	0	0	0,5	-
Output 7.4	CERTI	1,1	118896	0,15	0	0	0	1,25	118.896
Total activity resources	*Budget:* 588.628					*FTE:* 9,2			

Additional required resources for 2025

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 7.1	CERTI, NIS	0	83.268	0	0	0	0	0	83.268
Output 7.2	CERTI	0	47.000	0	0	0	0	0	47.000
Output 7.4	CERTI	0	81.104	0	0	0	0	0	81.104
Remarks	Additional budgetary requirement concerns likely requests for certification schemes in response to the adoption of legislative instruments concerning management security services (MSS), artificial intelligence (AI) and the EU Digital Identity Wallet (EUDIW). It follows that new requests for schemes once issued by the Commission to ENISA, and after they are accepted by the latter will require new financial resources over the application period.								

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. As such, this activity also seeks to lay the ground for a robust role of ENISA in the CRA notably in terms of market analysis, preparation of market sweeps and reporting of exploited vulnerabilities etc. Actions to support this activity include producing analyses and guidelines as well as good practices on cybersecurity requirements, 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. Platforms for collaboration among the cybersecurity market players, improve visibility 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.

To prepare this strategic advice, ENISA will take full account of past and ongoing research, development and technology assessment activities, and scan the horizon for emerging and future technological, societal and economic trends that may have an impact on cybersecurity.

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.

In addition this activity supports cybersecurity certification by monitoring standardisations being used by European cybersecurity of certification schemes and recommending appropriate technical specifications where such standards are not available.

The legal basis for this activity is Article 8 and 11 and Title III of the CSA.

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO5 High level of trust in secure digital solutions SO6. Foresight on emerging and future cybersecurity challenges	1. Monitor metrics such as number of certificates issued under an EU scheme; number of companies interested in EU certification; growth observed in the number of CABs / or EU certification functions thereof recorded in the MS. 2. Overall EU investment in R&I activities addressing emerging cybersecurity challenges

ACTIVITY 8 OBJECTIVES

DESCRIPTION	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
8.A Foster a robust European cybersecurity industry and market	CSA Article 8 CRA regulation	2025	Stakeholders' satisfaction with of the ENISA survey State of the EU cybersecurity industry and market for products and services (index) Industry perception of the internal market (survey)	Improved ability of ENISA and the EU to analyse the EU cybersecurity market
8.B Improve the conditions for the functioning of the internal market	CSA Article 8 and Title III CRA regulation	2025	Better informed choices by users of products in market niches analysed	Improve the understanding of stakeholders on the cybersecurity market conditions in the EU

8.C EU R&I funding programmes address emerging cybersecurity challenges identified by ENISA.	Art.11, EU Research Agenda	2025	Assessment of ENISA contribution to EU R&I funding programmes work programmes	50%[48]
8.D EU R&I funding programmes focus in the development of solutions made in the EU.	Art.11, EU Research Agenda	2025	Assessment of EU funded projects transitioning from research into deployment of new cybersecurity solutions	10
8.E EU cybersecurity R&I community generates knowledge on emerging cybersecurity challenges identified by ENISA.	Art.11	2025	Number of research articles and papers generated by the community reviewing emerging cybersecurity challenges identified by ENISA	10

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 in order to identify gaps, trends, opportunities and threats	Identifying current and emerging R&I needs and funding priorities	Academia, Industry and National R&I Entities (including NCCs) and EUIBAs	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Evaluation of the trends, wild cards and week signals on emerging cybersecurity challenges leading to R&I needs and priorities	Annual (annual work programme)	N/A	3
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)	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Cybersecurity market analysis; cybersecurity product and services analysis; analysis on vulnerabilities and dependencies in ICT products and services as appropriate;	Annual (report)	N/A	All reports produced as planned (Y out of Y reports)

[48] Percentage of funding programmes that address cybersecurity challenges proposed by ENISA

			analysis if other relevant market areas			
8.3 Support activities of market surveillance authorities and identification of categories of products for simultaneous coordinated control actions.	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	NLO / NCCA Commission	Collection of requirements Matching requirements with deliverables Time to carry out market sweeps	Catalogue, survey and categories of products in 2025-26 Market sweeps as from 2027 (3-years transition) or earlier if requested	N/A	Stakeholder satisfaction above 70%
8.4 Upon request, conduct evaluations of products that present a significant cybersecurity risk	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	ECCG SCCG (as appropriate) Commission	Metholdology for evaluations Profiles of experts	Method to evaluate products Guidance and criteria to accept evaluation results	N/A	Stakeholder satisfaction above 60%
8.5 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)
8.6 Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment.	Advising EU Funding programmes including the ECCC and it's Strategic Agenda and Action Plan.	EC including CNECT and JRC, ECCC and NCCs	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Number of contributions to EU funding programmes	Annual (reports)	N/A	5

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. 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									
OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 8.1	NIS	1,25	22.000	1,7	88.000	0	0	1,75	110.000
Output 8.2	CERTI, INDEX, CERTI	4,15	147487	0,1	0	0	0	4,25	147.487
Output 8.5	CERTI, NIS	2,75	136.666		0	0	0	2,75	136.666
Output 8.6				2	10.000	0	0	2	10.000
Total activity resources	*Budget: 404.154*				*FTE: 10,75*				

Additional required resources for 2025

OUTPUTS	SERVICE PACKAGE RELATED TO CATEGORY A	A (RESERVED FOR TASKS TO MAINTAIN STATUTORY SERVICE)		B (RESERVED FOR OTHER REGULAR STATUTORY TASKS)		C (RESERVED FOR AD HOC STATUTORY TASKS)		TOTAL	
		FTE	EUR	FTE	EUR	FTE		FTE	EUR
Output 8.3 NEW	CERTI	0,75	100 000	0	0	0	0	0,75	100.000
Output 8.4 NEW	CERTI	0	0	0	0	0,25	75000	0,25	75.000
Remarks	Additional resources for activity 8 are expected to be used towards the gradual response of ENISA to its new tasks under the CRA. While some of the CRA tasks will be extensions of current ones, particularly in regard to analysis and reporting, other will have to be developed from scratch; for instance, the role and practice of ENISA in terms of market sweeps fits this description								

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 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 of the Agency's expertise (e.g. cybersecurity risk management).

Under this activity ENISA will seek to achieve 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 ensures that the Agency adheres to sound financial management. In the area of IT systems and services, the IT management committee oversees and monitors the comprehensive application of the Agency's IT strategy and relevant 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 Maintain corporate performance and coordinate 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	EU Eco-Management and Audit Scheme (EMAS) established	Annual	N/A	Adopted by end 2024
	Develop efficient framework for ENISA continuous governance to safeguard high level of IT	Agency IT strategy aligned with corporate strategy Proportion of total IT budget allocated to	Annual	N/A N/A	Revised IT strategy by 2024 20% by 2024

		information security proportional to the level of risks across various IT systems within Agency			

ACTIVITY 9 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[49]**
9.1 Coordinate the implementation of the Agency's performance management framework, including Agency wide budget management and IT management processes, environmental management and regulatory compliance	Unified day to day practices across the agency upon implementing SPD Annual risk assessment and internal controls assessment performed and reported Legal and regulatory compliance are monitored; issues and areas of improvement identified Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy; reports from ITMC Streamlined budget management across the Agency; reports from BMC A plan to reduce CO2 emissions at ENISA's HQ	MT & relevant committees External and internal audits Statutory bodies	Efficiency and effectiveness of project management procedures and tools (survey)	Annual	N/A	>80%
			Number of high risks identified in annual risk assessment		3	<= 3
			Percentage of identified internal controls deficiencies addressed within timelines		N/A	100% for critical, 80% for major, 60% for moderate
			Number of complaints filed against ENISA/number of identified legal or regulatory breaches		3	<=3
			% of revised and up to date corporate rules (MBD, EDD, policies, processes)		N/A	60% corporate rules which have not been reviewed less than 3 years ago; 80% corporate rules which have not been reviewed less than 4 years ago
			MoU with Hellenic authorities for CO2 reduction		N/A	MoU process initiated by end 2024

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

			in ENISA HQ in place			
			Efficiency and effectiveness of ITMC/BMC processes (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 EUIBAs 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%
			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	Cybersecurity advisory in implementation of the new Regulation on a high common level of cybersecurity within EUIBAs 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 EUIBAs and European Commission, Staff Committee, Management Team						

ACTIVITY 9 RESOURCE FORECASTS							
Outputs	SERVICE PACKAGE SUPPORTED	CORE		ESSENTIAL		ON-DEMAND	
		FTE	EUR	FTE	EUR	FTE	EUR
Output 9.1	All service packages	4,2	150.192	0		0	0
Output 9.2	All service packages	2,5	184.882	0	20% IT investment – cybersecurity	0	0
Output 9.3		0,6	0	0		0	0
Output 9.4	All service packages	4,2	0	0	153.125	0	0
Total activity resources	*Budget: 488.199*			*FTE: 11,5*			
Other supplementary contribution	Budget: 54.604 SLA with ECCC, see annex XI for additional information			FTE: 0			

Additional required resources for 2025

Outputs	***Supporting service packages***	CORE		ESSENTIAL		ON-DEMAND		Outputs	
		FTE	EUR	FTE	EUR		FTE	EUR	FTE
Output 9.2	All service packages		55.926	0	0	0	0	0	0
Output 9.4	All service packages		50.000	0	0	0	0	0	0
Remarks	Additional budget requirements to further support compliance with Cybersecurity Regulation for EUIBAs and intramuros assistants								

Activity 10: Reputation and Trust

OVERVIEW OF ACTIVITY

The activity seeks to achieve 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.

Under 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 and reputation	Ensure efficient corporate services	Level of trust in ENISA (as per Biannual Stakeholder Survey)	Biennial	95%	95%
10.b Supports the activities implementing the core mandate by improving knowledge sharing	Ensure efficient corporate services	High satisfaction with essential communication and assistants services High satisfaction with demand driven communication and assistants services	Annual (MT survey Annual (MT survey)	N/A N/A	60 % 60%
	Developing service propositions with additional external resourcing	Limited disruption of continuity of internal and external communications	Annual (Business Continuity Plan)	N/A	Target set in business continuity plan and agreed response time objectives (RTO)

ACTIVITY 10 OUTPUTS

DESCRIPTION	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	LATEST RESULTS	TARGET 2025[50]

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

10.1 Implement the multiannual communications and stakeholders' strategies including corporate outreach	Increase transparency and outreach Engaged communities Increased impact of ENISA activities Relevant and easily accessible information is provided to stakeholders Implement EUAN leadership communications and EUAN yearly meeting	Management Team and agency stakeholders	Number & types of activities at each engagement level (stakeholder strategy implementation)	Annual (Internal report)	N/A	
			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 the quality and timing of ENISA internal communications	Annual (survey)	36%	>50%
10.3 Manage and provide the secretariat for the statutory bodies	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 received per NLO consultation	Annual (Internal report)	N/A	>2
			Number of feedback received per AG consultation	Annual (Internal report)	N/A	>2
			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 EUIBAs and European Commission, Staff Committee, Press

Involve / Engage: All ENISA stakeholders

ACTIVITY 10 RESOURCE FORECASTS							
Outputs	SERVICE PACKAGE SUPPORTED	CORE		ESSENTIAL		ON-DEMAND	
		FTE	EUR	FTE	EUR	FTE	FTE
Output 10.1	All service packages	2,5	440657	0	0	0	0
Output 10.2	All service packages	1		0	0	0	5000
Output 10.3	All service packages	2	50.000	0		0	0
Total activity resources	*Budget: 495.657*			*FTE: 5,50*			

Additional required resources for 2025

Outputs	SERVICE PACKAGE SUPPORTED	CORE		ESSENTIAL		ON-DEMAND		Outputs	
		FTE	EUR	FTE	EUR		FTE	EUR	FTE
Output 10.1	All service packages		250.052	0	0	0	0	0	0
Output 10.3	All service packages		50.000	0	0	0	0	0	0
Remarks	Additional resources required to further enhance corporate outreach via ENISA website and portals, and additional statutory bodies meetings								

Activity 11 Effective and efficient corporate services

OVERVIEW OF ACTIVITY

This activity seeks to support ENISA aspirations as stipulated in Art 3(4) which obliges the Agency to: "*develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation*".

The actions which will be pursued under this activity will focus on making sure that the Agency's HR resources fit the needs and objectives of ENISA, attracting retaining and developing talent and building ENISA's reputation , an agile and knowledge based organisation where staff can evolve personally and professionaly, keeping staff engaged, motivated and with sense of belonging. Emphasis will be placed on competency development and ways to **make ENISA an 'employer of choice'** in order to support ENISA's objectives The activity will seek to build an attractive workspace by establishing effective framework enabling teleworking outside the place of assignment, developing and maintaining excellent working conditions (premises, layout of office space) and implementing modern user-centric IT and teleconferencing tools delivering state of the art corporate services and supporting ENISA's business owners and stakeholders in line with the Agency's objectives.

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 through strategic worfkorce planning in order to ensure the effective functioning of the Agency and maintain high quality of services in the administrative and operational areas. ENISA will further improve the strategic planning and resource management support to the Agency, leading to a constant optimisation of resources under a short and long range time-frame. This would enable ENISA to enhance its future-readiness capabilities and continue its path towards agile, knowledge-based and matrix way of working. The Agency will continue to look into flexible (50/50) working arrangements to better balance work requirements in a pragmatic manner.

In parallel, ENISA will continue to **enhance** secure operational **environment** at the highest level, strive excellence in its infrastructure services based on best practices and agile frameworks. It will also explore cloud-enabled services that are fit for purpose and provide services in accordance with recognised european and international standards and ENISA IT strategy. Besides that, 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. As ENISA aspires to become a trusted partner it will continue by providing customer focused, multi-disciplinary teams that demonstrate a customer centric, can-do and agile attitude.

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	Annual	N/A	Actions implemented according to the timelines
	Caring and inclusive modern organisation	High participation in staff satisfaction survey	Annual	69 %	75 %
11.b Ensure sustainable and efficient corporate solutions and promote continuous improvement	Ensure efficient corporate services	Understand best practices in sustainable IT solutions	Annual	N/A	IT strategy updated accordingly
	Introduce digital solutions that maximise synergies and collaboration in the Agency	Limited disruption of continuity of corporate services	Annual	N/A	BCP for corporate IT, facilities, financial and HR services ensured
	Developing service propositions with additional external resourcing	Handling EUCI at the level of SECRET UE/EU SECRET	By Q2 2024	N/A	Has been accredited
	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				

ACTIVITY 11 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**LATEST RESULTS**	**TARGET 2025[51]**
11.1 Manage and provide horizontal, recurrent, quality support services in the area of resources for ENISA staff and partners	Implement payroll and recurrent administrative services Implement annual recruitment plan Implement annual L&D plan and staff performance Implement annual procurement plan via PPMT Implement insource mission service support Implementation of the ED decision on strategic workforce review [adopted in May 2023] Follow up on FIA centralisation and implementation of results of external analysis on simplification of ENISA financial procedures Analyse procurement services and tenders and propose simplifications Explore further synergies with PMO SLA (e.g. reimbursement of experts)	Management Team IT Management Committee Budget Management Committee Staff Committee	Turnover rates	Annual	4%	3 %
			Establishment plan posts filled		89%	>95%
			Time spent from vacancy announcement to candidate selection		n/a	<300 days
			Percentage of the implementation of approved Recruitment plan		n/a	>90%
			Percentage of the implementation of approved Procurement Plan		n/a	>90%
			Percentage of procurement procedures launched via e-tool (PPMT)		n/a	>90%
			Percentage of budget implementation		100%	>95%
			Average time for initiating a transaction (FIA role)		n/a	<7 days
			Average time for verifying a		n/a	<3 days

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

			transaction (FVA role)			
			Number of budget transfers		4	<4
			Late payments		n/a	<8%
11.2 Implement Agency's Corporate strategy including HR strategy with emphasis on initiatives in talent development, growth and welfare, innovation and inclusiveness areas	Establish / review corporate costing models and mechanisms to forecast, anticipate and timely manage emerging needs Revision of HR related MB decisions on middle management staff, on SNEs, on the framework for learning and development, on the appraisal of TA staff and CA staff, on reclassification of TA staff and CA staff indicated in the corporate strategy Set up of key HR policies in the area of learning and development and review staff welfare and mission policies Introduce modern digital solutions in managing talent that give real time input to managers Modernize the selection process by introducing automated IT tool in the process	Management Board Management Team Staff Committee EUAN BMC	Number of policies/IR revised or adopted	Annual	n/a	>1
			Number of processes reviewed/redesigned		n/a	>1
			Percentage of staff satisfaction survey with talent development		43%	>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, quality support services in the area of facilities, security and corporate IT for ENISA staff and partners	Implement annual IT project plan Implement annual FM plan, maintenance and upgrades, including physical security service provision Upgrade infrastructure to improve working conditions and create a conducive work environment to ensure sustained productivity and employee satisfaction Align the lifecycle of IT services and equipment (servers, used equipment) with objectives Ensure timely implementation of requirements to maintain EUCI at relevant level Review ENISA's geographically disperse IT solutions and systems and propose cost benefit solutions that	Management Team IT Management Committee Budget Management Committee Staff Committee	Satisfaction survey for working environment	Annual	n/a	80 %
			Safety and security incidents reported at workplace in any of the 3 ENISA offices		n/a	<3
			Average time for dealing with facilities management requests		n/a	<3 days

	would maximise ENISA's corporate resilience Follow up on the ServiceNow implementation and explore further synergies for integrating further services (HR, FM, EDO, etc) Follow up on AV implementation and upgrade of meeting rooms					
11.4 Enhance operational excellence and digitalisation through modern, safe and secure and streamlined ways of working and introducing self-service functionalities	Explore synergies between FM and Security service provision by integrating services via one service provider, hence reducing FWC numbers and provide all-inclusive services Implementation of an Identity and Access Management Solution to increase the Cybersecurity posture of the organisation Equipment renewal (laptops/mobiles) to ensure business continuity through updated technology, enhanced security measures and improved equipment performance Implement an effective backup solution (SAN) to enhance business continuity by safeguarding critical data, mitigating the risk of data loss and ensuring a swift operation recovery in the event of system failures, disasters or cyber-attacks Implement new A/V and conference equipment to bolster business continuity by facilitating seamless remote collaboration to ensure high-quality communication and collaboration, which is essential to maintain productivity and operational efficiency Implement of a cloud-based platforms and solutions automate IT delivery services, assure service availability, improve self-service functionalities and provide critical IT-related metrics enabling secure access and sharing of information or device from any location Upgrade physical security measures to ensure high standards for the other ENISA offices to get EUCI accreditation Further development of Athens data centre for high availability purposes to ensure the business continuation and minimisation of downtime risks	Management Team IT Management Committee	Resilience and quality of ENISA IT systems and services (automated or via surveys) [specific KPIs will be defined for each expected result of the output and will be monitored separately] – as generic indicators – • Critical systems uptime//downtime • Staff satisfaction with resolution	Annual	100 % 84 %	99 % 85 %
STAKEHOLDERS AND ENGAGEMENT LEVELS						
Partners: ENISA staff members and EU Institutions, Bodies and Agencies **Involve / Engage:** Private Sector and International Organisations						

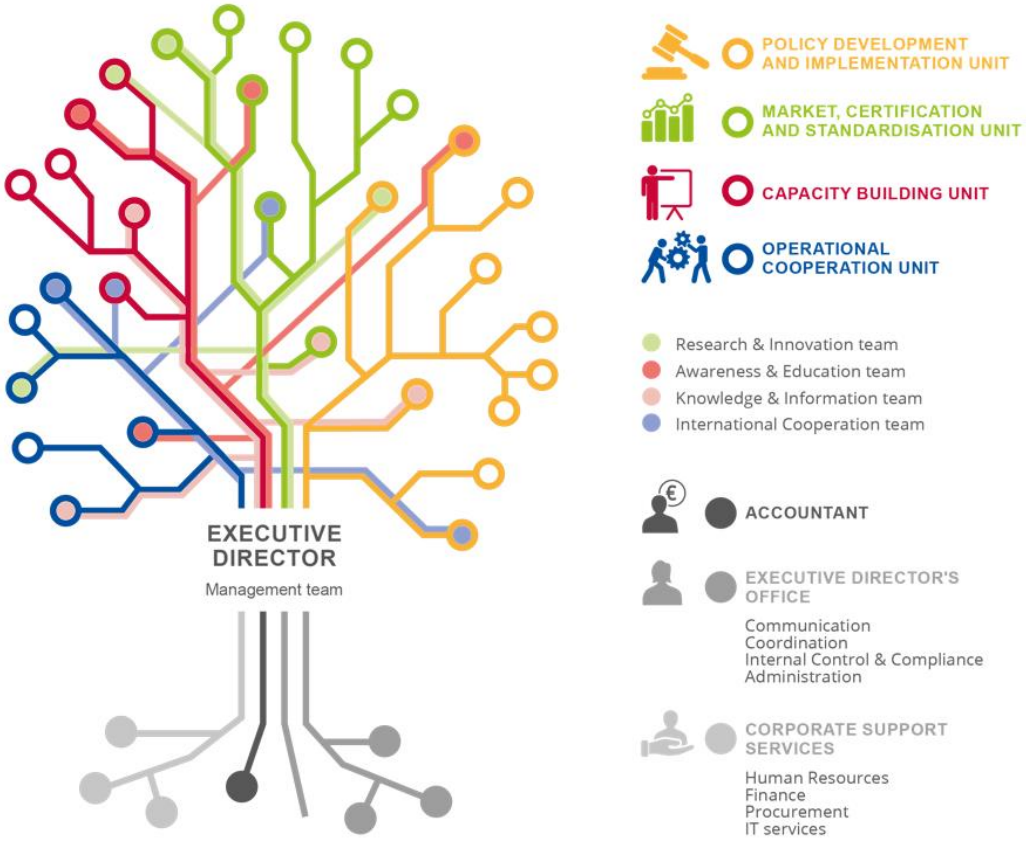
ACTIVITY 11 RESOURCE FORECASTS							
Outputs	SERVICE PACKAGE SUPPORTED	CORE		ESSENTIAL		ON-DEMAND	
		FTE	EUR	FTE	EUR	FTE	FTE
Output 11.1				7,25	443.726		
Output 11.2				4,75	963.484		
Output 11.3				3,75	2.748.387		
Output 11.4				2,75	271.661		
Total activity resources	*Budget: 4.427.258*	*FTE: 19,5*					

Additional required resources for 2025

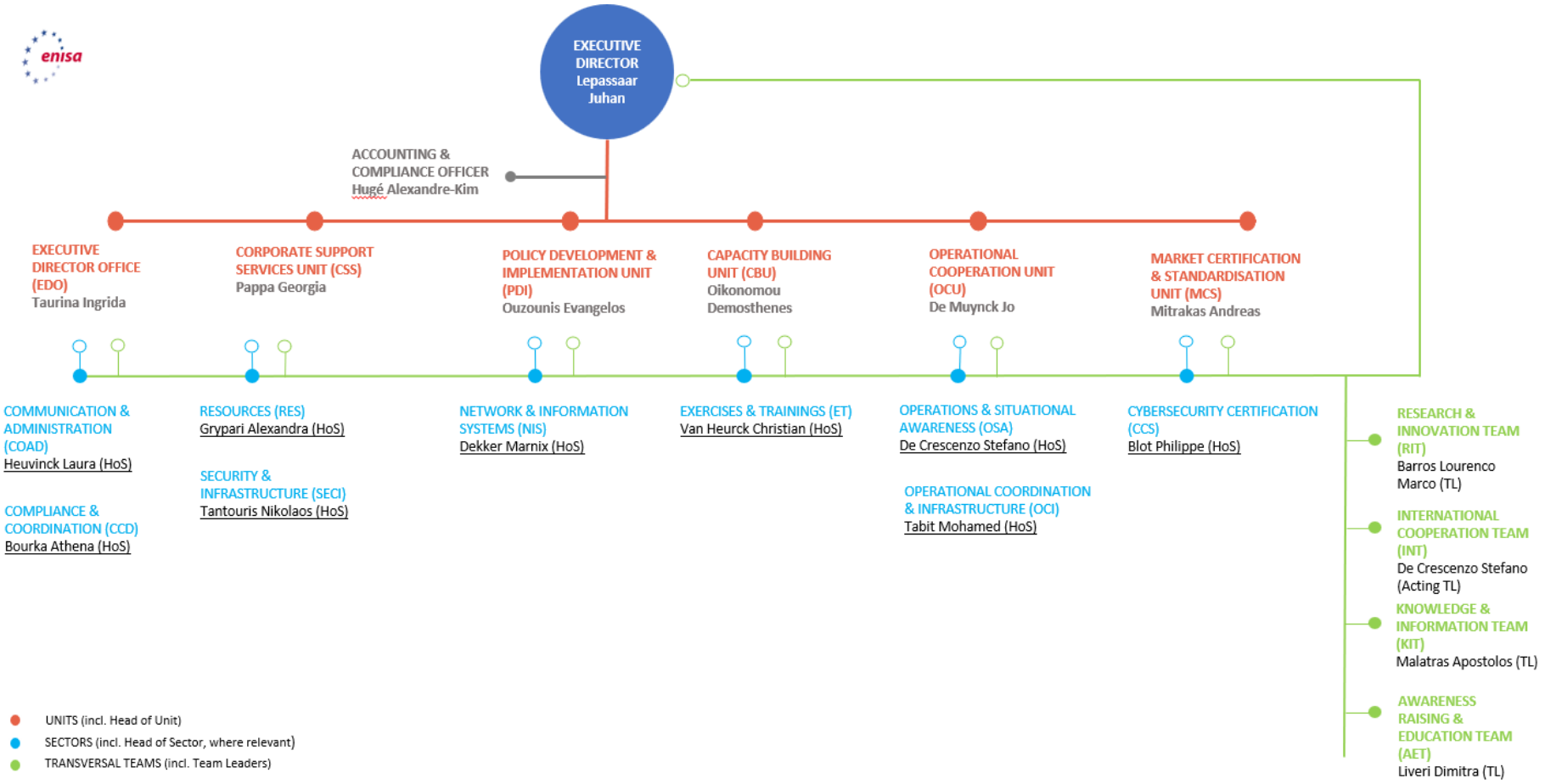
Outputs	SERVICE PACKAGE SUPPORTED	CORE		ESSENTIAL		ON-DEMAND		Outputs	
		FTE	EUR	FTE	EUR		FTE	EUR	FTE
Output 11,1		0	0	0	130.908	0	0	0	0
Output 11,2		0	0	0	180.000	0	0	0	0
Output 11,3		0	0	0	350.000	0	0	0	0
Output 11,4		0	0	0	154.180	0	0	0	0
Remarks	Additional resources required for additional IT equipment and services, intramuros services and HR consultancy support.								

ANNEX

I. ORGANISATION CHART AS OF 01.12.2022



Administrative Organigramme



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 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.
- 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) shall 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	2.359.818,45	10,86
Supporting implementation of Union policy and law	Activity 2	2.494.199,46	12,61
Building capacity	Activity 3	3.800.098,29	16,66
Enabling operational cooperation	Activity 4	3.836.864,47	13,86
Provide effective operational cooperation and situational awareness	Activity 5	2.847.845,46	11,86
Provide services for operational assistance and support	Activity 6	543.366,39	3,86
Development and maintenance of EU cybersecurity certification framework	Activity 7	1.933.619,64	9,56
Supporting European cybersecurity market, research & development and industry	Activity 8	1.967.131,45	11,11
Performance and sustainability	Activity 9	2.084.243,26	12,36
Reputation and trust	Activity 10	1.130.540,21	5,36
Effective and efficient corporate services	Activity 11	3.341.467,85	19,86
TOTAL		**26.339.196**	**128**

III. FINANCIAL RESOURCES 2025 - 2027

TABLE 1: REVENUE

Revenues	2024	2025
EU contribution	24.953.071	25.439.933
Other revenue (EFTA)	883.404	899.263
Other revenue (SLAs, Annex XI)	174.604	174.604
TOTAL	**26.011.079**	**26.513.800**

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	1,95%	25.439.933	25.936.532	26.442.532
- of which assigned revenues deriving from previous years' surpluses	*320.868*		*0*	*0*	*0*
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	883.404	1,80%	899.263	917.041	935.156
*- of which EEA/EFTA (excl. Switzerland) ** *	*883.404*	*1,80%*	*899.263*	*917.041*	*935.156*
- 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		174.604	174.604	174.604
7 CORRECTION OF BUDGETARY IMBALANCES					
TOTAL REVENUES	**26.011.079**	**1,93%**	**26.513.800**	**27.028.177**	**27.552.292**

* - 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 2025-2027 same surplus as indicated under 2024 is included with 3,58% EFTA proportionality factor

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

Table 2: Expenditure (excluding revenue for services rendered)

EXPENDITURE * **	2024		2025		2025
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations	Including Additional required budget
Title 1	14.739.106	14.739.106	15.137.001	15.137.001	15.187.001
Title 2	3.666.898	3.666.898	3.735.701	3.735.701	4.780.092
Title 3	7.430.471	7.430.471	7.466.494	7.466.494	9.582.984
Total expenditure	**25.836.475**	**25.836.475**	**26.339.196**	**26.339.196**	**29.550.077**

EXPENDITURE (in EUR)	Commitment and Payment appropriations * **						
	Adopted Budget 2023	Adopted Budget 2024	Draft estimated budget 2025	VAR 2025 / 2024	Including Aditional required budget 2025	Envisaged in 2026	Envisaged in 2027
Title 1. Staff Expenditure	**12.719.412**	**14.739.106**	**15.137.001**	**2,7%**	**15.187.001**	**15.432.611**	**15.733.817**
11 Staff in active employment	11.019.993	13.058.316	13.518.913	3,5%	13.518.913	13.782.924	14.051.932
12 Recruitment expenditure	404.684	517.889	341.000	-34,2%	341.000	347.659	354.445
13 Socio-medical services and training	923.735	754.501	856.739	13,6%	906.739	873.470	890.518
14 Temporary assistance	371.000	408.400	420.349	2,9%	420.349	428.558	436.922
Title 2. Building, equipment and miscellaneous expenditure	**3.519.470**	**3.666.898**	**3.735.701**	**1,9%**	**4.780.092**	**3.808.655**	**3.882.991**
20 Building and associated costs	1.357.750	1.000.719	1.028.096	2,7%	1.092.359	1.048.174	1.068.632
21 Movable property and associated costs (***)	0	0	0	n.a.	0	0	0
22 Current corporate expenditure	472.650	516.125	528.944	2,5%	954.870	539.273	549.799
23 Corporate ICT	1.689.070	2.150.054	2.178.661	1,3%	2.732.863	2.221.208	2.264.561
Title 3. Operational expenditure	**8.944.613**	**7.430.471**	**7.466.494**	**0,5%**	**9.582.984**	**7.612.307**	**7.760.880**
30 Activities related to meetings and missions	438.600	387.000	398.323	2,9%	690.000	406.102	414.028
37 Core operational activities	8.506.013	7.043.471	7.068.171	0,4%	8.892.984	7.206.205	7.346.852
TOTAL EXPENDITURE	**25.183.495**	**25.836.475**	**26.339.196**	**1,9%**	**29.550.076,67**	**26.853.573**	**27.377.688**
(*) Does not amounts (total of EUR 174 604) for possible revenue under SLAs with ECCC and EU-LISA, ref. Annex XI							
(**) Does not include the additional EUR 15 000 000 granted for Support Assistance Fund							
(***) As from 2023, "Movable property and associated costs" have been included in Chapter 21 and 22 for streamline purpose							

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

In addition to the EU contribution, ENISA is expected to execute in 2025 an additional amount of EUR 15 million stemming from a contribution agreement. This figure is based on Digital Europe Programme 2024 – please refer to Annex XI for the breakdown.

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**

*** unaudited budget outturn estimate**

Budget 2022 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 'normal' 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	2025	2026	2027
ESTABLISHMENT PLAN POSTS	**Authorised Budget**	**Actually filled as of 31/12/2023**	**Occupancy rate %**	**Adopted**	**Envisaged staff**	**Required**	**Envisaged staff**	**Envisaged staff**
Administrators (AD)	63	62	98%	63	63	69	69	69
Assistants (AST)	19	18	95%	19	19	19	19	19
Assistants/Secretaries (AST/SC)								
TOTAL ESTABLISHMENT PLAN POSTS	**82**	**80**	**98%**	82	82	88	88	88
EXTERNAL STAFF	**FTE corresponding to the authorised budget 2023**	**Executed FTE as of 31/12/2023**	**Execution rate %**	**Adopted FTE**	**Envisaged FTE**	**Required**	**Envisaged FTE**	**Envisaged FTE**
Contract Agents (CA)[52]	32	25	78%	32	32	32 + 10 CA contribution agreement	32 + 10 CA contribution agreement	32
Seconded National Experts (SNE)	14	10	57%	14	14	14	14	14
TOTAL External Staff	**46**	**33**	**72%**	**46**	**46**	**56**	**56**	**46**

[52] 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.

TOTAL STAFF[53]	**128**	**113**	**88%**	**128**	**128**	**144**	**144**	**134**

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	10	10	10	10
Seconded National Experts (SNE)	n/a	n/a	n/a	n/a	n/a
TOTAL	n/a	10	10	10	10

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

- Interim workers

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

[53] Refers to TAs, CAs and SNEs figures

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		Envisaged		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		4		4	4
AD 10		4		3		4		4		4	4
AD 9		11		13		14		14		14	14
AD8		25		10		15		15		15	15
AD 7		10		13		13		13		13	13
AD 6		4		16		7		6		6	6
AD 5											
AD TOTAL		63		62		63		63		63	63
AST 11											
AST 10											
AST 9								2		2	2
AST 8		3		3		3		2		2	2
AST 7		2		0		2		2		2	2
AST 6		8		6		7		7		7	7
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		82		82	82
GRAND TOTAL	82		80		82		82		82		82

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 authorised budget 2025	FTE corresponding to the authorised budget 2026	FTE corresponding to the authorised budget 2027
Function Group IV	30	18	30 + 10 contribution agreement	30 + 10 contribution agreement	30 + 10 contribution agreement	30 + 10 contribution agreement
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**	**42**	**42**	**42**	**42**

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 authorised budget 2025	FTE corresponding to the authorised budget 2026	FTE corresponding to the authorised budget 2027
TOTAL	**14**	**8**	**14**	**14**	**14**	**14**

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[54]	Internal (brackets)	External (brackets)	
Expert		6 TAs	n/a	n/a	n/a
Officer		n/a	n/a	n/a	n/a
Assistant		n/a	n/a	n/a	n/a

[54] 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 2017**	**Year 2018**	**Year 2019**	**Year 2020**	**Year 2021**	**Year 2022**	**Actual average over 5 years**	**Average over 5 years (According to decision C(2015)9563)**
AD05	-	-	-	-	-	-	-	2.8
AD06	1	2	3	-	1	1	3,8	2.8
AD07	-	-	-	1	-	2	3	2.8
AD08	1	1	1	2	1	3	4,1	3
AD09	-	1	-	-	-	-	10	4
AD10	-	-	-	-	-	2	10,5	4
AD11	-	-	-	-	-	-	-	4
AD12	-	-	-	-	1	-	10	6.7
AD13	-	-	-	-	-	-	-	6.7
AST1	-	-	-	-	-	-	-	3
AST2	-	-	-	-	-	-	-	3
AST3	1	1	1	-	-	1	5,2	3
AST4	1	1	1	1	-	-	4,33	3
AST5	-	1	-	-	1	-	5,5	4
AST6	-	-	-	1	1	-	3,5	4
AST7	-	-	-	-	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 31.12.2022	HOW MANY STAFF MEMBERS WERE RECLASSIFIED IN YEAR 2022	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	4	-	-	Between 5 and 7 years
	15	6	1	4	Between 4 and 6 years
	14	7	1	5,8	Between 3 and 5 years
	13	1	-	-	Between 3 and 5 years
CA III	12	1	-	-	-
	11	1	-	-	Between 6 and 10 years
	10	4	1	3	Between 5 and 7 years
	9	1	1	3	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[55]	29%
Male Managers	8	80%	5[56]	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

[55] This category comprises the ED and Heads of Unit level (Team Leaders not included)
[56] 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 *57	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%

[57] 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

While the overall mandate for ENISA is to contribute to achieving a high common level of cybersecurity across the Union, the Agency bears social and environmental responsibility for its operations to achieve climate neutrality by 2030 and has an obligation to support the European Commission Green Deal initiative in line with its SPD objectives and values as set by the Management Board.

In 2021 the Management Board of ENISA established – within the Agency's SPD for 2022-2025 – 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, in 2022 the Agency undertook an exercise to map its current climate footprint. Based on an audit of past ENISA emissions for which 2019 and 2021 were used as reference years, it was established that ENISA creates 584 485 GHG emissions (tnCO2eq) annually, with indirect emissions from purchased electricity (50.33%) and air travel (36.80%) being the main sources of impact on the climate.

Furthermore, the audit established that energy emissions per employee in Athens constitute 1 435 tnCO2 per employee whereas energy emissions per employee in Heraklion constitute 10 times as much (14 217 tnCO2/emp). While ENISA staff undertook 770 journeys by air (ENISA staff missions) in 2019, it also organised 79 in person meetings in 2019 (and 125 in person or hybrid/online meetings in 2022). It operated almost entirely online throughout the period MAR 2020 to MAY 2022.

In its path to achieve climate neutrality, a 41% 'automatic' reduction of GHG emissions in comparison to the base year transitional emissions (2019, 2021) is expected due to external factors (reforms undertaken by the host country – Greece). The remaining 59% or 413tn CO2eq will be tackled by ENISA itself, a) through changing and evolving its business practices to lessen their impact on the climate (fewer in-person participations in meetings or events) and b) by off-setting emissions if activities cannot be transformed without undermining the objectives of ENISA's operational mandate. This is pursued under the condition that offsetting is used only when other options are exhausted.

In order to ensure that ENISA is on the correct path towards climate neutrality by 2023 and to promote and enhance ecological sustainability across all the agency's operations, the following key goals (KPIs) have been adopted within its corporate strategy.

- Acquire an EMAS certificate by Q4 2023.
- 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,
- Offset all residual emissions generated through ENISA operations by 2030 at the latest.
- 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.

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 Brussels Office was completed in April 2022 and the office has been operational since then. The office is being used on a daily basis by Brussels based staff, which is a significant benefit for the Operational Cooperation Unit as they are able to communicate easily 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 2023. Indicative resources foreseen:

Resources (indicative)	2024	2025	2026	2027
Head count (FTEs)	**12-13**	**12-13**	**13-14**	**13-14**
Budget (one-off & maintenance costs)	**130.000**	**130.000**	**130.000**	**130.000**

VIII. PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education / day care
In accordance with Art. 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. 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 survey sought to assess the satisfaction levels of stakeholders in relation to the way the agency implements its projects, specifically how work is organised and managed and how the feedback from external stakeholders is taken into account. The results of the stakeholder satisfaction survey sheds much important light on how stakeholders perceive the added value of ENISA's work. On aggregate the results 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.

The mandate of the agency requires that the agency carry out its tasks while avoiding the duplication of Member State activities, therefore the result 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[58], 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.

[58] 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[59], which was adopted in line with the recommendations of the European Anti-Fraud Office (OLAF).

[59] 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	Q4 2023	20mio (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. 13,5 FTEs
2	Support Action fund (activities 5 & 6)	Pending	est. 15 mio	TBD	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. 13,5 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 60 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, the CERT of the EU institutions, bodies and agencies will be annexed to the Single Programming Document 2025-2027 as a separate document.

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

XX-00-00-000-XX-X

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

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

DRAFT Statement of Estimates 2025 (Budget 2025)

European Union Agency for Cybersecurity

CONTENTS

1. GENERAL INTRODUCTION

Explanatory statement

Legal Basis:

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

Reference acts

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

2. JUSTIFICATION OF MAIN HEADINGS

2.1 Revenue in 2025

The 2025 total revenue amounts to € 26339195,527 and consists of a subsidy of € 25439933 from the General Budget of the European Union and EFTA countries' contributions € 899262,527
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

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 82 Temporary Agent posts.

Total expenditure under Title 1 amounts to	€	15.137.000,78

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to	€	3.735.701,49

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of Work Programme 2025 and amounts to	€	7.466.493,72

3. STATEMENT OF REVENUE 2025

Title	Heading	Voted Appropriations 2023 €	DRAFT Appropriations 2024 €	DRAFT Appropriations 2025 €	Remarks - budget 2025
1	EUROPEAN COMMUNITIES SUBSIDY	24.475.757	24.953.071	25.439.933	Total subsidy of the European Communities
2	THIRD COUNTRIES CONTRIBUTION	707.738	883.404	899.263	Contributions from Third Countries.
3	OTHER CONTRIBUTIONS	0	0	0	Subsidy from the Government of Greece
4	ADMINISTRATIVE OPERATIONS	0	0	0	Other expected income.
	GRAND TOTAL	**25.183.495**	**25.836.475**	**26.339.196**	

Article Item	Heading	Voted Appropriations 2023 €	DRAFT 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	25.439.933	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security.
	CHAPTER 10	24.475.757	24.953.071	25.439.933	
	TITLE 1	24.475.757	24.953.071	25.439.933	
2	THIRD COUNTRIES CONTRIBUTION				
20	THIRD COUNTRIES CONTRIBUTION				
200	*Third Countries contribution*	707.738	883.404	899.263	Contributions from Associated Countries.
	CHAPTER 2 0	707.738	883.404	899.263	
	TITLE 2	707.738	883.404	899.263	
3	OTHER CONTRIBUTIONS				
30	OTHER CONTRIBUTIONS				
300	*Subsidy from the Ministry of Transports of Greece*	0	0	0	Subsidy from the Government of Greece.
	CHAPTER 30	0	0	0	
	TITLE 3	0	0	0	
4	ADMINISTRATIVE OPERATIONS				
40	ADMINISTRATIVE OPERATIONS				
400	*Administrative Operations*	0	p.m.	p.m.	Revenue from administrative operations.
	CHAPTER 40	0	0	0	
	TITLE 4	0	0	0	
	GRAND TOTAL	25.183.495	25.836.475	26.339.196	

4. STATEMENT OF EXPENDITURE 2025

Title	Heading	Voted Appropriations 2023 €	DRAFT Appropriations 2024 €	DRAFT Appropriations 2025 €	Remarks - budget 2025
1	STAFF	12.719.412	14.739.106	15.137.001	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE	3.519.470	3.666.898	3.735.701	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE	8.944.613	7.430.471	7.466.494	Total funding for operational expenditures.
	GRAND TOTAL	25.183.495	25.836.475	26.339.196	
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	10.167.810	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	10.167.810	

111	***Other staff***					
1110	Contract Agents		1.967.658	2.507.984	2.618.347	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	732.756	This appropriation is intended to cover basic salaries and all benefits of SNEs.
		Article 1 1 1	2.468.774	3.180.605	3.351.103	
		CHAPTER 11	**11.019.993**	**13.058.316**	**13.518.913**	
12	**RECRUITMENT/DEPARTURE EXPENDITURE**					
120	***Expenditure related to recruitment***					
1201	Recruitment and Departure expenditure		404.684	517.889	341.000	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	341.000	
		CHAPTER 1 2	**404.684**	**517.889**	**341.000**	

13	**SOCIO-MEDICAL SERVICES AND TRAINING**					
132	***Staff Development***					
1320	Staff Development		232.215	447.501	540.757	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	540.757	
133	***Staff Welfare***					
1332	Staff Welfare		691.520	307.000	315.982	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	315.982	
		CHAPTER 1 3	**923.735**	**754.501**	**856.739**	
14	**TEMPORARY ASSISTANCE**					
142	***Temporary Assistance***					
1420	External Temporary Staffing		371.000	408.400	420.349	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
		Article 1 4 2	371.000	408.400	420.349	
		CHAPTER 1 4	**371.000**	**408.400**	**420.349**	
		Total Title 1	**12.719.412**	**14.739.106**	**15.137.001**	
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	1.028.096	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	1.028.096	
		CHAPTER 2 0	**1.357.750**	**1.000.719**	**1.028.096**	
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	450.944	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	450.944	
223	***Corporate and Administrative Expenditures***					
2230	Corporate and Administrative Expenditures		93.000	78.000	78.000	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	
		CHAPTER 2 2	**472.650**	**516.125**	**528.944**	
23	**ICT**					
231	***Core and Corporate ICT expenditure***					
2312	Core and corporate ICT costs		1.689.070	2.150.054	2.178.661	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.
		Article 2 3 1	1.689.070	2.150.054	2.178.661	
		CHAPTER 2 3	**1.689.070**	**2.150.054**	**2.178.661**	
		Total Title 2	**3.519.470**	**3.666.898**	**3.735.701**	
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	398.323	This appropriation is intended to cover costs of outreach activities (communications, stakeholders' management, publication and translations), meetings (including meetings of ENISA's statutory bodies i.e. MB, AG, NLOs, and meetings with other stakeholders) and other representation costs. It also covers mission costs related to the implementation of Activities 9-11 as defined in the SPD 2025-2027 mainly covering horizontal tasks and other administrative services.
		Article 3 0 0	438.600	387.000	398.323	
		CHAPTER 3 0	**438.600**	**387.000**	**398.323**	

37	**CORE OPERATIONAL ACTIVITIES**					
371	***Activity 1***					
3710	Activity 1 - Providing assistance on policy development		330.262	357.135	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3711	Activity 1 - Support for policy monitoring and development		n/a	n/a	832.000	This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT and mission costs).
		Article 3 7 1	330.262	357.135	832.000	
372	***Activity 2***					
3720	Activity 2 - Supporting implementation of Union policy and law		773.404	720.268	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3721	Activity 2 - Supporting implementation of Union policy and law		n/a	n/a	720.268	This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT and mission costs).
		Article 3 7 2	773.404	720.268	720.268	
373	***Activity 3***					
3730	Activity 3 - Capacity building		1.709.239	1.236.591	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3731	Activity 3 - Capacity building		n/a	n/a	1.456.591	This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs).
		Article 3 7 3	1.709.239	1.236.591	1.456.591	
374	***Activity 4***					
3740	Activity 4 - Enabling operational cooperation		2.122.530	1.776.494	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3741	Activity 4 - Enabling operational cooperation		n/a	n/a	1.887.138	This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT and mission costs).
		Article 3 7 4	2.122.530	1.776.494	1.887.138	
375	***Activity 5***					
3750	Activity 5 - Contribute to cooperative response at Union and Member States level		913.512	867.459	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3751	Activity 5 - Provide effective operational cooperation and situational awareness		n/a	n/a	1.179.391	This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT and mission costs).
		Article 3 7 5	913.512	867.459	1.179.391	
376	***Activity 6***					
3760	Activity 6 - Development and maintenance of EU cybersecurity certification framework		804.578	571.896	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3761	Activity 6 - Provide services for operational assistance and support		n/a	n/a	p.m.	This appropriation is intended to cover direct operational costs relevant to the Activity 6 (including operational ICT and mission costs).
		Article 3 7 6	804.578	571.896	p.m.	
377	***Activity 7***					
3770	Activity 7 - Supporting European cybersecurity market and industry		356.027	266.666	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3771	Activity 7 - Development and maintenance of EU cybersecurity certification framework		n/a	n/a	588.628	This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT and mission costs).
		Article 3 7 7	356.027	266.666	588.628	
378	***Activity 8***					
3780	Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities		811.881	711.646	n/a	*As from 2025, whereas the operational activities have been streamlined, this budget line in not used anymore*
3781	Activity 8 - Supporting European cybersecurity market, research & development and industry		n/a	n/a	404.155	This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT and mission costs).
		Article 3 7 8	811.881	711.646	404.155	
379	***Activity 9 - Outreach and education***					
3790	Activity 9 - Outreach and education		489.209	409.315	n/a	This appropriation is intended to cover direct operational costs relevant to the Activity 9 (including operational ICT and mission costs).
		Article 3 7 9	489.209	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	n/a	This appropriation is intended to cover direct operational costs relevant to the Activity 10 (including operational ICT and mission costs).
		Article 3 7 0	195.371	126.000	n/a	

CHAPTER 3 7	8.506.013	7.043.471	7.068.171
TITLE 3	8.944.613	7.430.471	7.466.494
GRAND TOTAL	25.183.495	25.836.475	26.339.196

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

Draft Establishment plan 2025

Category and grade	Establishment plan in voted EU Budget 2024		Establishment plan 2025	
	Off.	TA	Off.	TA
AD 16				
AD 15		1		1
AD 14				
AD 13		2		2
AD 12		4		4
AD 11		3		4
AD 10		4		4
AD 9		14		14
AD 8		15		15
AD 7		13		13
AD 6		7		6
AD 5				
Total AD		**63**		**63**
AST 11				
AST 10				
AST 9				2
AST 8		3		2
AST 7		2		2
AST 6		7		7
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				
Total AST/SC				
TOTAL		**82**		**82**