EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA Single Programming Document 2026 - 2028

Including Multiannual planning,
Work programme 2026
and Multiannual staff planning

JANUARY 2026

CONTACT

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

LEGAL NOTICE

COPYRIGHT NOTICE

Luxembourg: Publications Office of the European Union, 2026

Language version	Output format	Catalogue number	ISBN	ISSN	DOI
English	PDF Web	TP-01-26-001-EN-N	978-92-9204-781-8	2467-4176	10.2824/6090316

ENISA Single Programming Document 2026 - 2028

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

Abbreviations

AAR	Annual Activity Report
ABAC	Accruals-based accounting
ABB	Activity Based Budgetary
ACER	Agency for the Cooperation of Energy Regulators
ACOO	Associated chief operational officer
ACT.	Activity
ADM	Administrator
AEV	Adversarial Exposure Validation
AFS	Anti-fraud strategy
AG	Advisory Group
AHWG	Ad-Hoc Working Group
AIA	AI act
AST	Assistant
BCP	Business Continuity Plan
BEREC	Body of European Regulators for Electronic Communications
BMC	Budget Management Committee
C1	Budget consumed in year
C8	Budget from year carried forward to be paid in following year
CA	Contract agenda
CAB	Conformity Assessment Body
CBU	Capacity Building Unit
CCU	Cybersecurity Certification Unit
CDR	Career Development Review
Cedefop	European Centre for the Development of Vocational Training
CEF	Connecting Europe Facility
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CERT-EU	Cybersecurity Service for the Union institutions, bodies, offices and agencies
CERTI	Certification
CIRAS	Cybersecurity Incident Reporting and Analysis System
CISO	Chief information security officer
COO	Chief operating officer
COSO	The Committee of Sponsoring Organizations of the Treadway Commission
COVID-19	Coronavirus disease 2019
CNECT	Directorate-General for Communications Networks, Content and Technology
CNW	CSIRTs Network
COM	European Commission
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSAT	Cyber Security Assessment Tool
CSDP	The Common Security and Defence Policy
CSIRT	Computer Security Incidence Response Team
CS-NCA	National competent authorities on the security of network and information systems
CSoA	Cyber Solidarity Act
CSPO	Cybersecurity Policy Observatory
CSS	Corporate Support Services Unit
CTF	Capture the Flag
CTI	Cyber threat intelligence
CTL	Cybersecurity Threat Landscape
CVE	Common Vulnerabilities and Exposures
DEP	Digital Europe Programme
DG	Director General
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG NEAR	Directorate General for Neighbourhood and Enlargement Negotiations
DNS	Domain Name System)
DORA	Digital Operational Resilience Act
DSP	Digital service providers
DSO	European Distribution System Operators
EBA	European Banking Authority
EC	European Commission
EC3	European Cybercrime Centre / Europol
ECA	European Court of Auditors
ECATS	European Competent Authorities for Trust Services
ECB	European Central Bank
ECCC	European Cybersecurity Competence Centre
ECEAC	Electricity Cybersecurity Early Alert Capabilities
ECSC	European Cyber Security Challanges
ECSF	European Cybersecurity Skills Framework
ED	Executive Director
EDA	European Defence Agency
ECCG	European Cybersecurity Certification Group
EDD	Executive Director Decision
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EECC	European Electronic Communications Code
EFTA	European Free Trade Association
eID	Electronic identification
eIDAS	Electronic Identification and Trust Services (eIDAS) Regulation
EIOPA	European Insurance and Occupational Pensions Authority
EIT	European Institute of Innovation & Technology
EMAS	Eco-Management and Audit Scheme
ESMA	European Securities and Markets Authority
ENISA	European Union Agency for Cybersecurity
ENTSO	European Network of Transmission System Operators for Electricity
EP ITRE	European Parliament's Committee on Industry, Research and Energy
ERA	European Railway Agency

ESA	European Space Agency
ESG	Environment, Social and Governance
ESMA	European Securities and Markets Authority
ETSI	European Telecommunications Standards Institute
EU Entities	European Union Institutions, Bodies, and Agencies
EUAN	EU Agencies Network
EUCC	European Union Common Criteria scheme
EUCI	European Union classified information
EUCR	European Union Cybersecurity Reserve
EUCS	EU Cloud Certification Scheme
EUDI	European Digital Identity
EUDIR	EU Digital Infrastructure Registry
EUDIW	European Digital Identity Wallets
EU5G	European Union certification scheme for 5G networks
EUIPO	European Union Intellectual Property Office
EU-CyCLONe	Cyber Crisis Liaison Organisation Network
EU-JCAR	EU Joint Cyber Assessment Report
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
EUMSS	EU Managed Security Services
Europol	European Union Agency for Law Enforcement Cooperation
EUVD	EU Vulnerability Database
FGI	Function Group
FIA	Financial Initiative Agent
FTE	Full-time equivalent
FVA	Financial Verification Agent
FWC	Framework Contract
GHG	Greenhouse gas
HoUs	Heads of unit
HRT	Human Resource Teams
HWPCI	Horizontal Working Party on Cyber Issues
IAS	Internal audit service
ICF	Internal Control Framework
ICT	Information and communication technology
IICB	Interinstitutional Cybersecurity Board
INTCEN	EU Intelligence and Situation Centre
IPR	Intellectual property rights
IRM	Interoperable EU Risk Management
IS	Information security
ISAC	Information Sharing and Analysis Centre
IT	Information technology
ITMC	IT management committee
JCAR	Joint Cyber Assessment Report
JCU	Joint Cyber Unit
JRC	Joint Research Centre
KDT	Key digital technologies
KPI	Key performance indicators
L&D	Learning and development
MB	Management Board
MBD	Management board decision
MFF	Multi-annual financial framework
MoU	Memorandum of understanding
MS	Member State
MSA	Market Supervisor Authorities
MSS	Managed Security Services
MT	Management Team
MTPS	Market, Technology & Product Security Unit
NCCA	National Cybersecurity Certification Authority
NCC	National Coordination Centres
NCCS	Network Code on Cybersecurity
NCSS	National Cyber Security Strategies
NIS	Networks and Information Systems
NISD	NIS Directive
NIS2	NIS2 Directive
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
NRA	National regulatory authorities
OCU	Operational Cooperation Unit
OES	Operators of Essential Services
OIB	Office for Infrastructure and Logistics i
OOTS	The Once Only Technical System
O-RAN	Open Radio Access Network
OSA	Operational & Situational Awareness Unit
OSINT	Open source intelligence
OSU	Operation & Support Unit
PMA	Policy Monitoring & Analyses Unit
PMO	Paymaster Office
PQC	Post-Quantum Cryptography
RA	Risk assessment
REU	Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
RFI	Request for information
RoCS	Resilience of Critical Sectors Unit
RP-NCA	see page 113
SC	Secretary
SCCG	Stakeholder Cybersecurity Certification Group
SITAW	Situational awareness
SitCen	Situational centre
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises
SNE	Seconded national expert
SOCs	Security Operation Centres
SOG-IS	Senior Officials Group Information Systems Security
SOP	Standard Operating Procedure
SPD	Single Programming Document
SRP	Single Reporting Platform
TA	Temporary agent
TBD	To be decided
TDL	Top level domain
TREX	Training and exercises
UA	Ukraine
URWP	Union Rolling Work Programme
vCISO	Virtual CISO
WS3	NIS Cooperation Group workstream 3

Foreword

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

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

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

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

Finally, the Agency welcomes the recently proposed Digital Omnibus and the revision of the Cybersecurity Act. In 2026, the Agency will work with our partners to ensure the final provisions will contribute to a trusted and secure single market. I am proud of the progress we have made so far and I am confident that the work outlined in this SPD will help us achieve our goals.

I would like to thank our partners, stakeholders and team members for their hard work and dedication to our mission. Together, we can break new ground towards an even more cyber-secure single digital market that meets the challenges of today and tomorrow.

Juhan Lepassaar
Executive Director

About the Single Programming Document (SPD)

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

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

The SPD is structured in three key sections:

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

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

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

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

Mission statement

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

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

ENISA Strategy

HORIZONTAL OBJECTIVES:

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

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

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

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

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

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

VERTICAL OBJECTIVES:

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

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

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

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

Strategic objective: Strong cyber security capacity within EU

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

Strategic objective: Building trust in secure digital solutions

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of assessing the security of information and communication technology (ICT) products, services and processes and ensuring their trustworthiness, a common European approach covering societal, market, research and foresight, economic and cybersecurity needs is required, along with the possibility of influencing the international community by introducing a competitive edge. Using means such as cybersecurity-by-design, market surveillance and certification will allow trust in digital solutions to be both enforced and promoted.

Section I

General context

The Single Programming Document sets outs the activities that ENISA will undertake in the years 2026 to 2028 in accordance with the Agency's Regulation EU2019/881 on the ENISA Cybersecurity Act[1] and takes into account the new ENISA Strategy, the transposition of the NIS2 Directive, the Cyber Resilience Act (CRA) and the Cyber Solidarity Act (CSoA) among other legislative acts and regulations.

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

These include the following.

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

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

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

Certification. 2025 marked the full entry into force of the EU Common Criteria scheme (EUCC), the very first European cybersecurity scheme adopted, with the celebration of the first EUCC notified Conformity Assessment Bodies (CABs) and of the first certificates, as well as the adoption of a first amendment of the scheme. This significant landmark in the certification field is paving the way for certified products and for the maintenance of certification schemes.

1 Regulation (EU) 2019/881

Also, EUCC certification being a possible option for ensuring conformity of digital products to the Cyber Resilience Act (CRA), ENISA launched pilots with industry on EUCC-CRA mapping. In the coming year, ENISA will develop the new European Digital Identity (EUDI) wallet and Managed Security Services (MSS) schemes according to requests received, with first versions expected to be available from 2026. It will also ensure the maintenance of the full certification framework, enlarging where necessary the scope of these schemes. In addition, work is ongoing on the finalisation and delivery of the EU Cloud Certification Scheme (EUCS) and the EU certification scheme for 5G networks (EU5G).

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

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

Other non-legislative policy developments include the Commission Recommendation on Secure and Resilient Submarine Cable Infrastructures for which ENISA is a member of the expert group of national authorities created under the Recommendation and the EU Action Plan on Cable Security and Commission Recommendation on Submarine Cables that was adopted as a follow-up to the Nevers[2] Call of 9 March 2022. In addition, ENISA continues to support the adoption of the European Cybersecurity Skills Framework and its role in facilitating a professional European attestation scheme.

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

Strengthening ENISA IT Infrastructure. The single programming document 2026-2028 takes into account the actions needed to further enhance the Agency's cybersecurity posture, as well as the migration of ENISA's data centre from Heraklion. The expanded legislative tasks of the Agency, such as the CRA, the EU Vulnerability Database and the Digital Operational Resilience Act (DORA) platforms, require ENISA to scale its cybersecurity maturity over the coming years and maintain it to the highest level with regular reassessments as mandated by Regulation EU2023/2841.

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

2 On 9 March 2022, the informal Council meeting of Telecom Ministers organised in Nevers (France) resulted in a joint call to reinforce the EU's cybersecurity capabilities.

cybersecurity maturity plan likewise will be initiated in 2025 and actions have been planned throughout 2026.

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

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

The full list of statutory tasks that the Agency undertakes under EU legislation is presented in Annex 15.

Section II

Multiannual programming 2026–2028

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA reviewed and updated the Agency's strategy in 2024, which builds on the Cybersecurity Act (CSA) and outlines how the Agency will strive to meet the expectations 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 European citizens and organisations not only benefit but are also key components in the effort to make Europe secure. Most importantly, ENISA's strategy outlines three horizontal strategic objectives and four vertical strategic objectives which are derived from the CSA and set the expected medium to long-term goals for the Agency.

1. MULTI-ANNUAL WORK PROGRAMME

The following table maps the strategic objectives stemming from ENISA's strategy and the indicators used to measure progress towards achieving those objectives. These strategic indicators are structured to cover several years, supporting continuous assessment and tracking progress towards the agency's long-term objectives.

Strategic objectives		Vertical strategic objectives			
		Effective and consistent implementation of EU policies on European cybersecurity	**Effective Union preparedness to respond to cyber incidents, threats and crises**	**Strong cybersecurity capacity within EU**	**Building trust in secure digital solutions**
Horizontal strategic objectives	**Empowered communities in an involved and engaged cyber ecosystem**	Uptake of ENISA recommendations to support Member States and stakeholders in implementing EU legislation	Use of ENISA's secure infrastructure and tools and the added value of support to operational cybersecurity networks	Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, training sessions)	Number of EU certification schemes developed and maintained, number of EU regulations making reference to the CSA, number of active Member States' NCCAs (e.g. issuing European certificates)
	Foresight on emerging and future cybersecurity opportunities and challenges	Number of identified future and emerging areas reflected in policy initiatives and interventions	Operationalisation of the EU Cybersecurity Reserve of which administration and operation is to be entrusted fully or partly to ENISA and used by MSs, Union Entities and on a case by case basis by DEP associated third countries	Number of advisory opinions and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC	Rate of satisfaction with ENISA's support for the implementation of the CRA (Market Supervisory Authorities (MSAs)) and with the European cybersecurity certification framework (ECCG)
	Consolidated and shared cybersecurity information and knowledge support for Europe	Uptake of recommendations stemming from NIS2 Art.18 report	EU Vulnerability Database is operationalised by ENISA and a satisfactory rating from MSs and stakeholders with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats	Percentage of MSs that use the European Cybersecurity Skills Framework (ECSF)	Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and is being successfully operated

1.1. ENISA Corporate Strategy

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

ENISA's corporate vision is to make available a contemporary and attractive workplace for all, based on trust and inclusion, while developing and transforming itself towards a dynamic, service-oriented organisation, an organisation that continuously improves its operational and administrative efficiency by redesigning its operational and administrative processes and optimising its structures, services and use of resources. ENISA aims to ensure that it does the right things in terms of actions or activities (effectiveness) in the correct way in terms of projects and resource management (efficiency) and capitalises on efficiency gains before reinforcing any area of work with extra resources. In order to address this vision, ENISA's 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; i.e. a people centric approach, sustainable governance and service delivery.

ENISA's corporate strategy presents a common vision for a contemporary, flexible and values-driven organisation that empowers staff to deliver outstanding results for people across the EU and beyond. The strategy addresses ENISA's ambition to perform at the highest level in the interests of Europeans while providing its staff members with an attractive workplace and a fulfilling career where excellence and effort are rewarded. Based on the strategies and practices of the European Commission, 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 will support the Agency's goals to enhance its future-readiness and continue on its path towards an agile, knowledge-based and matrix way of working.

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

2. HUMAN AND FINANCIAL RESOURCES: OUTLOOK FOR YEARS 2026-2028

2.1. Overview of the past and current situation

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

2.1.1. Structural adjustments

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

2.1.2. Reallocation of Human Resources

Over recent years, the Agency has introduced various measures to improve the efficiency of its human resources. Although the staff count under the Staff Policy Plan increased by 12 FTEs, from 118 in 2021 to 130[3] , in 2024 to support the Agency in tackling new responsibilities, internal restructuring has remained the primary method for reallocating resources to align with new priorities. A total of 20 posts were restructured and reallocated during this period, highlighting the Agency's agility and ability to adapt effectively to emerging and new service needs. Priority was given to operational units and functions by reallocating posts from corporate functions, many of which have been externalised as much as possible. While this shift has strengthened the human resources supporting the Agency's operational mandate, it has now reached its natural limit. Further internal adjustments at the expense of corporate activities would risk severely compromising essential administrative functions, including IT and physical security, legal compliance, financial and procurement processes and other critical corporate support services.

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

The Agency assessed its internal workforce needs for 2023-2025 during its previous annual workforce reviews, concluding that the Agency would need an additional 41.5 FTEs in order to address all external as well as internal expectations requisite with the tasks and mandate of the Agency. It also concluded that around 50% of all the needs were critical or highly critical (linked with emerging statutory tasks). Thus, on this basis the Agency took steps in 2023 and 2024 to address the highly-critical and critical internal FTE needs to the extent possible including signing a number of Contribution Agreements with the Directorate-General for Communications Networks, Content and Technology (DG CNECT) in 2023 and 2024, to be able to engage a total of 13 Contract Agenda (CA) agents to meet the specific objectives of the contribution agreements. Also, under the direction of its Management Board the Agency took steps to deprioritise or supress a number of outputs in previous work programmes and reassign staff to more critical tasks.

2.1.3. Improving Fulfilment of Posts

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

2.1.4. Maximising Financial Resources

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

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

3 This figure does not include the posts stemming from the contribution agreements.

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

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

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

2.1.5. Service Packages

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

2.1.6. Partnerships and Synergies

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

- **Collaboration with the European Commission**. This includes working with DG CNECT to enhance the preparedness of critical infrastructure in Member States and provide incident response support when needed. Under the Contribution Agreement signed in Q4 2023, the Agency and the European Commission have secured an additional €20 million for 2024–2026, alongside the possibility of a temporary increase of up to 12 contract agent posts to meet service delivery needs. This is in addition to the €15 million added to ENISA's budget to meet a request from Member States for enhanced cybersecurity support via the 'Cybersecurity Support Action' to ENISA in the wake of Russia's invasion of Ukraine. The delivery of support action services has enabled the Agency to implement actions with greater efficiency. This enhanced approach has been recognised and is highly valued by Member States, as evidenced by the significant adoption and use of these services by them and the feedback received. At the end of 2024, the Agency and DG CNECT signed yet another Contribution Agreement, which includes €15.25 million for the implementation of the CRA Single Reporting Platform and the continuation of the Support Action, which will be implemented by 31st December 2027. The agreement includes a remuneration of 7% of the total amount of the action for ENISA for the implementation of the activities. In addition, another contribution agreement was penned with the European Commission in August 2025, through which the Commission entrusts ENISA with the administration and operation of the EU Cybersecurity Reserve with EUR 36 million over three years, including 0.67 million for ENISA to support the Cyber Situation and Analysis Centre.

- **Structured Cooperation with CERT-EU.** Joint efforts have supported the development of better situational awareness across the Union, as required by Article 7 of the CSA Regulations. Products such as Joint Rapid Reports and Joint Cyber Assessment Reports, delivered in collaboration with the European Cybercrime Centre (EC3) and the European External Action Centre (EEAS), underscore the importance of this partnership.

- **Support for EU-LISA (EU Agency for the Operational Management of Large-scale IT Systems in the area of Freedom, Security and Justice)**. The renewal of annual agreements to plan, execute and evaluate cybersecurity exercises is bolstering the Agency's capacity-

building initiatives and enhancing the ability of EU-LISA to deal with complex threat landscapes.

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

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

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

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

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

2.2. OUTLOOK FOR THE YEARS 2026-2028

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

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

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

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

The Council conclusions[4] from 6 December 2024 acknowledge that the expansion of ENISA's important role is the result of recent legislative initiatives, such as the Cyber Resilience Act (CRA) or the revised Network and Information Systems Directive (NIS2), which have entrusted the agency with additional tasks. Its key role was also boosted by the growing scale and complexity of the cyber threats and challenges during the last few years. Therefore, the Council recommends that this increase in tasks should be reflected in adequate resources, without pre-empting the upcoming negotiation of the Multiannual Financial Framework. It is, however, equally important to prioritise actions and to have sound cooperation with other actors in the cyber domain to avoid duplication of tasks.

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

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

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

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

2.3. RESOURCE PROGRAMMING FOR THE YEARS 2026-2028

2.3.1. Financial resources

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

The current total appropriations in the EU Budget for 2026 amount to EUR 26.9 million. However, the Agency's draft estimates far exceed this budgetary limit and, despite deprioritising a number of statutory tasks in line with the guidelines agreed with the Agency's Executive Board[5] , the Agency needs more resources in 2026 to be able to fulfil its core mandate effectively. The additional required budget that the agency put forward in the second adopted draft of the single programming document 2026-2028 amounted to an additional EUR 11.85 million. This amount includes the budget required to scale up ENISA's cybersecurity maturity, migrate its data centre from Heraklion and funding needed to maintain its

4 https://data.consilium.europa.eu/doc/document/ST-16527-2024-INIT/en/pdf.
5 Criteria for prioritising operational activities are based on 1) Legal requirements: legislative mandates obligating the Agency to carry out specific tasks (NIS2, CRA, CSOA etc.); 2) Urgency and deadlines: legal acts requiring the Agency to take action within a specified timeframe or on a recurring basis, often requiring preparatory steps before a legal act is in force; 3) Resources: do new tasks lead to additional resource requirements in order to be able to carry out the work? 4) Stakeholder feedback: Actions prioritised by Member States (MSs) and the Commission based on their input and feedback; 5) Added value and impact: Impact and added value of the output for stakeholders as described in the Agency annual activity report.

operational activities in line with the needs of its stakeholders and the additional FTEs put forward to accommodate that end. For the years 2027 and 2028 the Agency put forward an additional required budget for the implementation of the cybersecurity maturity plan of EUR 3.5 million recurring per year from 2028 onwards and EUR 800 thousand from 2028 onwards recurring every year for the data centre migration.

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

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

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

2.3.2. Human resources

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

Though the initial internal workforce needs for 2026-2028 – which were put forward by the activity managers and subsequently assessed and validated by the administration – add up to a very similar total of 41 FTEs (it was 41.5 FTEs for the period 2023-2025) to cover all external expectations and essentially deliver the full plethora of tasks within ENISA's mandate, it is important to stress that 64.2% (or fully 27 FTEs) of those needs are considered non-critical. This means that the Agency will be able to mostly use its regular mechanisms via working programme reprioritisation of tasks in the mid-term perspective and the reprofiling or restructuring of current functions, to try to address these needs by the end of 2028.

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

The migration of the data centre and the scaling up of ENISA's cybersecurity maturity plan requires additional resources, for both the execution of the plan and on-going maintenance, from the operational and corporate units responsible for platforms, systems and capabilities. The Agency will capitalise on its human resources to undertake a large number of the tasks in-house, as described in Article 3 paragraph 4 of the CSA, in order to ensure trusted services and business continuity. The Agency put forward an additional 5.5 FTEs needed for both the

implementation of the cybersecurity maturity plan and the data centre migration in its adopted draft V.2 single programming document 2026-2028 of July 2025. For the years 2027 and 2028 the Agency requested additional human resources of 6 FTEs for the implementation of the cybersecurity maturity plan and 1.5 FTEs for the migration of the data centre.

2.4. STRATEGY FOR ACHIEVING EFFICIENCY GAINS

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

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

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

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

The Agency continues to implement its work programme by systematic use of its statutory bodies (NLO Network, ENISA Advisory Group) as well as other statutory groups such as the Stakeholder Cybersecurity Certification Group (SCCG as set out in CSA Art.22), NISD Cooperation Group and its work-streams, European Competent Authorities for Trust Services (ECATS) Art.18 of the eIDAS regulation, other expert groups created under Union law and its own ad hoc expert groups. The Agency relies on these groups so as to avoid duplication of efforts, to 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 Art.3(3) of the CSA, to avoid duplication of the activities of Member States and to take into consideration existing expertise in Member States. Hence, all activities listed under sections 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 examined by external experts.

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

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

In addition, as part of its strategy to achieve efficiency gains at the IT level, ENISA will focus on enhancing synergies and interoperability between existing and newly developed platforms, particularly in the domain of Cyber Threat Intelligence (CTI). ENISA aims to streamline information sharing and threat detection capabilities across the EU cybersecurity ecosystem. A key component of this strategy involves developing shared CTI platforms that integrate with existing systems, allowing for real-time data exchange. ENISA will also prioritise the creation of interoperable tools and interfaces, such as CRA, DORA, and the EU Vulnerability Database, reducing redundancy and enabling more efficient resource allocation. This approach not only supports operational readiness but also ensures that EU-wide cybersecurity efforts are more cohesive, scalable and adaptable to emerging threats. The shared platforms will enable ENISA to deliver targeted cybersecurity services to a wider range of stakeholders, enhancing overall resilience while optimising operational costs.

Section III

WORK PROGRAMME 2026

This is the main body of the Work Programme; It describes what the Agency's operational and corporate activities aim to deliver in 2026 towards achieving its strategic objectives based on ENISA's strategy and to fulfil its mandate. A total of eight operational activities and three corporate activities have been identified to support the implementation of ENISA's mandate in 2026.

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

1. 2026 WORK PROGRAMME PRIORITIES

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

1.1. Policy Monitoring & Resilience of Critical Sectors

State of Cybersecurity in the EU Report (NIS2 Article 18). ENISA will publish the second edition in cooperation with the NIS Cooperation Group and the European Commission and will ensure follow-up on the recommendations.

Critical Sector Resilience. ENISA will assist Member States in enhancing cybersecurity maturity through a study of NIS Investments, the NIS360 service catalogue and the EU action plan for hospitals and healthcare providers under NIS2.

Union Risk Assessments. ENISA conduct coordinated stress tests on resilience and assess supply chain risks to evaluate and strengthen critical infrastructure.

Sectorial & Horizontal Working Groups. ENISA will support NIS2 workstreams to refine policies and address emerging threats.

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

1.2. Capacity Building

Cyber Europe 2026. ENISA will host the 8th edition of Europe's largest cybersecurity exercise, testing the revised Cyber Crisis Management Blueprint in response to evolving geopolitical threats.

European Cybersecurity Skills Framework (ECSF). ENISA will assist Member States in adopting ECSF to standardise cybersecurity training and workforce development.

Strategic Alignment: Strong cybersecurity capacity within the EU.

1.3. Operational Cooperation, Support Services & Situational Awareness

Strengthen cooperation. ENISA will strengthen CSIRTs Network and EU-CyCLONe cooperation by providing threat assessments, vulnerability analysis and cross-border incident response.

Threat Intelligence & Preparedness. ENISA will ensure that stakeholders are informed about cyber threats, vulnerabilities and crises to improve EU-wide resilience.

EU Cybersecurity Reserve (Cyber Solidarity Act). ENISA will operationalise the reserve to enhance large-scale incident response capabilities (financed via contribution agreement).

EU Cybersecurity Networks & Platforms. ENISA will develop and upgrade IT systems for operational support, including the EU Vulnerability Database and CRA Single Reporting Platform (financed via contribution agreement).

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

1.4. Certification & Market Support

EU Certification Schemes. ENISA will develop candidate schemes for EU Managed Security Services (EUMSS) and EU Digital Wallet (EUDIW) in line with EU Cybersecurity Certification Framework.

Support implementation. ENISA will support CRA implementation with technical guidance, market surveillance and analysis, and the assessment of harmonised standards to help relevant stakeholders, SMEs in particular.

Strategic Alignment: Building trust in secure digital solutions.

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

1.5. Strengthening ENISA's IT infrastructure

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

Data Centre Migration. ENISA will complete the transition of its data centre from Heraklion by the end of 2026.

Cybersecurity maturity plan. ENISA will implement a comprehensive framework for cybersecurity maturity aligned with Regulation (EU) 2023/2841 that will support expanded legislative tasks under the CRA, the EU Vulnerability Database and other regulations.

The following graphs provide insights into the allocation of resources for each of the operational activities in the 2026 work programme.

Table 1 presents the budget allocated to each of ENISA's operational activities financed from the Title 3 EU subsidy budget. Please note that activity 4 manages the IT platforms and systems on behalf of the all-operational activity business owners. Actions under Activity 6 are financed via contribution agreements; see table 3 for further information on contribution agreements and annex 11.

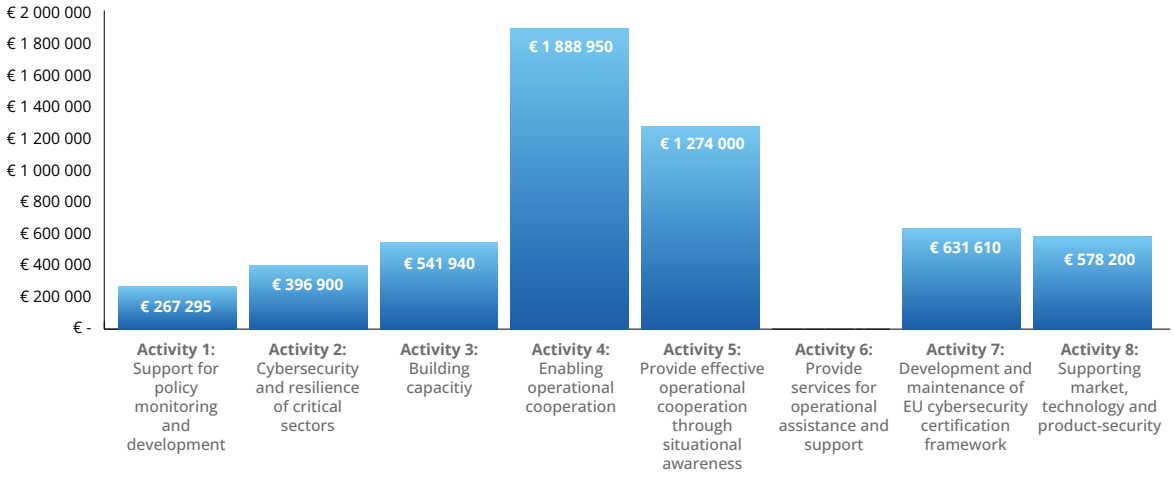


Table 2 presents the allocated number of target FTEs for each of ENISA's operational activities financed from Title 1 EU subsidy budget.

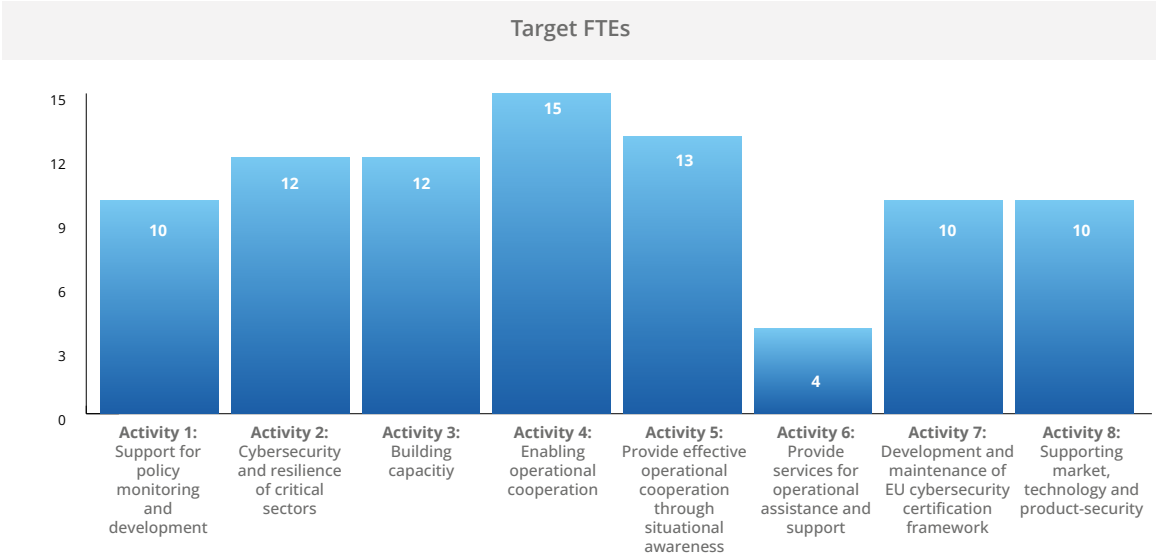


Table 3 presents the 2026 forecast appropriations for commitment in the contribution agreements in the Title 4 budget.

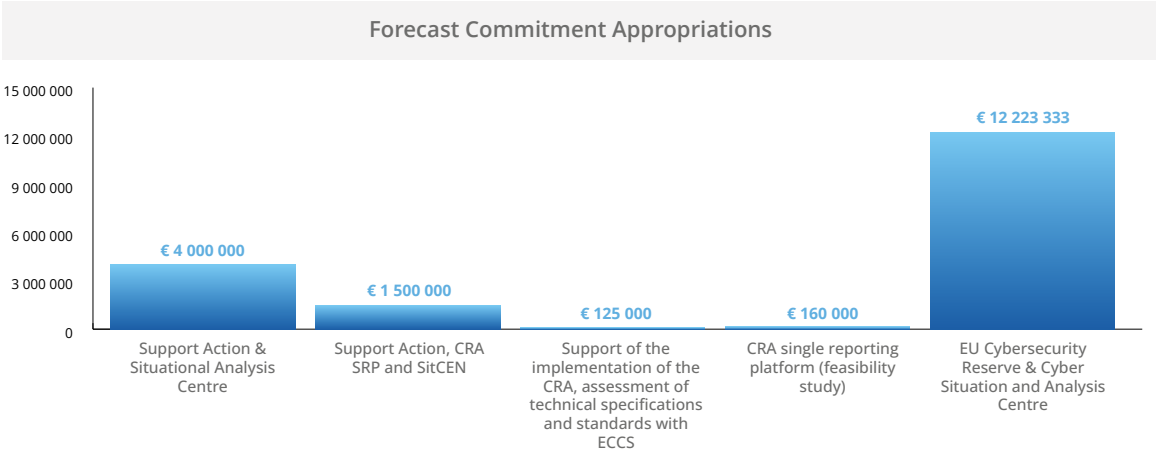
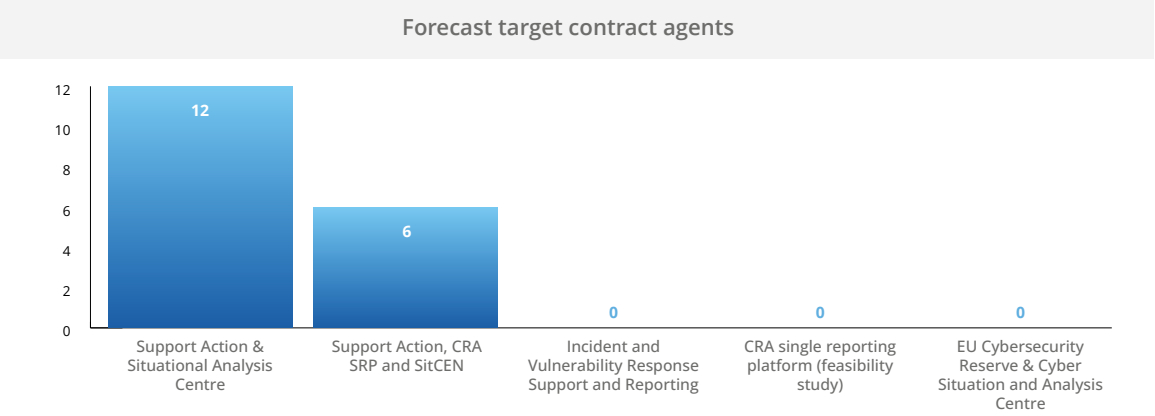


Table 4 presents the forecast number of FTE contract agents financed via the contribution agreements in the Title 4 budget.

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



Service packages

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

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

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

Stakeholders and engagement level

Stakeholder strategy is expected to the reviewed towards the end of 2025. As a result this section will be reviewed and updated according to the outcome of the strategy during the drafting of the 2027-2029 work programme.

KPIs / metrics

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

ACTIVITY 1:
Support for policy monitoring and development

Overview of activity

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

As such, under this activity, ENISA will support Union institutions and MSs on new policy initiatives[6] through evidence-based inputs into the policy development process. ENISA will also conduct policy monitoring in coordination with and in support of other EU institutions, bodies and MSs. Such monitoring will facilitate the identification of potential areas for policy development and measures for policy implementation. This will also be supported by the development of in-house capabilities to provide timely, regular, and consistent advice on the effectiveness of existing Union policy and law, in accordance with the EU's institutional competencies using the 'Implementation Check' model and together with Activities 2 and 8 in particular.

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

Activity 1 leads the Index service package and supports the NIS, TREX and CERTI service packages. The Activity supports the European Commission (COM) and European External Action Service (EEAS) initiatives for Eastern partnerships or similar.

The full list of statutory tasks that the activity undertakes based on EU legislation is presented in annex 15.

Link to strategic objective (ENISA strategy)

- Empowered communities in an involved and engaged cyber ecosystem.
- Consolidated and shared cybersecurity information and knowledge support for Europe.
- Effective and consistent implementation of EU policies for cyber resilience.

Indicator for strategic objectives

Uptake of recommendations stemming from NIS2 Art.18 report.

Number of identified future and emerging areas adopted for policy interventions.

6 Horizontal initiatives on NIS2 sectors and CRAs.1

ACTIVITY 1 OBJECTIVES

Description	CSA article and other EU policy priorities	Timeframe Of Objective	Indicator	Target
1.A By the end of 2026 implement a policy monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, support and assistance to national and Union policymakers in cybersecurity.	Art.5 CSA Art.9 CSA	2026 and continuous thereafter	Assessment of ENISA advice on EU policy (stakeholder survey, desktop research)	75% stakeholder satisfaction from ENISA's advice (among EU policy makers)
1.B By Q3 2026 and in collaboration with Activity 2, aim to ensure that two-thirds of policy observations within the first State of Cybersecurity in the Union report have been followed up by MSs and COM.	Art.18 NIS2	2026 and continuous thereafter	Assessment of MSs use of the Art.18 report (stakeholder survey, desktop research)	Two-thirds of MSs are using Art.18 report as input for their cybersecurity strategies All MSs use ENISA support and tools for work on their NIS Strategies

ACTIVITY 1 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
1.1 Assist MSs to implement, assess, review National Cybersecurity Strategies and policies. Enhance a culture of trust and cooperation among MSs, also through peer reviews.	Stakeholders receive technical advice with the evidence needed for policy-making activities and the definition of implementation measures	NIS CG, including relevant work streams; National Liaison Officers (NLOs), including relevant subgroups, Advisory Group	Rate of use by MSs of the National Capabilities assessment framework or the peer review framework, including the code of conduct.	Biennial (Survey), Annual dialogues, and annual desktop research	NA	Two thirds of MSs are using Art.18 report as input for their cybersecurity strategies and policy-making. All MSs use ENISA support and tools for the work on their NIS Strategies and policy-making
1.2. Collect relevant evidence by maintaining and enhancing the EU cybersecurity index and use such evidence to inform ENISA's support on strategies, as per output 1.1. Present collected knowledge in the Report on the State of Cybersecurity in the Union, further contextualising it with other ENISA sources, e.g. the CRA Market Analysis (Activity 8).			Rate of contribution to State of the Cybersecurity in the Union Report by CSIRT N and NIS CG.		Contribution by all MSs	100%
1.3. Maintain analyses of time-sensitive policy observations offering technical advice for policy development and implementation by mapping gaps, challenges and needs in implementing NIS2 and other EU legislative acts.			Assessment of timeliness, regularity and consistency of advice provided during policy development.		NA	75% stakeholder satisfaction from ENISA's advice (among EU policy-makers)

Stakeholders and Engagement Levels

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

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

ACTIVITY 1 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: EUR €267 295**	**FTE: 10[7]**

7 Target FTEs.

ACTIVITY 2:
Cybersecurity and resilience of critical sectors[8]

Overview of activity

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

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

Secondly, under this activity, ENISA supports MSs and the Commission in addressing specific threats and risk scenarios for the Union related to critical sectors (supply chains), by considering technology or market developments such as Open Radio Access Networks (O-RAN) and other Union coordinated risk evaluations (such as Nevers call in 2024, Cyber risk posture for telecoms and energy in 2024), the Council Cyber Posture[9] , the Union coordinated supply-chain risk assessments (under NIS2), and Union coordinated preparedness tests (aka resilience stress tests, under the Cyber Solidarity Act). Based on the stress tests methodology developed by ENISA, this activity supports the implementation of the cables security[10] toolbox.

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

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

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

The full list of statutory tasks that the activity undertakes based on EU legislation is presented in annex 15.

8 The term critical sectors is used in this context to cover ALL sectors within the scope of the NIS2 Directive.
9 https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.
10 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009.

Link to strategic objective (ENISA strategy)

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

Indicator for strategic objectives

Uptake of ENISA recommendations to support Member States and stakeholders in implementing EU legislation

ACTIVITY 2 OBJECTIVES

Description	Csa Article And Other Eu Policy Priorities	Timeframe Of Objective	Indicator	Target
2.1. Implement common frameworks and joint tools for NIS2 in the areas of (a) risk management, (b) security measures and (c) incident reporting for all EU sectors, and in line with industry good practices and international standards.	CSA Art.5 and Art.6 NIS2 Directive	Frameworks pilot by 2026	Implementation of pilot programme (number of sectors piloting the frameworks, feedback scores on usability)	20MSs to adopt, use or endorse the frameworks
		Full implementation by 2027		>75% usability score
2.2. Provide continuous comprehensive support to MSs for implementing Union's regulatory cybersecurity requirements and raising resilience across critical sectors.	CSA Art.5 and Art.6 NIS2 Directive	Full implementation by 2027	Requests received by the NIS CG or MSs or other community groups	>80% of requests received have been resolved for a maximum of 20 requests
				>75% satisfaction with ENISA support over period
2.3. Help increase the overall maturity level of critical sectors under the NIS2 Directive.	CSA Art.5 [possibly NCCS] NIS2 Directive	End of 2027	Maturity assessment based on the updated NIS360 methodology	>2 sectors improving maturity

ACTIVITY 2 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
2.1. Support Member States with implementation of policy files (such as NIS2, DORA, etc)	NIS2 frameworks for risk management, security measures and incident reporting	DG CNECT NIS CG	Framework usage	Annual (Internal count)	N/A	to be mapped against national frameworks from 3 MS
			EU register for digital entities is used by all MSs	Annual (Report)	(2025) 5 MSs use EUDIR	at least 10 MS to use EU Digital Infrastructure Registry (EUDIR)
			Coherence in the level of implementation between NIS2 and other frameworks, e.g. DORA, NCCS	Satisfaction survey	N/A	60%
2.2. Support Member States with union coordinated risk evaluations, and union coordinated preparedness tests	Support Union-wide risk evaluations and risk scenarios (health, transport, vehicles) and their follow-up (5G, Nevers) Coordinated risk assessment of critical supply chains	DG CNECT NIS CG	Stakeholder satisfaction	Biennial (Survey)	94%	70%
			Number of sectorial situational awareness reports	Annual (Internal count)	6	6
2.3. Improve cybersecurity and resilience in the NIS sectors	Stakeholders use the NIS service packages to improve the security and resilience of the sectors	DG CNECT, NIS CG, Sectorial EU ISACS, Sectorial EU agencies	Number of critical sectors increasing maturity based on NIS360	Annual (Internal count)	3	3
			Number and frequency of services or workflows delivered to NIS sectors	Annual (Internal count)	21	10
			Stakeholder satisfaction	Biennial (Survey)	94%	70%
2.4. Perform an annual check on policy implementation and improve maturity of sectors	MSs and EU institutions, both horizontal and sectorial stakeholders, use the NIS investments, the NIS360 and the cyber posture briefs as reference documents for policy making	DG CNECT, NIS CG, Sectorial EU ISACS, sectorial EU agencies, AG as necessary	Number of critical sectors assessed by NIS360 and cyber posture briefs	Annual (Internal count)	10	at least 6

Stakeholders and engagement levels

Partners: CNECT, NIS CG, National competent authorities, Sectorial DGs, Sectorial Union Entities, Sectorial competent authority groups, sectorial ISACs.
Involve / Engage: NLOs, essential and important entities in the scope of NIS2 and industry associations/ representatives, ENISA Cybersecurity Directors Group.

ACTIVITY 2 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: €396 900**	**FTE[11]: 12**

11 Target FTEs.

ACTIVITY 3:
Capacity Building

Overview of activity

This activity seeks to improve the capabilities of Member States, Union Institutions, bodies and agencies, as well as public and private stakeholders from NIS2 Sectors. It focuses on improving stakeholders' resilience and response capabilities and increasing their preparedness.

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

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

The Agency, in collaboration with relevant Union Entities, Members States' operational communities and NIS2 sectors, will conduct a limited number of targeted exercises (CSA Art.6(1)h) and accompanying training sessions (CSA Art.6(1)(i) focusing on empowering the trainers and enhancing the resilience, maturity and preparedness of the NIS sectors (in cooperation with activities 2, 4 and 6). In cooperation with CERT-EU, it will devise and deliver a targeted capacity building programme to assist Union Entities in implementing Regulation (EU) 2023/2841. In addition, ENISA will support the Cybersecurity Blueprint in the context of Cyber Europe. Given the advanced planning stage of Cyber Europe, ENISA will integrate the strategic and political layers and their scope in accordance with the resources available.

The activity will contribute to the INDEX service package by developing indicators and collecting data to measure progress in closing the cyber talent gap in line with the EC Communication on the Cybersecurity Skills Academy. It will provide analytical insights on EU cybersecurity capacity and the awareness and cyber hygiene of citizens and SMEs in the EU in the context of the State of Cybersecurity in the Union (NIS2 Art.18).

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

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

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex 15.

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

Percentage of MSs that use the European Cybersecurity Skills Framework

ACTIVITY 3 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
3.1. Maintain and regularly update the European Cybersecurity Skills Framework (ECSF).	EU Communication on Cyber Security Skills Academy Arts.10 and 6	2027	Number of MSs endorsing the ECSF framework	18
			Stakeholder satisfaction rate	95%
3.2. Community empowerment through maintaining and evolving relevant toolkits, methodologies and standards.	CSA Arts.4, 6, 7(5) and 10 REU Art.10	2027	Number of MSs and Union institutions, bodies, offices and agencies using ENISA's toolkits, methodologies and frameworks	20

ACTIVITY 3 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
3.1. Support the adoption and uptake of EU's Cybersecurity Skills Framework	Measure and report on the skills gap including developing indicators to be used for Cybersecurity IndexArt.18a Map the skills arising from new policy instruments Promote the adoption of ECSF in MSs, in training organisations and academia and ensure its regular update in line with the Cyber Skills Academy Communication, to include skills attestation schemes.	Ad hoc Working Group (AHWG) on Cybersecurity Skills, ECCC WG 5 on Skills	Stakeholder satisfaction	Biennial (Survey)	91%	93%
			Number of MSs endorsing ECSF	Annual	N/A	17
			Number of training organisations endorsing ECSF in their training programmes	Biennial	N/A	3
			Number of Training Organisations endorsing ECSF in their training programmes	Annual	N/A	8
3.2. Organise targeted exercises and support stakeholders to plan and execute their own exercises	Organise a set of limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders (e.g. Cyclone, CSIRTs Network, Union Entities). Orchestrate the execution of exercises for specific target audiences including those defined in Cooperation Agreements with other EU entities providing tools such as methodologies, templates and providing them access to a community of peers. Follow up on the findings of previous exercises and ensure timely and appropriate implementation of lessons learned. Assist Union Entities in implementing Regulation (EU) 2023/2841 (mostly arts.4 and 11) by providing tools such as methodologies, templates as well as access to a community of peers.	NLO Network (as necessary) CSIRTs Network (as applicable) EU-CyCLONe members (as applicable) NIS Cooperation Group (as applicable) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as applicable) CERT-EU	Number of people impacted directly and/or indirectly by exercises organised by ENISA	Annual (Report)	N/A	10 000
			Satisfaction of entities or communities participating in the capacity building activities organised by ENISA	Annual	N/A	93%

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

Stakeholders and engagement levels

Involve / Engage: Training organisations, private entities in NIS2 sectors, CSIRTs Network and related operational communities, European ISACs, EU-CyCLONe members, Blueprint, National Competent Authorities through the NIS Cooperation Group Work Streams, AHWG on Awareness Raising and Education, AHWG on Skills, EEAS, DG NEAR, DG CONNECT, Cybersecurity professionals, the Horizontal Working Party on Cyber Issues (HWPCI), the European Digital Infrastructure Consortium (EDIC), ECCC Working Group 5, European Digital Infrastructure Consortium.

ACTIVITY 3 RESOURCE FORECASTS

	Budget		FTEs
Activity resources from EU subsidy	**Budget: €541 940**		**FTE[12]: 12**

12 Target FTEs.

ACTIVITY 4: Enabling operational cooperation

Overview of activity

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

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

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

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

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

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

Finally, this activity will also seek to contribute to the Union's efforts to cooperate with third countries and international organisations on cybersecurity, including implementing the revised ENISA international strategy[13] and to contribute to the ENISA stakeholder strategy.

This activity supports SITAW, INDEX and NIS service packages.

The full list of statutory tasks that the activity undertakes arising from EU legislation is presented in annex 15.

13 Inline where applicable with the EU International Digital Strategy adopted in June 2025.

Link to strategic objectives (ENISA STRATEGY)

- Empowered communities in an involved and engaged cyber ecosystem
- Effective Union preparedness and response to cyber incidents, threats and cyber crises
- Consolidated and shared cybersecurity information and knowledge support for Europe

Indicator for strategic objectives

Use of ENISA's secure infrastructure and tools and standard operating procedures coordinated by ENISA

EU Vulnerability Database is operationalised by ENISA and used by MSs

Reporting platform under CRA is operationalised and used by stakeholders

ACTIVITY 4 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
To strengthen the interaction and trust within and between key EU operational and cyber-security communities (CSIRTs Network, EU-CyCLONe, HWPCI and the NIS Cooperation Group)	NIS2 Arts.7, 10, 15 and 16 CSA Arts.6 and 7 CRA Art.16 CSOA Art.11	End of 2026	Assessment of high level of operational interaction between CSIRTs Network, EU-CyCLONe, HWPCI and the NIS Cooperation Group.	>60% of stakeholders agree that ENISA has enabled the functioning of a network and supported the building of trust within the network
			ENISA is judged as a key enabler of trust within and between the CSIRTs Network, CyCLONe, HWPCI and the NIS Cooperation Group.	>60% of stakeholders agree that ENISA has enabled interaction and trust between the networks and communities
Review and implement both the ENISA stakeholder strategy and ENISA international strategy	CSA Art.12	2026	Coherence of ENISA's International Engagement with the Agency's strategy.	Updated international strategy
			Comprehensive knowledge management and stakeholder management system is established.	Establish framework for knowledge management and stakeholder management
Develop and maintain relevant operational IT systems and platforms to support all operational communities and enhance synergies.	NIS2 Arts.7, 10, 12, 15 and 16 CSA Art.7 CRA Art.16	2026	Relevant IT systems are maintained and new mandatory platforms are developed.	IT Operations are consolidated and synergy plan being implemented (2026)

ACTIVITY 4 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
4.1. Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs Network and EU-CyCLONe members HWPCI and the NIS Cooperation Group.	Enhanced Information Sharing and cooperation among the CSIRTs Network and EU-CyCLONe members and enhanced interaction with HWPCI and the NIS Cooperation Group.	CSIRTs Network and EU-CyCLONe members, HWPCI and NIS Cooperation Groups.	Stakeholder satisfaction	Biennial (survey)	89%	89%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)	N/A	Core platforms remain operational during at least one large-scale cyber exercise annually
			Number of joint sessions established	Annual (report)	1 joint session per year	1 joint session per year.
4.2. Maintain, develop and promote ENISA Cyber Partnership programme aiming at information exchange to support the Agency's understanding of threats, incidents involving vulnerabilities and cyber security events	Operationalisation of the Cyber Partnership Programme	CSIRT Network, EU CyCLONe, Union Entities, HWPCI, MB	Stakeholder satisfaction	Biennial (survey)	84%	80%
			Number of new and total partners in the ENISA partnership programme	Annual (report)	4	4
			Percentage of RFI answered by members of partnership programme	Annual (report)	N/A	50%
4.3. Implement the revised ENISA international strategy and outreach programme	EU values recognised by international stakeholders International cooperation that supports ENISA objectives	MT, EEAS, COM and (MB as required)	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Internal satisfaction with international coordination	Annual (survey)	N/A	>70
4.4. Develop, maintain and upgrade IT systems and platforms for operational activities	Consolidation of operational IT with view to supporting ENISA operations	CSIRTs Network, CyCLONe members, NIS Cooperation Group and Business owners for ENISA Operational IT systems.	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			IT architecture for external operational IT services	Biennial update	N/A	One IT architecture for Operational IT services
			ENISA operational IT	Annual (report)	N/A	Key deliverables included in ENISA annual report
4.5 Development of stakeholder and knowledge management systems and frameworks	Implementation of stakeholder strategy	MT and MB as required	Stakeholder satisfaction with knowledge management and stakeholder management system.	Biennial (survey)	N/A	Phase 1: assessment of operational needs achieved

Stakeholders and engagement levels

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

Involve / Engage: NISD Cooperation Group, operators of essential services (OESs) and digital service providers (DSPs), Information Sharing and Analysis Centres (ISACs).

ACTIVITY 4 RESOURCE FORECAST

	Budget	FTEs
Activity resources from EU subsidy	**Budget: €1 888 950**	**FTE[14]: 15**

14 Target FTEs.

ACTIVITY 5:
Provide effective operational cooperation through situational awareness

Overview of activity

This activity contributes to cooperative preparedness and responses at the level of the Union and Member States through data-driven threat analysis, operational and strategic recommendations based on collections of incidents, and vulnerability and threat information to contribute to the Union's common situational awareness.

ENISA delivers on this activity by collecting and analysing security events, cyber incidents, vulnerabilities and threats based on its own monitoring, information shared by external stakeholders due to legal obligations[15] or voluntarily, by aggregating and analysing reports, ensuring information flow between the CSIRTs Network, EU-CyCLONe, and other technical, operational and political decision-makers at Union level and including cooperation finalised to increase situational awareness with other Union entities services such as relevant Commission services and in particular DG CNECT, CERT-EU, Europol/EC3, and EEAS including European Union Intelligence and Situation Centre (INTCEN) This activity benefits from ENISA's Cyber Partnership Programme managed under Activity 4 and the Agency's international cooperation frameworks.

Moreover, this activity includes the preparation of the regular in-depth EU Cybersecurity Technical Situation Report in accordance with CSA art.7(6), also known as the EU Joint Cyber Assessment Report (EU-JCAR), regular weekly OSINT reports, joint reports together with CERT-EU and other ad-hoc reports as needed. Under this activity the Agency prepares threat landscapes and provides topic-specific as well as general assessments on the expected societal, legal, economic, technological and regulatory impact, with targeted recommendations for Member States and Union institutions, bodies, offices and agencies. Under this activity, a semi-annual report in accordance with NIS2 Art.23(9) is prepared and the work related to the Cyber Solidarity Act – Incident Review Mechanism (Art.21) is undertaken.

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

The work on the EUVD and CRA Single Reporting platform is complemented through the delivery of vulnerability services for EU stakeholders. This activity manages participation in the Common Vulnerabilities and Exposures (CVE) Programme, namely the work related to the CVE Root and participation in CVE governance structures.

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

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

15 NIS2, CRA and Regulation (EU) 2023/2841.

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

The budget of this activity is partially financed through a contribution agreement between ENISA and the Commission to support the work on the CRA and CSOA as well as contributions to the Commission's Situation and Analysis Centre.

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

The full list of statutory tasks that the activity undertakes arising from EU legislation is presented in annex 15.

Link to strategic objectives (ENISA STRATEGY)

- Empowered communities in an involved and engaged cyber ecosystem
- Effective Union preparedness and response to cyber incidents, threats and crises
- Consolidated and shared cybersecurity information and knowledge support for Europe

Indicator for strategic objectives

EU Vulnerability Database is operationalised by ENISA and a satisfaction rate (by MSs and stakeholders) with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats
Reporting platform under CRA is established within 21 months of the entry into force of the Regulation and successfully operated

ACTIVITY 5 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
5.1. Build a common situational awareness between Member States based on shared accurate data and underpinned by validated joint analysis	CSA Art.7 NIS2 Art.23(9) CSOA Art.21	2025 to end of 2027	EU MSs contribute to and validate EU JCAR.	Cyber Security Assessment Tool (CSAT) for Joint Cyber Assessment Report (JCAR) >4 75% of EU MSs contribute to JCAR
			ENISA knowledge base is open to Member States and the leverage of information provided by EU MSs	Knowledge base is used by 40% of EU MSs.
				Feedback provided by EU MSs pertaining to missing or inaccurate entries is less than 10% of the total of incidents taken into account.
			Establish and test processes and procedures for the Incident Review Mechanism under Art.21 of CSOA	Process for Interoperable EU Risk Management (IRM) is endorsed by EU MSs by Feb 2026 CSAT on IRM report is > 4
5.2. Regularly provide general as well as specific threat landscapes and threat analysis, based on observed and data-driven trends in incidents and vulnerabilities	CSA Arts.7 and 9 NIS2 Art.23(9) CSOA Art.21 CRA Arts.14-17	2025 - 2027	Publish ENISA Threat Landscapes	Publish an annual Threat Landscape CSAT on ETL is >4 from selected communities
			JCAR includes threat analysis based on incidents and vulnerabilities available within ENISA data repositories (EUVD, Cybersecurity Incident Reporting and Analysis System (CIRAS), CRA SRP)	Incident analysis is included in JCAR as of Q4 2025.
				CRA SRP, Adversarial Exposure Validation, (AEV) and Incidents analysis is included by Q4 2026
			Ability of ENISA to publish accurate threat analyses based on incidents, vulnerabilities and on the Agency's own monitoring, shared by external stakeholders voluntarily or due to legal obligations[16]	80% of recipients score quality of threat analysis provided by ENISA above 4 (1-5)
				80% of recipients score ability of ENISA to use information available to produce threat analyses and recommendations above 4 (1-5)
			CRA SRP is established and operational	CRA SRP is used to carry on tasks under CRA by Q4 2026

16 - NIS2, CRA and Regulation 2023/2841.

ACTIVITY 5 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
5.1. Collect, organise and consolidate information (including for the general public) on common cyber situational awareness, threat analysis, technical situational reports, incident reports and support consolidation as well as exchange of information on strategic, operational and technical levels[17]	Establishment of a Threat Information Management Platform Publication of situational awareness and threat analysis reports, production of briefings and summaries of incidents and vulnerabilities Increased understanding and timely access to information regarding latest threats, incidents and vulnerabilities	CSIRT Network, EU CyCLONe, Union entities, National Authorities within MSs subscribed to the reports	Overall stakeholder satisfaction	Biennial (survey)	84%	85%
			Timeliness and Accuracy of reports	Biannual (survey)	84,2%	85%
5.2. Provide analysis and risk assessment (such as JCAR and ETL) jointly with other operational partners including Union Entities, Member States, industry partners, and non-EU partners	Union joint reports and briefings, sectorial analysis, threat analysis[18] Recipients receive accurate and timely assessment of threats faced by the EU Internal Market	CSIRT Network, EU CyCLONe, Union entities, HWPCI, Management Board	Stakeholder satisfaction	Biennial (survey)	84,2%	85%
			Number of contributing EU MSs to EU JCAR	Annual (report)	10	15
5.3. Collect and analyse information to report on the cyber threat landscapes	Mapping threats Generate recommendations for stakeholders to take up	NLO, CSIRTs Network / CyCLONe ISACs Advisory Group	Overall stakeholder satisfaction	Biennial (survey)	91.5%	90%
			Number of downloads of ETL	Annual (report)		+10%
5.4. Analyse and report on incidents as required by Art.5(6) of CSA as well as other sectorial legislations (e.g. DORA, eIDAS Art.10, etc.)	Analysis of incidents Generate recommendations for stakeholders to take up	Workstream 3 the NISD CG, CSIRT Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>91%
5.5. Establish the CRA Single Reporting Platform and operationalise the EU Vulnerability Database (EUVD) Services	CRA SRP platform work is scoped and implementation is initiated Operational and business processes are defined together with primary stakeholder	CSIRT Network	Operational processes expected for 2025 are defined CRA Platform is operational EU vulnerability database	Biennial (survey)	N/A	by 11 Sept 2026 Key enhancement validated by stakeholders

17 Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.
18 Including JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and CNECT Situation Centre.

Stakeholders and engagement levels

Partners: EU Member States (including CSIRTs Network members, EU-CyCLONe and NIS Cooperation Group), EU Entities, Other technical and operational blueprint actors, partnership programme for 5.3 (with trusted vendors, suppliers and partners), CTL AHWG

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

ACTIVITY 5 RESOURCE FORECAST

	Budget	FTEs
Activity resources from EU subsidy	**Budget: €1 274 000**	**FTE[19]: 13**
Other supplementary contributions	**Budget planned for 2026: €263 806 (outputs 5.1 and 5.2) SitCen Budget, €5 754 460 (output 5.5) to implement CRA SRP tasks + €100 000 CRA preparatory work** **Total contribution Budget: €447 973 (outputs 5.1 and 5.2) for SitCen Budget €11 947 620 (output 5.5) to implement CRA SRP tasks[20] + €400 000 prep work for CRA SRP[21]**	**FTE: 7[22]**

19 Target FTEs.

20 Please refer to annex 11 for further details regarding contribution agreements. The amount indicated refers to years 2026 to 2027.

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

22 Additional FTE financed via contribution agreements (SitCen and CRA SRP). Please refer to annex 11 for further details regarding contribution agreements.

ACTIVITY 6:
Provide services for operational assistance and support

Overview of activity

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

This activity also implements Cybersecurity Support Action, through which the Agency provides services such as pentesting, threat hunting, risk monitoring and assessment, customised exercises and training sessions, and supports Member States with incident response. Following the establishment of the Reserve, the Cybersecurity Support Action will be phased out in 2026, with service delivery expected to end in all MSs by the end of Q2.

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

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

In addition to the activities mentioned above, ENISA will, in collaboration with CERT-EU, work towards operationalising a virtual CISO (vCISO) service to provide advisory services to three agencies conducting risk assessment, or full risk assessment services depending on the case.

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

The full list of statutory tasks that the activity undertakes arising from EU legislation is presented in annex 15.

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

ACTIVITY 6 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
Deliver and complete ENISA's Cybersecurity Support Action by the end of Q2 2026	CSA Arts.6 and 7	Q2 2026	Ability of ENISA to support EU Member States to further develop preparedness and response capabilities through implementation and delivery of ex-ante and ex-post services (survey) Complete tasks on time and in budget (survey)	4 (1 to 5 score)
By the end of Q2 2026 and thereafter, deploy the European Cyber Reserve under CSOA.	CSA Arts.6 and 7	Q2 2026	Reaching consensus on actions and their prioritisation with the EC on the European Cyber Reserve. (survey) Timely deliver. (survey)	4 (1 to 5 score)

ACTIVITY 6 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
6.1. EU Cybersecurity Reserve	Operationalisation of the Reserve and delivery of incident response services to the users of the Reserve, with the possibility of conversion of pre-committed services to incident preparedness and response services	MSs CNECT CERT-EU	Percentage of MSs for which the Reserve is operational Satisfaction score	Annual (survey)	N/A	90% of MSs 4 (1 to 5 score)
6.2. Cybersecurity Support Action	Delivery of ex-ante and ex-post services until completion of the programme	MSs CNECT Beneficiaries	Percentage of MSs receiving service under Support Action Satisfaction score		N/A	80% of MSs 4 (1 to 5 score)

Stakeholders and engagement levels

Partners: EU Member States, Selected Beneficiary Entities, Commission, Union Entities, CERT EU

Involve / Engage: EU-CyCLONe, CSIRT Network, DG CONNECT, NIS Cooperation Group (CG), private sector providers[23]

23 ENISA cybersecurity support action services.

ACTIVITY 6 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: N/A**	**FTEs: 4**
Other supplementary contributions	**This activity is funded by contribution agreements between ENISA and the Commission. The figures below reflect the direct costs related to the implementation of the contribution agreements[24].** **Budget planned for 2026:** • **€4 562 434 contribution agreement signed in 2023[25]** • **€380 977 contribution agreement signed 2024** • **€10 835 869 contribution agreement signed in 2025**	**5 FTEs financed from the Contribution Agreement signed in 2023 and 3 FTEs financed from the Contribution Agreement signed in 2025**

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

25 Please refer to annex 11 for further details regarding contribution agreements.

ACTIVITY 7:
Development and maintenance of EU cybersecurity certification framework

Overview of activity

In line with the political priorities of the new EC established in 2024, the development, maintenance and promotion of the EU cybersecurity certification framework is crucial given its impact on promoting the EU cybersecurity digital market and overall resilience. The work on certification expands not only in developing new candidate certification schemes but, as of 2025, EUCC and other schemes will be in force. These too will require the maintenance, promotion and support of National Cybersecurity Certification Authorities (NCCAs) with capacity building and uptake initiatives. It is essential therefore to ensure that this activity is adequately resourced to cater for the additional streams of work.

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

ENISA has developed one candidate scheme, based on an EC request from 2019, in accordance with Art.49.2, which was adopted as an Implementing Regulation, the EUCC. ENISA is currently developing four other candidate schemes also based on EC requests, the EU Cloud Certification Scheme (EUCS), the EU Managed Security Services (EUMSS), the EU Digital Wallet (EUDIW) and the EU Certification Scheme for 5G Networks (EU5G), in accordance with Art.49.2. The URWP was adopted in February 2024, and the most recent request received for the development of an EUDI wallet candidate scheme is in line with Art.49.1. The request for an EU scheme on MSs is in line with Art.48.2, as foreseen by the URWP and the amendment to the CSA, based on a feasibility study by ENISA. ENISA also explores feasibility studies on other topics listed in the URWP but for which no candidate scheme request is formally issued in order to facilitate the delivery of the candidate schemes once the request has been received.

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

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

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

The full list of statutory tasks that this activity undertakes as required by EU legislation is presented in annex 15.

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

Number of EU certification schemes developed and maintained, number of EU regulations making reference to CSA, number of active Member States' NCCAs (e.g. issuing European certificates)

ACTIVITY 7 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe of objective	Indicator	Target
Between 2025-2027, timely development of feasibility studies for future potential schemas	CSA Art.49	2027	Number of feasibility studies concluded in view of upcoming requests	Three (pending potential new requests for scheme)
			Elements of feasibility study reflected or aligned in EC request for new schemes	More than 50%
Between 2025-2027, timely finalisation of candidate schemes following formal requests for drafting new cybersecurity certification schemes	CSA Art.49	2027	Number of drafts of certification schemes delivered to COM (ID Wallet Certification and Managed Security Services	2
			ECCG endorsement of draft certification schemes	Positive ECCG endorsement
			SCCG satisfaction on draft certification schemes (satisfaction survey)	More than 60%
Ensure the maintenance of existing schemes and support their roll-out	CSA Art.49	2027	Number of schemes maintained with ENISA active involvement	1 (EUCC)
			Satisfaction by ECCG with ENISA's supporting efforts for documents for maintenance	75%
			Number of certificates issued and published under an EU certification scheme; high usage rate in the market.	Proportionate[26] number of certificates issued migrating to a new EUCC scheme compared to a previous framework

26 ENISA monitors the certificates issued under SOG-IS and the transition to EUCC will have to be proportional to the number of certificates issued.

ACTIVITY 7 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
7.1. Drafting and contributing to the preparation (via feasibility studies *inter alia*) and establishment of candidate cybersecurity certification schemes[27]	Scheme meets stakeholder requirements, notably those 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 hoc Working Groups actively involved	Ad hoc working groups on certification ECCG European Commission	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			Number of opinions of stakeholders managed	Annual (report)	27 MSs and the Commission delivered through ECCG	5% increase compared to latest results
			Number of people or organisations engaged in the preparation of certification schemes	Annual (report)	EUCS scheme: 17 EU5G: 25 EUDI Wallet: 25 MSs: 15	5% increase compared to latest results
7.2. Implementing and maintaining the established schemes including evaluating adopted schemes, reviewing and updating state-of-the-art documents, etc., monitoring the dependencies and vulnerabilities of ICT products and services	Review of schemes to improve efficiency and effectiveness Take up of schemes by stakeholders	ECCG European Commission	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			ECCG satisfaction with ENISA's efforts on schemes adopted	Triennial (survey)	N/A	5% increase compared to latest results
7.3. Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks; supporting peer reviews and capacity building of NCCAs		ECCG European Commission SCCG NCCAs	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			Feedback from statutory bodies including NCCAs on ENISA's role	Annual (survey)	72%	5% increase compared to latest results
			Satisfaction with ENISA's role in NCCA peer reviews	Triennial (survey)	n/a	5% increase compared to latest results
7.4. Developing and maintaining necessary provisions, tools and services concerning the Union's cybersecurity certification framework (including certification website, supporting the Commission in relation to the core stakeholders service platform of CEF (Connecting Europe Facility) for collaboration, and the publication and promotion of the implementation of the cybersecurity certification framework, etc.)	Supporting with transparency and trust ICT products, services and processes Stakeholders engagement and promotion of certification	ECCG European Commission SCCG	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			Users' satisfaction concerning the certification services on the website	Annual (survey)	N/A	5% increase compared to latest results
			Usage of certification website	Annual (report)	N/A	75%
7.5. Promoting and monitoring the uptake of certification and the interplay with other legislative files (e.g. CRA, AI Act, etc.)	Increase in uptake of certification Increase in NCCAs maturity	ECCG European Commission NCCAs	Composite indicator on number of issued certificates and their use	Annual (survey)	N/A	TBD
			Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results

27 Notably on the EU Digital Identification Wallets (EUDIW) and Managed Security Services (MSS).

Stakeholders and engagement levels

Partners: EU Member States (including National Cybersecurity Certification Authorities, ECCG, European Commission, Union institutions, bodies, offices and agencies

Selected stakeholders as represented in the SCCG

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

ACTIVITY 7 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: € 631 610**	**FTE[28]: 10**

28 Target FTEs.

ACTIVITY 8:
Supporting market, technology and product-security

Overview of activity

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

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

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

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

Finally, this activity supports the assessment of the conformity of products with digital elements to EU standards, as well as their cybersecurity certification, by monitoring the cybersecurity standards being used by European digital products and certification schemes respectively, and by recommending appropriate technical specifications where such standards are not available or deficient.

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

The full list of statutory tasks that the activity undertakes based on EU legislation is presented in annex 15.

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

Rate of satisfaction with ENISA's support to the implementation of the CRA Market Supervisory Authorities (MSAs) and the European cybersecurity certification framework (ECCG)

Amount of advice and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC

ACTIVITY 8 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
Implement a 'market' monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, reports on the trustworthiness of products with digital elements under the CRA, including important critical products	CSA Arts.8, 52, 59 and 60	End of 2026	Timeliness of ENISA reports	Reports delivered on time
			Acceptance of ENISA reports by MSs	2/3rds of MSs endorsing ENISA reports
			Validity of ENISA framework	2/3rds of MSs validating and endorsing the ENISA framework
Provide continuous comprehensive support to market surveillance by MSs and notify authorities and the COM as well as manufacturers including SMEs that they should implement CRA requirements	CRA Arts.29, 52, 59 and 60	2026	MSs and COM stakeholder satisfaction survey	More than 70%
Create a technology and innovation radar to understand the level of impact that new technologies have on cybersecurity	CSA Arts.9 and 11	2026	Number of cybersecurity trends and patterns accurately identified through an evidence-based methodological approach	5% increase over reference data
			Impact of assessment EU cybersecurity R&I	5% increase over reference data

ACTIVITY 8 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
8.1. Collect and analyse information on new and emerging information and communications technologies (notably AI and PQC), support the COM and MSs with appropriate technical guidelines as necessary, and provide strategic advice to ECCC on the EU agenda on cybersecurity research, innovation and deployment	Identifying current and emerging ICT gaps, trends, opportunities and threats and providing guidelines on them Advising EU funding programmes including the ECCC and its Strategic Agenda and Action Plan.	Academia, Industry and National R&I bodies, MSs' market authorities (including NCCs) and Union Entities NIS CG, EC including CNECT and JRC, ECCC and NCCs, as appropriate	Stakeholder satisfaction	Biennial (survey)	91%	5% increase over reference data
			Findings endorsed by MSs (NCCs and market authorities)	Annual (survey)	N/A	5% increase over reference data
			Guidelines issued and endorsed by NIS CG	as relevant	N/A	5% increase over reference data
			ECCC Strategic Agenda and Action Plan alignment	Annual (survey with ECCC GB)	N/A	5% increase over reference data
8.2. Market analyses on the main trends in the cybersecurity market on both the demand and supply sides, and prepare the framework for the biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements[29]	Improved understanding of the market and industry Framework for the ENISA biennial technical report under the CRA	Cybersecurity market analysis by ad hoc working groups Advisory Group NLO (as necessary) MSs' Market surveillance authorities (as necessary)	Stakeholder satisfaction	Biennial (survey)	88%	5% increase over reference data
			Cybersecurity market analysis; cybersecurity products and services	Annual (framework and reports) (survey)	N/A	5% increase over reference data
			Endorsement by MSs of report on emerging trends regarding cybersecurity risks in products with digital elements	Biennial (report)	N/A	5% increase over reference data
8.3. Support for the implementation of the CRA, including assessment of standards, technical guidance and the activities of market surveillance authorities as well as the identification of categories of products for simultaneous coordinated control actions and, upon request, conducting evaluations of products that present a significant cybersecurity risk.	Assessment of 41 vertical and horizontal standards (CRA standardisation request) Monitoring and following-up on requirements of market surveillance authorities Identify categories of products; produce a methodology for market surveillance and product testing, including in view of market sweeps; carry out market sweeps Technical recommendations on conformity assessment, including in view of notification of CABs under the CRA Technical guidance for the security-by-design and security-by-default principles including for SMEs Evaluations to be carried out ideally on the basis of input from market sweeps; rely on external expertise.	MSs' Market Surveillance Authorities NLOs Commission MSs Notifying authorities CRA Expert group	Collection of requirements Matching requirements with deliverables Time to carry out market sweeps Methodology for evaluations Profiles of experts	Assessment of standards on continuous basis starting in 2025 Security-by-design and security-by-default technical guidelines (reports, checklists) to be issued in 2026 and updated on a continuous basis ENISA SME strategy for the CRA in 2026 and updated on a continuous basis Technical support and recommendations on conformity assessment to be issued in 2026 and updated on a continuous basis	N/A	5% increase over reference data

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

				Market sweeps as of 2027 (3-years transition) or earlier if requested Method to evaluate products in 2026, to be updated regularly Guidance and criteria to accept evaluation results in 2026 to be updated on regular basis		
8.4. Monitoring developments in related areas of standardisation, analysis of standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification	Monitoring of cybersecurity standardisation activities Input to the EU standardisation agenda	CEN/CENELEC/ETSI European Commission Ad hoc working groups (as necessary) Advisory Group NLO (as necessary)	Stakeholder satisfaction	Biennial (survey)	88%	5% increase over reference data
			Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification.	Annual (report)	N/A	5% increase over reference data
8.5. Supporting the implementation of eIDAS2 Regulation and the deployment and uptake of European Digital Identity Wallets	Best practices and guidelines to support implementation of eIDAS2 Monitoring of the uptake of Digital Wallets	European Digital Identity Cooperation Network EC	Stakeholder satisfaction	Annual (survey)		5% increase over reference data

Stakeholders and engagement levels

Partners: EU Member States (including market surveillance authorities and entities with an interest in cybersecurity market monitoring e.g. NCCA, National Standardisation Organisations, European Commission, Union institutions, bodies, offices and agencies, European Standardisation Organisations (CEN, CENELEC, ETSI), private sector or ad hoc standards setting organisations, EC Joint research centre, National and EU R&I entities, academia and industry, European Cybersecurity Competence Centre and National Cybersecurity Coordination Centres, EC AI Office, European Digital Identity Cooperation Group, European Data Innovation Board

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

ACTIVITY 8 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: € 578 200**	**FTE: 10**

3. CORPORATE ACTIVITIES

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

ACTIVITY 9: Performance and sustainability

Overview of activity

This activity seeks to achieve requirements under 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**, its methods of operation and its **diligence in carrying out its tasks'**. This objective requires inter alia an efficient performance and risk management framework and the development of individual administrative practices as well as the promotion of sustainability across all the Agency's operations. In addition, and in line with Art.4(2) of the CSA, this activity includes contributing to efficiency gains, e.g. via shared services in the EU Agencies network by relying on the Agency's own expertise (e.g. cybersecurity risk management).

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

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

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

ACTIVITY 9 ANNUAL OBJECTIVES

Description	Link To Corporate Objectives	Activity Indicators	Frequency (Data Source)	Latest Result	Target
9.A Enhance corporate performance and strategic planning	Ensure efficient corporate services	Proportion of SPD KPIs meeting targets	Annual	73%	>80% of indicators outperformed
	Continuous innovation and service excellence	Results of Internal control framework assessment	Annual	Effective (Level 2)	Effective level 1 or 2
	Developing service propositions with additional external resourcing	High satisfaction with essential corporate services in the area of compliance and coordination	Annual	75%	>60%
9.B. Increase corporate sustainability	Ensure ENISA is climate neutral by 2030	Maintain EU Eco-Management and Audit Scheme (EMAS)	Annual	EMAS audit conducted on 27/2/25	Timely implementation of follow up actions to ensure EMAS certification is maintained
	Develop efficient framework for ENISA's continuous governance to safeguard high level of IT	Agency IT strategy aligned with corporate strategy Proportion of total IT budget allocated to information security proportional to the level of risks identified across IT systems within Agency	Annual	Revised IT strategy proposal submitted end 2024; strategy to be adopted by Q2 2025 18% of total IT costs	70% implementation (ITMC reporting) 20%

ACTIVITY 9 OUTPUTS

Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2026
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; under ITMC Streamlined budget management across the Agency; under BMC Maintenance of EMAS Certificate	MT, ITMC & BMC External and internal audits Statutory bodies	Number of high risks identified in annual risk assessment	Annual (survey, internal reports)	3	<3 30% reduction in high risks identified in previous year
			Effective monitoring of high risks and critical recommendations to follow up on timely implementation of mitigation measures by business owners		N/A	Risk plans are generated in a timely manner, agreed with risk owners and reported to MT (on a quarterly basis at least)
			Percentage of identified deficiencies in internal controls addressed within timelines		No critical recommendation issued in 2023 ICF assessment. Out of 3 moderate and 2 major – the recommendations remain valid as the deficiencies have not been fully mitigated	100% for critical, 80% for major, 60% for moderate
			Timely follow-up and resolution of internal and external audits (in particular from IAS and ECA) recommendations and findings			<180 days
			Number of identified regulatory breaches		3	0 for critical/ major, <=3 for moderate
			Percentage of revised and up to date corporate rules (MBD, EDD, policies, processes)		23 MBDs on corporate rules from before 2019	60% corporate rules which have not been reviewed less than three years ago; 80% corporate rules which have not been reviewed less than four years ago
			Annual report on ARES maintenance and actions		N/A	Follow up of maintenance and actions
			Reduction of CO2 emissions in ENISA HQ		N/A	Timely submission of report with actions and recommendations
			Efficiency and effectiveness of ITMC & BMC (survey)		TMC: 75% BMC: 63%	> 60%

9.2. Maintain and enhance ENISA's cybersecurity posture in line with the Agency's multiannual cybersecurity maturity plan (2026 – 2028)	Compliance with Regulation (EU) 2023/2841 on a high common level of cybersecurity within Union entities Timely identification and response to cybersecurity risks Continuous monitoring of cybersecurity of IT systems and timely identification of issues and areas for improvement (first level and second level controls) Coordination and implementation of the cybersecurity maturity plan of the Agency for 2026	MT and relevant committees Statutory bodies Interinstitution-al Cybersecurity Board (IICB) External and internal audits	Percentage of identified high risk mitigation measures addressed within timelines	Annual	All high risks addressed within timelines and/ or accordingly reported and planned	>90%
			Annual risk assessment (RA) and risk treatment plan with the relevant business owners	Annual	N/A	RA and risk treatment plans conducted timely and in line with Regulation (EU) 2023/2841
			Cybersecurity measures implemented according to maturity plan and for set timelines	Annual	N/A	Measures and timelines in accordance with the cybersecuri-ty masterplan
			Address all potential cybersecurity incidents	Annual	N/A	All cybersecurity incidents addressed in a timely way
			Cybersecurity training for staff and managers	Annual	Two training sessions by ISO; training programme and phishing exercise (via dedicated training platform)	>2 training sessions by ISO
9.3. Provide support services to the EU Agencies network and in key areas of the Agency's expertise	Shared services in the area of data protection, legal services and accounting EUAN troika shared services pilot	MT, BMC EUAN (Agencies receiving ENISA's support)	Satisfaction within the EU Agency network with ENISA support services	Annual	High satisfaction expressed by the agencies that received ENISA's services	70% satisfaction for the services offered under the EUAN Shared Services Pilot (survey)
9.4. Ensure the implementation of single administration processes across the Agency	Streamlined document management practices	MT Staff committee	Percentage of staff considering that the information they need to do their job is easily available or accessible within ENISA	Annual (survey)	66% of staff survey respondents agree that ENISA's internal communication is timely and clear (last year's survey showed 39%)	50%
			Response timeliness to external parties (internal reporting)	Annual	High response rates in accordance with ENISA's code of conduct	High response rates in accordance with ENISA's code of conduct

Stakeholders and engagement levels

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

ACTIVITY 9 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	**Budget: €432 000**	**FTE: 15[30]**
Other supplementary contributions	**Budget: €54 604 SLA with ECCC, see annex 11 for additional information** **Budget: €1 269 100[31]**	**FTE: N/A**

30 Target FTEs Including ED, COO, ACOO and accounting officer.

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

ACTIVITY 10:
Reputation and Trust

Overview of activity

This activity seeks to meet the 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, its methods of operation, and its diligence in carrying out its tasks'. This objective requires that a transparent and proactive approach be taken to maximise the quality and value provided to stakeholders. It also includes contributions to efficiency gains by optimising the way it engages with stakeholders and, to increase the Agency's outreach, offering on-demand services in addition to the essential services it provides.

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

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

ACTIVITY 10 ANNUAL OBJECTIVES

Description	Link to corporate objectives	Activity indicators	Frequency (Data source)	Latest result	Target
10a. Protect and grow the Agency's brand	Ensure efficient corporate services	Level of trust in ENISA (as per Biannual Stakeholder Survey)	Biennial	95%	95%
10b. Improve the outreach of ENISA's mandate	Ensure efficient corporate services				
		Stakeholder satisfaction with ENISA events	Annual (Survey)	88%	>80%
		Number of unique website visitors	Annual	N/A	>5% increase year on year

ACTIVITY 10 OUTPUTS

Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2026
10.1. Review and implement the multiannual communications strategy and support stakeholders' strategy including corporate outreach	Enhanced transparency and outreach Engaged communities Increased impact of ENISA activities Relevant and easily accessible information is provided to stakeholders	Management Team and Agency stakeholders	Number of social media engagements	Annual (Media monitoring)	66.3k	68k
			Stakeholder satisfaction with ENISA outreach	Biennial (survey)	96%	>80%
			Number of total ENISA website visits	Annual (website analytics)	2.3 million	1.5 million[32]
10.2. Implement internal communications strategy	Engaged staff	Management Team and staff committee	Staff satisfaction with ENISA internal communications	Annual (survey)	65%	>70%
10.3. Manage and provide the secretariat for statutory bodies, i.e. EB, MB, AG, NLO (excluding certification)	Support the operation and organisation of ENISA statutory bodies Support effectiveness of implementation of work programmes (validation of operational outputs) Provide administrative support for the day-to-day working of the Management board's decisions and recommendations from NLO & AG	Statutory bodies, Management Team and Committees	Number of times feedback is received per NLO consultation	Annual (Internal report)	27 for NLO subgroups (3.6 is average for validations in NLO Network	>6
			Number of times feedback is received per AG consultation	Annual (Internal report)	11.3 on average	>8
			Satisfaction of statutory bodies with ENISA's support to fulfil their tasks as described in CSA	Annual (survey)	97%	>80%

Stakeholders and engagement levels

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

Involve / Engage: All ENISA stakeholders

ACTIVITY 10 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	**Budget: €1 270 815**[33]	**FTE :7.5**[34]

32 New website and analytics have impacted measurement.

33 Including the budget centralised for operational missions and large-scale events.

34 Target FTEs.

ACTIVITY 11:
Effective and efficient corporate services

Overview of activity

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

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

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

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

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

ACTIVITY 11 ANNUAL OBJECTIVES

Description	Link to corporate objectives	Activity indicators	Frequency (Data source)	Latest result	Target
11a. Enhance people-centric services by implementing the Corporate and HR strategy	Effective workforce planning and management Efficient talent acquisition, development and retention Caring and inclusive modern organisation	Implementation of Strategic Workforce Planning and Review decisions	Annual	Fully implemented	Fully implemented
		Implementation of the Corporate and HR strategies		Vacated staff posts in 2024 were fulfilled within 143 days. The indicated KPI was to fulfil posts within 300 days	Proposal new KPI: Vacated post are fulfilled within 200 days Provide updates on new and revisions of: Policies introduced Policies updated Related MB decisions Related ED decisions
		High participation in staff satisfaction survey		80%	75% participation rate

11b. Ensure sustainable and efficient corporate solutions and promote continuous improvement	Ensure efficient corporate services Introduce digital solutions that maximise synergies and collaboration within the Agency Developing service propositions with additional external resourcing Promote and enhance ecologic sustainability across all the Agency's operations Develop efficient framework for ENISA's continuous governance to safeguard high level of IT and physical security	Implement best practices in sustainable IT solutions	Annual	Fully implemented according to plan	IT strategy updated accordingly
		Limited disruption of continuity of corporate services	Annual	Effective disaster recovery is in place to ensure business continuity of its core services.	On demand corporate IT facilities, financial and HR services in 2025
		Handling EUCI at the level of SECRET UE/EU SECRET	Annual	EU Classified Information (EUCI) inspection took place and the report will be sent in 2025.	Operational for the first full year in 2025

ACTIVITY 11 OUTPUTS

Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2026[46]
11.1. Manage and provide horizontal, recurrent, administrative services in the area of HR, Finance and Procurement for ENISA staff and partners	Services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently. Implementation of the Unit's annual plan in procurement, L&D and recruitment Set up Service Level Agreements in areas such as HR, Finance, Procurement and Contract Management Establish reporting capabilities in areas such as HR, Finance and Procurement (monthly Heads of Unit (HoUs), quarterly Introduce MS planner to all Corporate Support Services Unit (CSS) to capture workload indicators Introduce Service Now as main ticketing system across all CSS services Expand Service Catalogue to Paymaster Office (PMO) and DG HR Review ENISA CSS intranet page	Management Team IT Management Committee Budget Management Committee Staff Committee	Turnover rates	Annual (internal reports)	4.1%	<5%
			Posts in Establishment Plan filled		98%	>95%
			Percentage of the approved Recruitment plan that is implemented		94%	>90%
			Percentage of the approved Procurement Plan that is imple-mented		63.63%	>90%
			Percentage of the budget that is implemented		100%	>95%
			Average time for initiating a transaction Financial Initiating Agent (FIA) role		7.51%	<7 days
			Average time for verifying a transaction Financial Verification Agency (FVA) role)		0.19	<3 days

11.2. Implement the Agency's Corporate strategy, including HR strategy with emphasis on talent development, growth and welfare	Objectives and goals set out in the corporate and HR strategies are met Launch and evaluation of Staff Satisfaction Survey Implementation of the ED decision on annual workforce review [adopted in April 2024] Revision of following policies: 1/ Recruitment & External Mobility 2/ Staffing 3/ Wellbeing and Medical 4/ Probation 5/ MB Seconded National expert (SNE) rules 6/ Amendment of Financial Regulations 7/ Management of Indirect costs 8/ Reimbursement of Experts 9/ Physical Security and Access Control 10/ Incident Reporting and Facility Fault Response 11/ Evacuation and Preparedness (Priority 2025) 12/ Learning & development (L&D) policy 13/ Trainee policy 14/ Stand-by duty policy	Management Board Management Team Staff Committee EUAN Budget Management Committee (BMC)	Number of policies/ IR reviewed/ processes revised	Annual (internal report)	10	> 10
			Percentage of staff satisfaction with talent development		52%	>50%
			Percentage of actions implemented as follow up on results of staff satisfaction survey and implemented on time		N/A	>80%
			Number of competency-driven training and development activities implemented		<10	< 10
			Number of multisource feedback evaluations implemented and followed up		16	> 5
11.3. Manage and provide horizontal, recurrent support services in the area of facilities, security and corporate IT for ENISA staff and partners	Services such as corporate IT, facilities and security are performed efficiently with minimal disruption. Decommission data centre in Heraklion and programme manage new data centre Programme manage EC tools of budget & HRT transition Expand Service Now (Finance, Procurement, HR, Reporting) Improve Physical security services	Management Team IT Management Committee Budget Management Committee Staff Committee	Staff satisfaction with working environment	Annual	80%	>70%
			Time to respond to IT, safety and security incidents.		n/a	<3 days to respond
			Average time to respond to facilities management requests		2 days	<1 day to acknowledge and <3 days to respond
11.4. Enhance operational excellence and digitalisation through modern, safe, secure and streamlined ways of working and the introduction of self-service functionalities	Services such as access management, meeting room facilities, equipment renewal, cloud-based solutions and data availability are efficient.	Management Team IT Management Committee	Critical systems uptime/downtime	Annual	100%	99%
			Staff satisfaction with IT resolution		82.53%	85%

Stakeholders and engagement levels

Partners: ENISA staff members and EU Entities

Involve / Engage: Private Sector and International Organisations

ACTIVITY 11 RESOURCE FORECASTS

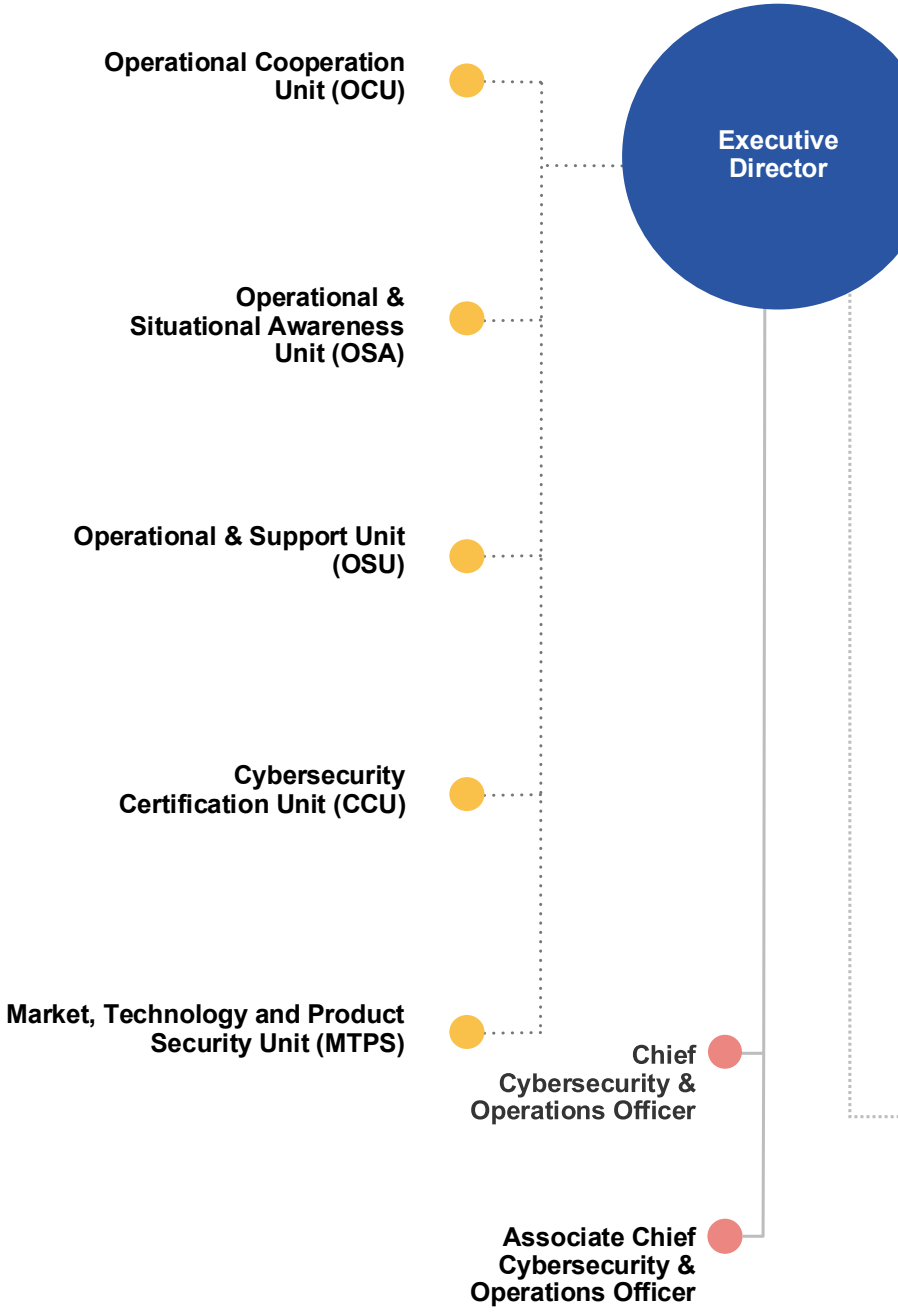
	Budget	FTEs
Total activity resources	**Budget: €4 495 624**[35]	**FTE : 21.5**[37]
Other supplementary agreements	**Budget: €320 900**[36]	

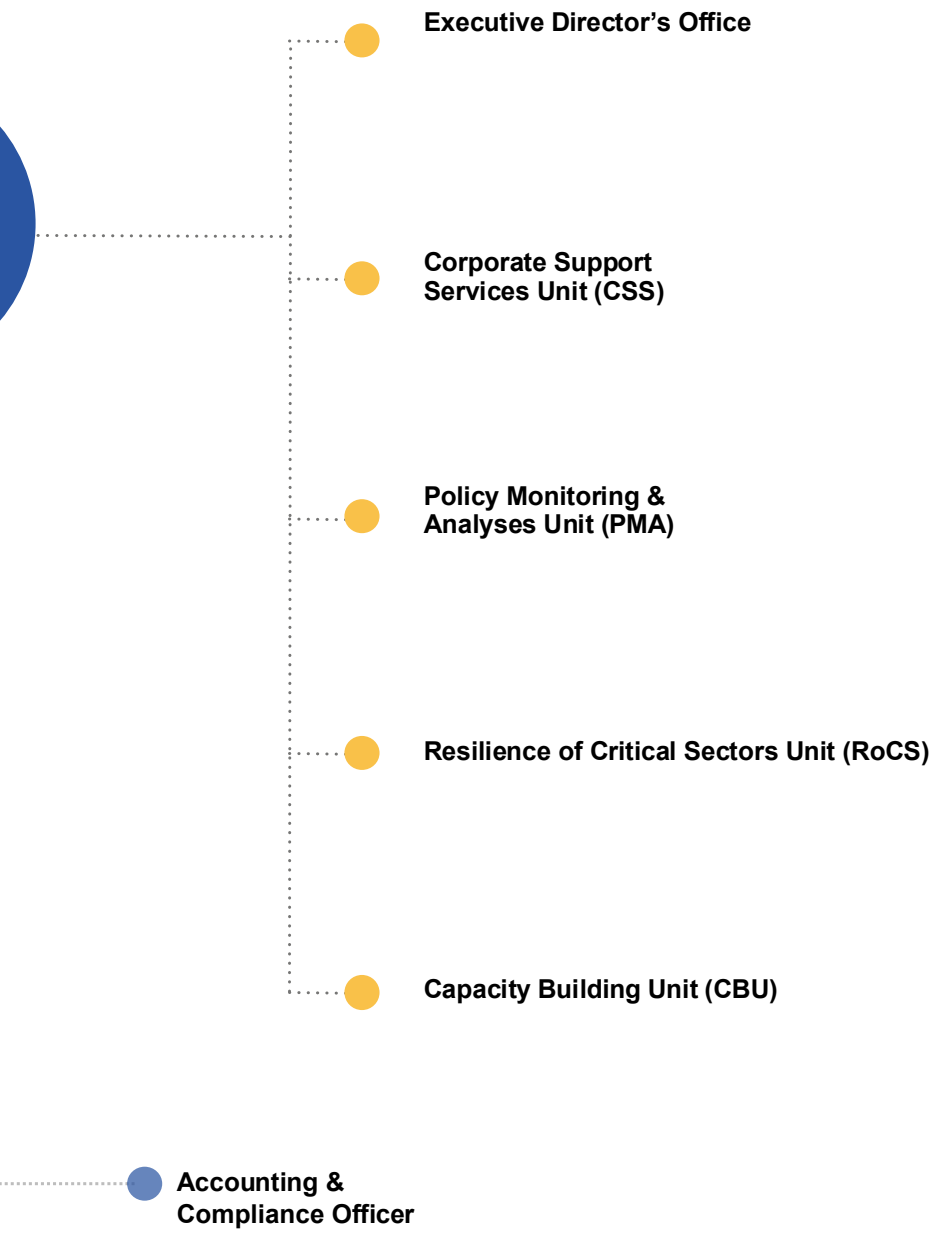
35 Excluding staff in active employment and recruitment expenditure including €414 500 from C1 for data centre migration.
36 Target FTEs.
37 Budget from contribution agreements forecasted for date centre migration; please see annex 11 for further information.

Annex A

ANNEX 1
ORGANISATION CHART AS OF 31.12.2025

Administrative organigramme




Executive Director's Office
Corporate Support Services Unit (CSS)
Policy Monitoring & Analyses Unit (PMA)
Resilience of Critical Sectors Unit (RoCS)
Capacity Building Unit (CBU)
Accounting & Compliance Officer

ANNEX 2
RESOURCE ALLOCATION PER ACTIVITY 2026–2028

The indicative allocation of the total 2026 financial and human resources following the activities as described in part 3.1 in Section III and the corporate activities as described in part 3.2 in Section III are presented in the table below. The allocation was done following the direct budget and FTEs indicated for each activity with the indirect budget being assigned based on causal relationships.

The following assumptions are used in the simplified Activity Based Budgeting (ABB) methodology:

- The budgets granted to ENISA through the Contribution Agreements signed in 2023, 2024 and 2025 are not included in the calculations as activities (as well as budgets) defined in these agreements run from 2024 to 2028.
- Additional FTEs granted to ENISA through the Contribution Agreements signed in 2023, 2024 and 2025 are not included in the calculations as their direct and indirect costs should be fully covered by the Contribution Agreement.
- Budget allocations to activities 1-8 include the Direct and Indirect budgets attributed to each activity, while activities 9-11 are calculated only on the Indirect budget attributed to these activities.
- The Direct Budget is the cost estimate of each of the 8 operational activities as indicated under Section 3.1 of the SPD 2026-2028 (carried out under Arts.5-12) in terms of goods and services to be procured.
- Budgets for operational missions and large-scale operational events are allocated to operational activities (Activities 1-8) based on the direct FTEs under each activity.
- The Indirect Budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs attributable to each activity based on the link of the activity to the budget line (as indicated in the Statement of Estimates). The indirect budget is allocated to activities based on different drivers. The main driver for costs allocation was the number of foreseen direct FTEs for each activity in 2026.
- In order to estimate the full costs of operational activities, corporate activities 9 to 11 should be distributed according to all operational activities based on their respective drivers.

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2026)	Activities as referred to in Section 3	Direct and Indirect budget allocation (in EUR)	FTE allocation
Support for policy monitoring and development	Activity 1	1 872 380	10
Cybersecurity and resilience of critical sectors *	Activity 2	2 323 002	12
Building capacity	Activity 3	2 468 042	12
Enabling operational cooperation	Activity 4	4 296 578	15
Provide effective operational cooperation through situational awareness *	Activity 5	3 360 610	13
Provide services for operational assistance and support *	Activity 6	642 034	4
Development and maintenance of EU cybersecurity certification framework	Activity 7	2 236 695	10
Supporting European cybersecurity market, research & development and industry	Activity 8	2 183 285	10
Performance and sustainability	Activity 9	2 530 892	15
Reputation and trust	Activity 10	1 470 149	7.5
Effective and efficient corporate services	Activity 11	3 807 135	21.5
TOTAL		**27 190 802**	**130**

* Activities 2, 5 and 6 are implementing activities agreed under the Contribution Agreements signed in 2023, 2024 and 2025 where additional budget were granted accordingly as well as additional FTEs for implementation of the agreed activities during 2024-2028. Further information can be found in Annex 11.

ANNEX 3
FINANCIAL RESOURCES 2026–2028

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

Revenue	2025 amended budget	VAR 2026 / 2025	Draft Estimated budget 2026	Envisaged 2027	Envisaged 2028
1. Revenue from fees and charges					
2. EU contribution	25 993 311	1,93%	26 495 438	26 720 032	27 236 032
– of which assigned revenues deriving from previous years' surpluses	150 299		155 877	250 000	250 000
3. Third countries contribution (incl. EEA/EFTA and candidate countries)	721 020	-3,56%	695 364	695 364	695 364
– of which EEA/EFTA (excl. Switzerland)**	721 020	-3,56%	695 364	695 364	695 364
– of which Candidate Countries					
4. Other contributions***	24 463 333	N/A	p.m.	p.m.	p.m.
5. Administrative operations – of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art.58)					
6. Revenues from services rendered against payment****	60 000	N/A	p.m.	p.m.	p.m.
7. Correction of budgetary imbalances					
TOTAL REVENUES	**51 237 664**	**-46,93%**	**27 190 802**	**27 415 396**	**27 931 396**

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

** For the purpose of calculating EFTA funds for 2026-2028, the average surplus of the previous 3 years (EUR 250 000) was used with 2.79% the EFTA proportionality factor in 2025.

*** Two new contribution agreements were signed in December 2024, for up to EUR 15 million (prefinancing 80%) and up to EUR 400 000 (prefinancing 60%) for which the first instalments were received in 2025, ie EUR 12 million for Support Action, SitCEN and CRA SRP. Another new contribution agreement was signed in August 2025 of which EUR 12.233 million was received for the EU cyber reserve and SitCEN. See annex 11.

**** Revenue foreseen from the existing SLAs signed with ECCC and EU-LISA. See Annex 11.

***** The budget estimates for 2028 throughout this document are for illustrative purposes only and do not forecast the next multiannual financial framework.

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

Expenditure (in EUR) * **	2025		2026	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	15 555 529	15 555 529	16 031 333	16 031 333
Title 2	4 159 348	4 159 348	4 290 159	4 290 159
Title 3	6 999 454	6 999 454	6 869 310	6 869 310
Total expenditure	**26 714 331**	**26 714 331**	**27 190 802**	**27 190 802**

Expenditure (in EUR)* **	Commitment and Payment appropriations * **					
	Adopted Budget 2024	Adopted Budget 2025	Draft estimated budget 2026	VAR 2026 / 2025	Envisaged in 2027	Envisaged in 2028
Title 1. Staff Expenditure	**14 809 106**	**15 555 529**	**16 031 333**	**3.1%**	**16 163 751**	**16 467 977**
11 Staff in active employment	13 058 316	1 3840 860	14 598 932	5.5%	14 719 518	14 996 562
12 Recruitment expenditure	517 889	508 469	217 593	-57.2%	219 391	223 520
13 Socio-medical services and training	824 501	688 200	626 808	-8.9%	631 985	643 880
14 Temporary assistance	408 400	518 000	588 000	13.5%	592 857	604 015
15 External services on HR matters	**N/A**	**N/A**			**0**	**0**
Title 2. Building, equipment and miscellaneous expenditure	**3 671 144**	**4 159 348**	**4 290 159**	**3.1%**	**4 325 596**	**4 407 010**
20 Building and associated costs	1 004 965	1 081 300	1 061 957	-1.8%	1 070 729	1 090 882
21 Movable property and associated costs (***)	0	0			0	0
22 Current corporate expenditure	516 125	687 000	336 858	-51.0%	339 640	346 033
23 Corporate ICT	2 150 054	2 391 048	2 891 344	20.9%	2 915 226	2 970 095
Title 3. Operational expenditure	**7 739 551**	**6 999 454**	**6 869 310**	**-1.9%**	**6 926 050**	**7 056 409**
30 Activities related to meetings and missions	402 780	1 536 000	1 290 415	-16.0%	1 301 074	1 325 562
36/37 Core operational activities	7 336 771	5 463 454	5 578 895	2.1%	5 624 976	5 730 847
TOTAL EXPENDITURE	**26 219 801**	**26 714 331**	**27 190 802**	**1.8%**	**27 415 396**	**27 931 396**

* - Does not include EUR 174 604 for possible revenue under SLAs with ECCC and EU-LISA, ref. Annex 11

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

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

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

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

In December 2024, two additional Contribution Agreements were signed, resulting in a total increase of EUR 15.4 million in funding. Of this amount, EUR 400 000 was allocated to a feasibility study on a single reporting platform under the Cyber Resilience Act while the agency was funded by EUR 15 million for the implementation of the 'Incident and Vulnerability Response Support and Reporting' action under the Digital Europe Programme (DEP).

In July 2025 ENISA received another EUR 36.67 million to finance the implementation of the EU Cybersecurity Reserve as well as the Cyber Situation and Analysis Centre.

Please refer to Annex 11 for details of all Contribution Agreements.

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

Budget outturn	2022	2023	2024
Revenue actually received (+)	39 227 392	25 293 935	42 473 035
Payments made (-)	-20 396 780	-21 11 392	
Carry-over of appropriations (-)	-18 836 095	-4 228 452	-16 945 798
Cancellation of appropriations carried over (+)	248 745	149 739	
Adjustment for carry-over of assigned revenue appropriations carried over (+)	33 743	53 469	163 909
Exchange rate difference (+/-)	-17 88	0	
Total	**276 988**	**150 299**	**155 877**

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

With steady budget increases over the last few years of up to EUR 26.2 million in 2024, a commitment rate of 100.00% (100.00% in 2023 and 99.93% in 2022) of appropriations for the year (C1 funds) at the year-end has been reached which shows the already proven capacity of the Agency to fully implement its annual appropriations.

In 2024 commitment appropriations were cancelled in an amount of EUR 1 080 representing 0.004% of the total budget.

The payment rate for the full budget of EUR 26.2 million reached 83.05% (in 2023 it was 83.86%, in 2022 for ENISA 'standard' budget it was 84.11%). The total amount carried forward to 2025 was EUR 4 442 833 or 16.95%.

No payment appropriations were cancelled during 2024.

The appropriations of 2023 carried over to 2024 were used at a rate of 96.19% (automatic carry-overs) which indicates a proven capability for estimating needs (in 2023 it was 99,20%). From the total amount of EUR 4 064 543 carried forward, the amount of EUR 154 797 was cancelled (or 3.81%). This cancellation represents 0.61% of the total committed appropriations in 2023 of EUR 25 182 935 (fund source C1).

ANNEX 4
HUMAN RESOURCES – QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2026 - 2028

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

Statutory staff and SNEs

Staff numbers	2024			2025	2026	2027	2028
ESTABLISHMENT PLAN POSTS	Authorised budget	Actually filled as of 31/12/2024	Occupancy rate %	Adopted	Envisaged staff	Envisaged staff	Envisaged staff
Administrators (ADM)	64	62	97%	64	65	65	65
Assistants (AST)	19	19	100%	19	18	18	18
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	83	81	98%	83	83	83	83
EXTERNAL STAFF	**FTE corresponding to the authorised budget 2024**	**Executed FTE as of 31/12/2024**	**Execution rate %**	**Envisaged FTE**	**Envisaged FTE**	**Envisaged FTE**	**Envisaged FTE**
Contract Agents (CA)[38]	32	28	88%	32	32	32	32
Contract Agents (stemming from contribution agreements)				+16* CA contribution agreement	+18* CA contribution agreement	+18* CA contribution agreement	
Seconded National Experts (SNE)	**15**	**11**	**73%**	**15**	**15**	**15**	**15**
TOTAL STAFF[39]	**130**	**120**	**92%**	**146**	**148**	**148**	**130**

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

Human Resources	2024	2025	2026	2027	2028
	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	12	16	18[40]*	18*	
Seconded National Experts (SNEs)	n/a	n/a	n/a	n/a	n/a
TOTAL	12	16*	18*	18*	

38 Article 38.2 of the ENISA Financial Rules allows the opportunity to 'offset the effects of part-time work'. ENISA will explore this option in 2025 and may use this option in the future to offset long-term absences and part-time work using short term contracts with CAs.

39 Refers to TAs, CAs and SNEs figures.

40 Please see annex 11 for additional information.

Other Human Resources

Structural service providers

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

Interim workers

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

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

Function group and grade	2024				2025		2026		2027		2028
	Authorised budget		Actually filled as of 31/12/2024		Authorised[41]		Envisaged		Envisaged[42]		Envis-aged
	Perm. Posts	Temp. posts	Perm. Posts	Temp posts	Perm. Posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts	Temp. posts
ADM 16											
ADM 15		1		1		1		1		1	1
ADM 14											
ADM 13		2		1		2		2		2	2
ADM 12		4		4		4		4		4	4
ADM 11		3		2		3		3		3	3
ADM 10		4		3		4		4		4	4
ADM 9		14		15		14		14		14	14
ADM 8		15		11		16[43]		16		16	16
ADM 7		13		12		13		14		14	14
ADM 6		7		13		7		7		7	7
ADM 5		1									
ADM TOTAL		64		62		64		65		65	65
AST 11											
AST 10											
AST 9		2		2		1		2		2	2
AST 8		1		1		3		2		2	2
AST 7		0		0		3		1		1	1
AST 6		9		7		6		7		7	7
AST 5		4		5		4		4		4	4
AST 4		2		2		2		2		2	2
AST 3		1		1							
AST 2				1							
AST 1											
AST TOTAL		19		19		19		18		18	18
AST/SC 6											
AST/SC 5											
AST/SC 4											
AST/SC 3											
AST/SC 2											
AST/SC 1											
AST/SC TOTAL											
TOTAL		83		81		83		83		83	83
GRAND TOTAL	83		81		83		83		83		83

41 Modification of 2025 establishment plan was pending in Q4 2025.

42 Envisaged reflects future reclassification exercises.

43 EU 2026 general budget has not yet been published.

External personnel

Contract Agents

Contract agents	FTEs corresponding to the authorised budget 2024	Executed FTEs as of 31/12/2024	FTEs corresponding to the authorised budget 2025	FTEs corresponding to the envisaged budget 2026	FTEs corresponding to the envisaged budget 2027	FTEs corresponding to the envisaged budget 2028
Function Group IV	30	21 + 12 contribution agreement	30 + 16 contribution agreement	30 + 18 contribution agreement	30 + 18 contribution agreement	30 + pm
Function Group III	2	6	2	2	2	2
Function Group II	0	0	0	0	0	0
Function Group I	0	1	0	0	0	0
TOTAL	32	40	48	50	50	32

Seconded National Experts

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

Table 3: Recruitment forecasts for 2026 following retirement or 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[44]	Internal (brackets)	External (brackets)	
Expert	1 TA	5 TAs 6 CAs (FG4 IV)	n/a	n/a	n/a
Officer	n/a	n/a	n/a	n/a	
Assistant	n/a	n/a	n/a	n/a	n/a

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

ANNEX 5
HUMAN RESOURCES – QUALITATIVE

A. RECRUITMENT POLICY

Implementing rules in place

		Yes	No	If no, which other implementing rules are in place?
Engagement of CAs	Model Decision C(2019)3016	x		
Engagement of TAs	Model Decision C(2015)1509	x		
Middle management	Model decision C(2018)2542	x		
Type of posts	Model Decision C(2018)8800		x	C(2013) 8979

B. APPRAISAL AND RECLASSIFICATION/PROMOTIONS

Implementing rules in place

		Yes	No	If no, which other implementing rules are in place?
Reclassification of TAs	Model Decision C(2015)9560	x		
Reclassification of CAs	Model Decision C(2015)9561	x		
Appraisal of TA	Model Decision C(2015)1513	x		
Appraisal of CA	Model Decision C(2015)1456	x		

Table 1: Reclassification of TA or promotion of official

		Average seniority in the grade among reclassified staff							
Grades		Year 2019	Year 2020	Year 2021	Year 2022	Year 2023	Year 2024	Actual average over 5 years	Average over 5 years (According to decision C(2015)9563)
ADM 05		-	-	-	-	-		-	2.8
ADM 06		3	-	1	1	1	2	3.15	2.8
ADM 07		-	1	-	2	1	3	3.5	2.8
ADM 08		1	2	1	3	1	2	3.9	3
ADM 09		-	-	-	-	2		2.75	4
ADM 10		-	-	-	2	-		10.5	4
ADM 11		-	-	-	-	-		-	4
ADM 12		-	-	1	-	-		10	6.7
ADM 13		-	-	-	-	-		-	6.7
AST 1		-	-	-	-	-		-	3
AST 2		-	-	-	-	-		-	3
AST 3		1	-	-	1	-		6.75	3
AST 4		1	1	-	-	1	1	2.76	3
AST 5		-	-	1	-	1	-	4.05	4
AST 6		-	1	1	-	-	-	3.5	4
AST 7		-	-	1	1	1	-	3.92	4
AST 8		-	-	-	-	-	2	-	4
AST 9		-	-	-	-	-		-	N/A
AST 10 (Senior assistant)		-	-	-	-	-		-	5
There are no AST/SCs at ENISA: n/a									
AST/SC 1									4
AST/SC 2									5
AST/SC 3									5.9
AST/SC 4									6.7
AST/SC 5									8.3

Table 2: Reclassification of contract staff

Function group	Grade	Staff in activity at 31.12.2024	How many staff members were reclassified in year 2024	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	3	-	-	Between 6 and 10 years
	16	9	2	-	Between 5 and 7 years
	15	4	-	4.5	Between 4 and 6 years
	14	14	-	3.31	Between 3 and 5 years
	13	3	-	4.15	Between 3 and 5 years
CA III	12	3	-	-	-
	11	1	2	2	Between 6 and 10 years
	10	2	1	3	Between 5 and 7 years
	9	0	-	4.9	Between 4 and 6 years
	8	0	-	4.8	Between 3 and 5 years
CA II	6	-	-	-	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
CA I	3	1	-	-	n/a
	2	-	-	-	Between 6 and 10 years
	1	-	-	-	Between 3 and 5 years

C. GENDER REPRESENTATION

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

		Official		TAs		CA		Grand total	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	-	-	23	28,4%	14	34,1%	37	30,3%
	Assistant level (AST and AST/SC)	-	-	13	16,0%	5	12,2%	18	14,8%
	Total	**-**	**-**	**36**	**44,4%**	**19**	**46,3%**	**55**	**45,1%**
Male	Administrator level	-	-	39	48,1%	19	46,3%	58	47,5%
	Assistant level (AST and AST/SC)	-	-	6	7,4%	3	7,3%	9	7,4%
	Total	**-**	**-**	**45**	**55,6%**	**22**	**53,7%**	**67**	**54,9%**
Grand total		**-**	**-**	**81**	**100%**	**41**	**100,0%**	**122**	**100%**

Table 2: Data regarding gender evolution over 5 years on middle and senior management (31.12.2024)

	2020		31.12.2024	
	Number	%	Number	%
Female Managers	2	25%	2[45]	29%
Male Managers	6	75%	5[46]	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 some 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.

45 This category comprises the ED and Heads of Unit level.

46 This category comprises the ED and Heads of Unit level.

D. GEOGRAPHICAL BALANCE

Table 1: Data as of 31.12.2024 - statutory staff only

Nationality	AD + CA FG IV		AST/SC- AST + CA FGI/CA FGII/CA FGIII		Total	
	Number	% of total staff members in AD and FG IV categories	Number	% of total staff members in AST SC/AST and FG I, II and III categories	Number	% of total staff
BE	4	4,2%	2	7,4%	6	4,9%
BG	2	2,1%		0,0%	2	1,6%
CY	2	2,1%	2	7,4%	4	3,3%
CZ	1	1,1%		0,0%	1	0,8%
DE	1	1,1%		0,0%	1	0,8%
Double *	5	5,3%	4	14,8%	9	7,4%
EE	2	2,1%		0,0%	2	1,6%
EL	38	40,0%	13	48,1%	51	41,8%
ES	3	3,2%		0,0%	3	2,5%
FR	7	7,4%	1	3,7%	8	6,6%
HU	1	1,1%		0,0%	1	0,8%
IT	8	8,4%		0,0%	8	6,6%
LT	2	2,1%	1	3,7%	3	2,5%
LV	2	2,1%		0,0%	2	1,6%
NL	4	4,2%		0,0%	4	3,3%
PL	3	3,2%	1	3,7%	4	3,3%
PT	3	3,2%	1	3,7%	4	3,3%
RO	6	6.3%	1	3,7%	7	5,7%
SE	1	1,1%		0,0%	1	0,8%
RO		0,0%	1	3,7%	1	0,8%
TOTAL	95	100%	27	100%	122	100%

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

Most represented nationality	2020		31.12.2024	
	Number	%	Number	%
Greek	29 (out of 74)	39,2	51 (out of 121)	41,8

E. SCHOOLING

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

ANNEX 6
ENVIRONMENT MANAGEMENT

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

As a first step, the agency undertook an exercise in 2022 to map its current climate footprint by conducting an audit of past ENISA emissions for which 2019 and 2021 were used as reference years.

ENISA further strengthened its environmental management and carried out an overarching audit during the course of 2023 on the CO2 impact of all the operations of the agency in 2023.

In order to ensure that ENISA is on the correct path towards climate neutrality by 2030 and to promote and enhance ecological sustainability across all the agency's operations, the following key actions were undertaken during the course of 2024/2025 with a view to acquiring an EMAS certificate.

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

- Several actions for the reduction of greenhouse gas (GHG) emissions were further implemented. These included recycling office waste in a structured manner (via dedicated recycling bins and guidelines on the proper use of the bins), the modernisation of the water system, the incorporation of provisions on GHG emissions in the agency's public procurement procedures and tenders, awareness raising sessions and dedicated training for all staff about Eco-Management and Audit Scheme (EMAS) and the greening initiatives of the agency.
- During 2024 the registration and implementation of an environmental management system (according to the EMAS regulations) took place with the creation of EMS (European Management System) templates and procedures.
- An internal audit and environmental performance evaluation also took place during the course of 2024/2025.
- The agency also proceeded to the drafting of its environmental statement for which the formal approval by ENISA's management Team
- ENISA will communicate externally via it's website about EMAS and the greening initiatives of the Agency

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

ANNEX 7
BUILDING POLICY

CURRENT BUILDINGS

The Heraklion office is expected to be vacated by the 30th June 2026.

Building name and type	Location	Location surface area (in m²)			Rental contract			Host country (grant or support)	Build-ing present value (EUR)
		Office space (m²)	non-office (m²)	Total (m²)	Rent (EUR per year)	Duration	Type		
Heraklion office	**Herak-lion**	706		706		01/01/2021 to 28/02/2030;	Lease	Rent is fully covered by Hellenic authorities	N/A
Athens office	**Chalan-dri**	4 498	2 617	7 115		01/01/2021 to 28/02/2030;	Lease	Rent is fully covered by Hellenic authorities	N/A
Brussels office	**Brussels centre**	98		98	56 496	N/a	SLA with OIB		N/A
Total	**Location**	5 302	2 617	7 920					

BRUSSELS OFFICE

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

Resources (indicative)	2026	2027	2028
Head count (FTEs)	13-14	13-14	13-14
Budget (one-off and maintenance costs)	130 000	130 000	130 000

ANNEX 8
PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education/day care
In accordance with Art.23 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 04 October 2019 and is applicable to ENISA and its staff.	In accordance with Art.35 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement the 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 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.

ANNEX 9
EVALUATIONS

In 2025 ENISA concluded the second biennial stakeholder satisfaction survey of its work programmes for the years 2023 and 2024. The results of the second stakeholder satisfaction survey shed important light on how stakeholders perceive the added value of ENISA's work.

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

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

Aggregate results:

- Aggregate results for added value 88% (down 4%) and take up 82% (down 3%) were slightly lower in 2023-2024 than the resounding results in 2021-2022.
- Aggregate results for the non-duplication with MSs activities 89% improved by 6% in 2023-2024 compared to 2021-2022.
- Aggregate results for how ENISA operates with stakeholders improved in the area of taking onboard stakeholder feedback 94% (up 2%) and facilitating community interaction 96% (up 1%). However how ENISA organised its work and processes was 89%, down 6% compared to 2021-2022.
- Finally, trust in ENISA's ability to achieve its mandate increased by 1% to 96% in 2023-2024 compared to 2021-2022.

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

ANNEX 10

STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

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

The Control Environment is the set of standards for 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 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 its objectives. In this respect, both external and internal communication need to be considered. External communication provides the Agency's stakeholders and EU citizens with information on ENISA's policies, objectives, actions and achievements. Internal communication provides ENISA staff with the information required to support the achievement of objectives and an 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 network of EU Agencies, in 2022 ENISA conducted 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. ENISA's revised internal control framework has been used since 2023 for the assessment of internal controls, together with a comprehensive methodology for enterprise risk assessment across the Agency.

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

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

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

The Agency applies the mandatory signing of declarations of conflict of interest and confidentiality by all experts replying to a Call of Expression of Interest (CEI) and by parties contracted through a procurement procedure. Annual declarations of interest shall also be submitted by members of the Management Board and their alternates, members of the National Liaison officers network, members of the Advisory group and members of Ad hoc Working Groups. Additionally, at the start of each meeting the members, observers and any experts participating in the meeting of an Ad Hoc Working Group should declare any interests that could be considered to be prejudicial to their independence with respect to any of the points on the agenda.

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

ANNEX 11

PLAN FOR GRANT, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS

	SLA	Date of signature	Total amount	Duration	Counter-part	Short description
1	SLA with ECCC (Activity 9)	20/12/2022	54 604	Renewal on annual basis auto-matically	ECCC	The scope of this Service Level Agreement covers support services offered by ENISA to ECCC: data protection officer, accounting officer.
2	SLA with EU-LISA M-CBU-24-C35 (Activity 3)	08/05/2024	120 000	31/12/2025 (with option to renew)	EU-LISA	The scope of this Service Level Agreement covers support services offered by ENISA to EU-LISA on the planning, execution and evaluation of upcoming annual Security and Business Continuity Exercises.
			Contribution agreements			
1	Preparedness and Incident Response Support for Key Sectors	21/12/2023	20 000 000 (prefinanc-ing rate 80%)	up to 31/12/26	DG CNECT	The action is developed through the 'ENISA Cybersecurity Support Action Programme' which has three parts: 1) EU-level cyber reserve with services from trusted private providers for incident response; 2) penetration tests in key sectors and 3) DG CNECT's contribution to the Cyber Analysis and Situation Centre.
2	Incident and Vulnerability Response Support and Reporting HAS as-sessment / EUCC pilots (Addendum I - LC-03708221)	19/12/2024	Up to 15 250 000 (prefinanc-ing rate 80%) (+250 000 follow-ing the amend-ment)	2025 to 2027	DG CNECT	1) The following activities: 1) Gradual set-up and operation of an EU-level cyber reserve with services from trusted private providers to deliver relevant services to mitigate the impact of serious incidents; 2) Contribution to the Cyber Analysis and Situation Centre; and 3) The establishment, management, and maintenance on a day-to-day basis of the Cyber Resilience Act single reporting platform. 2) Additional actions following the amendment: Ac-tions in support of the implementation of the Cyber Resilience Act, notably actions related to the devel-opment and assessment of technical specifications and standards, and interplay with the European Cybersecurity Certification schemes.
3	CRA single reporting platform (fea-sibility study)	09/12/2024	Up to 400 000 (pre-financing rate 60%)	up to 31/07/26	DG CNECT	The purpose of this Agreement is to provide the Agency with a financial contribution to conduct a feasibility study on a single reporting platform under the Cyber Resilience Act that will inform the future steps of the platform's development.
4	EU Cyberse-curity Reserve & Cyber Situation and Analysis Centre	31/07/2025	Up to 36 670 000 (pre financing rate 100% for the first contri-bution 12months)	2025 to 2028 (36 months)	DG CNECT	The purpose of this agreement is to provide a fi-nancial contribution to finance the implementation of the action 'EU Cybersecurity Reserve', and of the action 'Cyber Situation and Analysis Centre'.

Detailed breakdown of planned resource consumption under the contribution agreements

Contribution agreement	Implementation period	Start date	CA total budget EUR	Remaining Amount to be received from 2026 onwards	2024 Instalments	2025 Instalments	2026 forecast of commitment appropriations	2027 forecast of commitment appropriations	2028 forecast of commitment appropriations	Related Activities
Preparedness and Incident Response Support for Key Sectors (Support Action & Situational Analysis Centre)	until 31/12/2026	21/12/2023	20 000 000	4 000 000	16 000 000	0	4 000 000	0	0	Act.6
Incident and Vulnerability Response Support and Reporting (Support Action, CRA SPR and SitCEN)	until 31/12/2027	19/12/2024	15 000 000	3 000 000	0	12 000 000	1 500 000	1 500 000	0	Act.4 Act.5 Act.6 Act.7 Act.8 Act.9 Act.11
Support for the implementation of the Cyber Resilience Act, notably actions related to the development and assessment of technical specifications and standards and the interplay with European Cybersecurity Certification schemes[48] and the CRA	until 31/12/2027	3/7/2025	250 000	250 000	0	0	125 000	125 000	0	Part of the above CA, reference Act.7 and Act.8
Single reporting platform (feasibility study), the EU	until 31/07/2026	9/12/2024	400 000	160 000	0	240 000	160 000	0	0	Act. 5
Cybersecurity Reserve and the Cyber Situation and Analysis Centre	36 months	31/7/2025	36 670 000	24 446 666.67	0	12 223 333.33	12 223 333.33	12 223 333.33	0	Act.4 Act.6 Act.9 Act.11
Total Budget			**72 320 000**	**31 856 667**	**16 000 000**	**24 463 333.33**	**18 008 333**	**13 848 333.34**	**0**	

48 Amendment no.1 to the 2024 Contribution Agreement on the Implementation of the 'Incident and Vulnerability Response Support and Reporting' Action.

Contribution agreement	2026 forecast of Contract agents	2027 forecast of Contract Agents	2028 forecast Contract Agents	Related Activities
Preparedness and Incident Response Support for Key Sectors (Support Action & Situational Analysis Centre)	12	0	0	Act.6, Act.5
Incident and Vulnerability Response Support and Reporting (Support Action, CRA, SPR and SitCEN)	6	8		Act.5, Act.2, Act.7, Act.8
HAS Amendment no.1 to the 2024 Contribution Agreement on the Implementation of the 'Incident and Vulnerability Response Support and Reporting' Action	0	0	0	Part of the above CA, Act.7, Act.8
CRA single reporting platform	0	0	0	Act.5
EU Cybersecurity Reserve & Cyber Situation and Analysis Centre	0	10	13	Act.6, Act.5, Act.2
Total	**18**	**18**	**13**	

ANNEX 12

STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

ENISA'S international strategy confirms the Agency's mandate in terms of its focus on the EU and EU actors, while also allowing increased flexibility to engage with international partners in line with the strategic objectives outlined in the ENISA Strategy for a Trusted and Cyber Secure Europe of July 2020 and in support of the EU's international priorities. The Agency's international strategy was adopted by the MB in 2021. A new international strategy is expected to be presented to the MB for endorsement in Q4 2025.

Article 12 of the Cybersecurity Act (CSA) states that 'ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity' in various ways, including facilitating the exchange of best practices and providing expertise, at the request of the Commission.

Article 42 'Cooperation with third countries and international organisations' states the following 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, working arrangements shall comply with the Staff Regulations of Officials and Conditions of Employment of Other Servants in any event.
3. The Management Board shall adopt a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent. The Commission shall ensure that ENISA operates within its mandate and the existing institutional framework by concluding appropriate working arrangements with the Executive Director.

ANNEX 13

ANNUAL COOPERATION PLAN 2026

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

ANNEX 14
PROCUREMENT PLAN 2026

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

ENISA UNIT	TITLE of Contract	TYPE of procedure	Tender launch (2026)	Contract signature	Total budget est. 4 years EUR
PMA (Policy Monitoring and Analyses Unit)	Supporting ENISA in the monitoring and analysis of strategies and policies	Open – 4 years FWC (Framework Contract)	Q1	Q1	800 000
RoCS (Resilience of Critical Sectors Unit)	Supporting analysis of cybersecurity investments and business resilience	Open – 4 years FWC	Q4	2027	1 200 000
CBU (Capacity Building Unit)	External Cloud-Based Training Platform Access and Support Services	Open – 4 years FWC	Q3	Q3	4 000 000
CBU	Support for the European Cybersecurity Skills Framework (ECSF), attestation schemes, skills gap reporting	RoC	Q2	Q2	200 000
OCU (Operational Cooperation Unit)	Security assessment, monitoring and ICT services	Open – 4 years FWC	Q3	Q4	3 000 000
OCU	IT infrastructure management and consultancy services	Open – 4 years FWC	Q2	Q2	1 700 000

OCU	Consultancy services to improve incident response and crises management in the EU	Open – 4 years FWC	Q1	Q2	1 600 000
CCU (Cybersecurity Certification Unit)	EU Common Criteria Scheme (EUCC) maintenance	RoC	Q1	Q1	45 000
CCU	Supporting the development of the EU5G scheme	RoC	Q1	Q1	30 000
CCU	Support for ECCC subgroup on crypto	RoC	Q1	Q1	30 000
CCU	Development and maintenance services for the EU cybersecurity index tool	Open – 4 years FWC	Q2	Q3	1 000 000
EDO (Executive Director's Office)	Tax Consultation Services	Open – 4 years FWC	Q2	Q2	200 000
EDO	Management services for the organisation of events and meetings	Open – 4 years FWC	Q3	Q4	7 000 000
EDO	Risk assessment, control and governance framework	RoC	Q1	Q1	25 000
EDO	Penetration tests for 6 to 8 apps per year (centralised)	RoC	Q1	Q1	70 000
EDO	Maturity assessment, BIA, BCP execution and cybersecurity plans	RoC	Q1	Q1	30 000
CSS	Facilities Management Services	Restricted – 4 years FWC	Q3	Q4	1 600 000
CSS	Provision of Medical services	Open – 4 years FWC	Q3	Q4	260 000

The total indicative budget reserved for procurement is approximately 2.8 million euros.

ANNEX 15

ENISA STATUTORY OPERATIONAL TASKS ARISING FROM EU LEGISLATION 2024

The following is a list of EU legislation mapped by activity as of September 2024.

Please note functions of asterisks:

* - denotes responsibility for only part of a legal provision

** - denotes shared responsibility for the same legal provision

EU legislation	Article	Legal provisions	Responsible unit/activity under Art.3(3) MB/2024/10
AIA	Art.67(5)	**Advisory forum**. The Fundamental Rights Agency, ENISA, the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), and the European Telecommunications Standards Institute (ETSI) shall be permanent members of the advisory forum.	ACTIVITY 8
CRA	Art.10	**Enhancing skills in a cyber resilient digital environment**. For the purposes of this Regulation and in order to respond to the needs of professionals for support in the implementation of this Regulation, Member States with, where appropriate, the support of the Commission, the European Cybersecurity Competence Centre and ENISA, while fully respecting the responsibility of the Member States in the field of education, shall promote measures and strategies for cyber skills.	ACTIVITY 3
CRA	Art.16(4)	**Managing risks to the security of the single reporting platform**. ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single reporting platform and the information submitted or disseminated via the single reporting platform. It shall notify without undue delay any security incident affecting the single reporting platform to the CSIRTs network as well as to the Commission.	ACTIVITY 4

CRA	Art.14(1)	**Reporting obligations of manufacturers**. A manufacturer shall immediately notify any actively exploited vulnerability contained in any product with digital elements of which it becomes aware to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA.	ACTIVITY 5
CRA	Art.14(3)	**Reporting obligations of manufacturers**. A manufacturer shall immediately notify any severe incident having an impact on the security of the product with digital elements of which it becomes aware to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA.	ACTIVITY 5
CRA	Art.14(7)	**Reporting obligations of manufacturers**. The notifications referred to in paragraphs 1 and 3 of this Article shall be submitted via the single reporting platform referred to in Article 16 using one of the electronic notification end-points referred to in Article 16(1). The notification shall be submitted using the electronic notification end-point of the CSIRT designated as coordinator for the Member State where the manufacturers have their main establishment in the Union and shall be simultaneously accessible to ENISA.	ACTIVITY 5
CRA	Art.14(9)	**Reporting obligations of manufacturers**. Within 12 months from the date of entry into force of this Regulation, the Commission shall adopt a delegated act in accordance with Article 61 to supplement this Regulation by specifying the terms and conditions for applying cybersecurity related grounds in relation to delaying the dissemination of notifications as referred to in Article 16(2). The Commission shall cooperate with the CSIRTs network as established pursuant to Article 15 of Directive EU2022/2555 and ENISA in preparing the draft delegated act.	ACTIVITY 5
CRA	Art.14(10)	**Reporting obligations of manufacturers**. The Commission may, by means of implementing acts, specify further the format and procedures of the notifications referred to in this Article as well as in Articles 15 and 16. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). The Commission shall cooperate with the CSIRTs network and ENISA in preparing those draft implementing acts.	ACTIVITY 5
CRA	Art.15(1)	**Voluntary reporting**. Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or to ENISA.	ACTIVITY 5
CRA	Art.15(2)	**Voluntary reporting**. Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of a product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.	ACTIVITY 5

CRA	Art.15(3)	**Voluntary reporting**. The CSIRT designated as coordinator or ENISA shall process the notifications referred to in paragraphs 1 and 2 of this Article in accordance with the procedure laid down in Article 16.	ACTIVITY 5
CRA	Art.15(5)	**Voluntary reporting**. The CSIRTs designated as coordinators as well as ENISA shall ensure the confidentiality and appropriate protection of the information provided by a notifying natural or legal person.	ACTIVITY 5
CRA	Art.16(1)	**Establishment of a single reporting platform**. For the purposes of the notifications referred to in Articles 14(1) and (3) and Articles 15(1) and (2) and in order to simplify the reporting obligations of manufacturers, a single reporting platform shall be established by ENISA. The day-to-day operations of that single reporting platform shall be managed and maintained by ENISA. The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification end-points.	ACTIVITY 5
CRA	Art.16(2)	**Establishment of a single reporting platform**. Where a CSIRT decides to withhold a notification, it shall immediately inform ENISA about the decision and provide both a justification for withholding the notification as well as an indication of when it will disseminate the notification in accordance with the dissemination procedure laid down in this paragraph. ENISA may support the CSIRT on the application of cybersecurity related grounds in relation to delaying the dissemination of the notification. Only the information that a notification was made by the manufacturer, the general information about the product, the information on the general nature of the exploit and the information that security related grounds were raised are made available immediately to ENISA until the full notification is disseminated to the CSIRTs concerned and ENISA. Where, based on that information, ENISA considers that there is a systemic risk affecting security in the internal market, it shall recommend to the recipient CSIRT that it disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.	ACTIVITY 5
CRA	Art.16(5)	**Establishment of a single reporting platform**. ENISA, in cooperation with the CSIRTs network, shall provide and implement specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single reporting platform referred to in paragraph 1, including at least the security arrangements related to the establishment, operation and maintenance of the single reporting platform, as well as the electronic notification end-points set up by the CSIRTs designated as coordinators at national level and ENISA at Union level, including procedural aspects to ensure that, where no corrective or mitigating measures are available for a notified vulnerability, information about that vulnerability is shared in line with strict security protocols and on a need-to-know basis.	ACTIVITY 5

CRA	Art.17(1)	**Other provisions related to reporting**. ENISA may submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established under Article 16 of Directive (EU) 2022/2555 information notified pursuant to Article 14(1) and (3) and Article 15(1) and (2) if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level. For the purpose of determining such relevance, ENISA may consider technical analyses performed by the CSIRTs network, where available	ACTIVITY 5
CRA	Art.17(2)	**Other provisions related to reporting**. Where public awareness is necessary to prevent or mitigate a severe incident having an impact on the security of a product with digital elements or to handle an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the CSIRT designated as coordinator of the relevant Member State, may, after consulting the manufacturer concerned and, where appropriate, in cooperation with ENISA, inform the public about the incident or require the manufacturer to do so.	ACTIVITY 5
CRA	Art.17(3)*	**Technical Report**. ENISA, on the basis of the notifications received pursuant to Article 14(1) and (3) and Article 15(1) and (2), shall prepare, every 24 months, a technical report on these matters.	ACTIVITY 5
CRA	Art.17(5)	**European vulnerability database**. After a security update or when another form of corrective or mitigating measures is available, ENISA shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified pursuant to Article 14(1) or Article 15(1) of this Regulation to the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555.	ACTIVITY 5
CRA	Art.70(2)	**Evaluation and review**. Within 45 months from the date of entry into force of this Regulation, the Commission shall, after consulting ENISA and the CSIRTs network, submit a report to the European Parliament and to the Council, assessing the effectiveness of the single reporting platform set out in Article 16, as well as the impact of the application of the cybersecurity related grounds referred to in Article 16(2) by the CSIRTs designated as coordinators on the effectiveness of the single reporting platform as regards the timely dissemination of received notifications to other relevant CSIRTs.	ACTIVITY 5

CRA	Art.17(3)*	**Reporting obligations**. ENISA, on the basis of the notifications received pursuant to Article 14(1) and (3) and Article 15(1) and (2), shall prepare, every 24 months, a technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555. The first such report shall be submitted within 24 months after the obligations laid down in Article 14(1) and (3) begin to be applied. ENISA shall include relevant information from its technical reports in its report on the State of Cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555.	ACTIVITY 5
CRA	Art.17(3)*	**Emerging trends regarding cybersecurity risks in products with digital elements**. ENISA shall include relevant information from its technical reports in its report on the State of Cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555.	ACTIVITY 8
CRA	Art.33(2)	S**upport measures for microenterprises and small and medium-sized enterprises, including start-ups**. Member States may, where appropriate, establish cyber resilience regulatory sandboxes. Such regulatory sandboxes shall provide for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with this Regulation for a limited period of time before being placed on the market. The Commission and, where appropriate, ENISA may provide technical support, advice and tools for the establishment and operation of regulatory sandboxes.	ACTIVITY 8
CRA	Art.52(4)	**Market surveillance and control of products with digital elements in the Union market**. Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification authorities designated pursuant to Article 58 of Regulation (EU) 2019/881 and exchange information on a regular basis. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 14 of this Regulation, the designated market surveillance authorities shall cooperate and exchange information on a regular basis with the CSIRTs designated as coordinators and with ENISA.	ACTIVITY 8
CRA	Art.52(5)	**Market surveillance and control of products with digital elements in the Union market**. The market surveillance authorities may request a CSIRT designated as a coordinator or ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 54, market surveillance authorities may request the CSIRT designated as coordinator or ENISA to provide an analysis to support evaluations of the compliance of products with digital elements.	ACTIVITY 8

CRA	Art.52(10)	**Market surveillance and control of products with digital elements in the Union market**. Market surveillance authorities may provide guidance and advice to economic operators on the implementation of this Regulation, with the support of the Commission and, where appropriate, CSIRTs and ENISA.	ACTIVITY 8
CRA	Art.52(14)	**Market surveillance and control of products with digital elements in the Union market**. For products with digital elements that fall within the scope of this Regulation which are classified as high-risk AI systems pursuant to Article 6 of the Regulation, the market surveillance authorities that are designated for the purposes of regulation under the AI Regulation shall be the authorities responsible for the market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to the AI Regulation shall cooperate, as appropriate, with the market surveillance authorities designated pursuant to this Regulation and, with respect to the supervision of the implementation of the reporting obligations pursuant to Article 14 of this Regulation, with the CSIRTs designated as coordinators and with ENISA.	ACTIVITY 8
CRA	Art.56(1)	**Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk**. Where the Commission has sufficient reason to consider, including reasons based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk does not comply with the requirements laid down in this Regulation, it shall inform the relevant market surveillance authorities.	ACTIVITY 8
CRA	Art.56(2)	**Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk**. Where the Commission has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of non-technical risk factors, it shall inform the relevant market surveillance authorities and, where appropriate, the competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary. The Commission shall also consider the relevance of the identified risks for that product with digital elements in view of its tasks regarding coordinated security risk assessments, at Union level, of critical supply chains provided for in Article 22 of Directive (EU) 2022/2555 and consult as necessary with the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and ENISA.	ACTIVITY 8

CRA	Art.56(3)	**Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk**. In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the product with digital elements referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission shall carry out an evaluation of compliance and may request ENISA to provide an analysis to support it. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.	ACTIVITY 8
CRA	Art.57(6)	**Compliant products with digital elements which present a significant cybersecurity risk**. Where the Commission has sufficient reason to consider, including any reason based on information provided by ENISA, that a product with digital elements, although compliant with this Regulation, presents the risks referred to in paragraph 1 of this Article, it shall inform and may request the relevant market surveillance authority or authorities to carry out an evaluation and follow the procedures referred to in Article 54 and paragraphs 1, 2 and 3 of this Article.	ACTIVITY 8
CRA	Art.57(7)	**Compliant products with digital elements which present a significant cybersecurity risk**. In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the product with digital elements referred to in paragraph 6 continues to present the risks referred to in paragraph 1, and no effective measures have been taken by the relevant national market surveillance authorities, the Commission shall carry out an evaluation of the risks presented by that product with digital elements and may request ENISA to provide an analysis to support that evaluation and shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate as necessary with ENISA.	ACTIVITY 8
CRA	Art.59(2)	**Joint activities of market surveillance authorities**. The Commission or ENISA shall propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products with digital elements that fall within the scope of this Regulation with the requirements laid down in this Regulation.	ACTIVITY 8

CRA	Art.60(3)	**Sweeps**. Where, in the performance of its tasks, including those based on the notifications received pursuant to Article 14(1) and (3), ENISA identifies categories of products with digital elements for which sweeps may be organised, it shall submit a proposal for a sweep to the coordinator referred to in paragraph 2 of this Article for the consideration of the market surveillance authorities.	ACTIVITY 8
CSA	Art.5(1)	**Assisting**. ENISA shall assist and advise on the review and development of Union policy and law in the field of cybersecurity and on sector-specific policy and legal initiatives where matters related to cybersecurity are involved, in particular by providing its independent opinion and analysis as well as carrying out preparatory work.	ACTIVITY 1
CSA	Art.6(1)f	**Assisting**. ENISA shall assist Union institutions in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation.	ACTIVITY 1
CSA	Art.6(1)e**	**Assisting**. ENISA shall assist Member States in developing national strategies on the security of network and information systems where requested pursuant to Article 7(2) of Directive (EU) 2016/1148 and promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices.	ACTIVITY 1
CSA	Art.6(1)e**	**Assisting**. ENISA shall assist Member States in developing national strategies on the security of network and information systems where requested pursuant to Article 7(2) of Directive (EU) 2016/1148 and promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices.	ACTIVITY 1
CSA	Art.5(2)	**Assisting**. ENISA shall assist Member States to implement Union policy and law regarding cybersecurity consistently, in particular in relation to Directive (EU) 2016/1148, including by means of issuing opinions and guidelines as well as providing advice and best practices on topics such as risk management, incident reporting and information sharing, as well as by facilitating the exchange of best practices between competent authorities in that regard.	ACTIVITY 2
CSA	Art.5(3)	**Assisting**. ENISA shall assist Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet.	ACTIVITY 2
CSA	Art.5(4)	**Assisting**. ENISA shall contribute to the work of the Cooperation Group pursuant to Article 11 of Directive (EU) 2016/1148 by providing its expertise and assistance.	ACTIVITY 2

CSA	Art.5(5)b	**Supporting**. ENISA shall support the promotion of an enhanced level of security of electronic communications, including by providing advice and expertise as well as by facilitating the exchange of best practices between competent authorities.	ACTIVITY 2
CSA	Art.6(1)j	**Assisting**. ENISA shall assist the Cooperation Group in the exchange of best practices, in particular with regard to the identification by Member States of operators of essential services, pursuant to point (l) of Article 11(3) of Directive (EU) 2016/1148, including in relation to cross-border dependencies, regarding risks and incidents.	ACTIVITY 2
CSA	Art.6(2)	**Supporting**. ENISA shall support information sharing in and between sectors, in particular between the sectors listed in Annex 2 to Directive (EU) 2016/1148, by providing best practices and guidance on available tools and procedures as well as on how to address regulatory issues related to information-sharing.	ACTIVITY 2
CSA	Art.9(c)	**Advising**. ENISA shall, in cooperation with experts from Member States' authorities and relevant stakeholders, provide advice, guidance and best practices for the security of network and information systems, in particular for the security of the infrastructures supporting the sectors listed in Annex 2 to Directive (EU) 2016/1148 and those used by the providers of the digital services listed in Annex 3 to that Directive	ACTIVITY 2
CSA	Art.6(1)h	**Assisting**. ENISA shall assist Member States by regularly organising the cybersecurity exercises at Union level referred to in Article 7(5) on at least a biennial basis and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them.	ACTIVITY 3
CSA	Art.6(1)i	**Assisting**. ENISA shall assist relevant public bodies by offering training regarding cybersecurity in cooperation with stakeholders where appropriate.	ACTIVITY 3
CSA	Art.6(1)c*	**Assisting**. ENISA shall assist Union institutions, bodies, offices and agencies to improve their capabilities to respond to cyber threats and incidents, in particular through appropriate support for the CERT-EU.	ACTIVITY 3
CSA	Art.6(1)c*	**Assisting**. ENISA shall assist Union institutions, bodies, offices and agencies in their efforts to improve the prevention, detection and analysis of cyber threats and incidents, in particular through appropriate support for the CERT-EU.	ACTIVITY 3

CSA	Art.7(5)	**Organising**. ENISA shall regularly organise cybersecurity exercises at Union level, and shall support Member States and Union institutions, bodies, offices and agencies in organising cybersecurity exercises upon their requests. Such cybersecurity exercises at Union level may include technical, operational or strategic elements. On a biennial basis, ENISA shall organise a large-scale comprehensive exercise. Where appropriate, ENISA shall also contribute to and help organise sectoral cybersecurity exercises together with relevant organisations that also participate in cybersecurity exercises at Union level.	ACTIVITY 3
CSA	Art.10(a)	**Raising public awareness**. ENISA shall raise public awareness of cybersecurity risks and will provide guidance on good practices for individual users aimed at citizens, organisations and businesses, including in cyber hygiene and cyber literacy.	ACTIVITY 3
CSA	Art.10(d)	**Best practices**. ENISA shall support closer coordination and the exchange of best practices among Member States on cybersecurity awareness and education.	ACTIVITY 3
CSA	Art.10(b)	**Outreach campaigns**. ENISA shall, in cooperation with the Member States, Union institutions, bodies, offices and agencies and industry, organise regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate;	ACTIVITY 3
CSA	Art.10(c)	**Cybersecurity awareness**. ENISA shall assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education.	ACTIVITY 3
CSA	Art.12(a)	**International cooperation**. ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity by, where appropriate, engaging as an observer in the organisation of international exercises and analysing and reporting to the Management Board on the outcome of such exercises.	ACTIVITY 4
CSA	Art.12(b)	**International cooperation**. ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity by, at the request of the Commission, facilitating the exchange of best practices.	ACTIVITY 4
CSA	Art.12(c)	**International cooperation**. ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity by, at the request of the Commission, providing it with expertise.	ACTIVITY 4

CSA	Art.12(d)	**International cooperation**. ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity by providing advice and support to the Commission on matters concerning agreements for the mutual recognition of cybersecurity certificates with third countries, in collaboration with the European Cybersecurity Competence Centre (ECCG) established under Article 62.	ACTIVITY 4
CSA	Art.6(1)b	**Assisting**. ENISA shall assist Member States and Union institutions, bodies, offices and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.	ACTIVITY 4
CSA	Art.7(1)	**Supporting**. ENISA shall support operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders.	ACTIVITY 4
CSA	Art.7(2)a	**Supporting**. ENISA shall cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies, including the CERT-EU, with the services dealing with cybercrime and with supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern.	ACTIVITY 4
CSA	Art.7(4)b*	**Supporting**. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by assisting, at the request of one or more Member States, through the provision of expertise and, in particular, by encouraging the voluntary sharing of relevant information and technical solutions between Member States.	ACTIVITY 4
CSA	Art.7(3)	**Secretariat**. ENISA shall provide the secretariat of the CSIRTs network pursuant to Article 12(2) of Directive (EU) 2016/1148 and in that capacity shall actively support information sharing and the cooperation among its members.	ACTIVITY 4
CSA	Art.7(4)	**Cooperation**. ENISA and CERT-EU shall engage in structured cooperation to benefit from synergies and to avoid the duplication of activities in performing tasks listed under Art.7(4) points a-d.	ACTIVITY 4
CSA	Art.7(4)a*	**Supporting**. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by advising on how to improve their capabilities to prevent, detect and respond to incidents.	ACTIVITY 4

CSA	Art.7(7)b	**Cross-border incidents**. ENISA shall contribute to developing a cooperative response at the level of the Union and Member States to large-scale cross-border incidents or crises related to cybersecurity, mainly by ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level.	ACTIVITY 4
CSA	Art.7(7)d	**Cross-border incidents**. ENISA shall contribute to developing a cooperative response at the level of the Union and Member States to large-scale cross-border incidents or crises related to cybersecurity, mainly by supporting Union institutions, bodies, offices and agencies and, at their request, Member States in the public communications relating to such incidents or crises.	ACTIVITY 4
CSA	Art.7(7)e	**Cross-border incidents**. ENISA shall contribute to developing a cooperative response at the level of the Union and Member States to large-scale cross-border incidents or crises related to cybersecurity, mainly by testing cooperation plans for responding to such incidents or crises at the Union level and, at their request, supporting Member States in testing such plans at the national level.	ACTIVITY 4
CSA	Art.6(1)d	**Assisting**. ENISA will assist Member States in developing national CSIRTs, where requested pursuant to Article 9(5) of Directive (EU) 2016/1148.	ACTIVITY 4
CSA	Art.(1)g	**Assisting**. ENISA will assist national and Union CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state-of-the-art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices.	ACTIVITY 4
CSA	Art.5(6)a	**Supporting**. ENISA will support regular reviews of activities related to Union policy by preparing an annual report on the state of the implementation of the respective legal framework regarding information on Member States' incident notifications provided by the single point of contact to the Cooperation Group pursuant to Article 10(3) of Directive (EU) 2016/1148.	ACTIVITY 5
CSA	Art.5(6)b	**Supporting**. ENISA will support regular reviews of activities relating to Union policy by preparing an annual report on the state of the implementation of the legal framework regarding summaries of notifications of breaches of security or losses of integrity received from trust service providers advised by the supervisory bodies to ENISA, pursuant to Article 19(3) of Regulation (EU) 2014/910 of the European Parliament and of the Council.	ACTIVITY 5

CSA	Art.5(6)c	**Supporting**. ENISA will support regular reviews of activities relating to Union policy by preparing an annual report on the state of the implementation of the legal framework regarding notifications of security incidents transmitted by the providers of public electronic communications networks or of publicly available electronic communications services, advised by the competent authorities to ENISA, pursuant to Article 40 of Directive (EU) 2018/1972.	ACTIVITY 5
CSA	Art.6(1)a	**Assisting**. ENISA will assist Member States in their efforts to improve the prevention, detection and analysis of their capability to respond to cyber threats and incidents by providing them with knowledge and expertise.	ACTIVITY 5
CSA	Art.7(4)a*	**Supporting**. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by, at the request of one or more Member States, providing advice in relation to a specific cyber threat.	ACTIVITY 5
CSA	Art.7(4)b*	**Supporting**. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by assisting, at the request of one or more Member States, in the assessment of incidents having a significant or substantial impact.	ACTIVITY 5
CSA	Art.7(4)c	**Supporting**. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by analysing vulnerabilities and incidents on the basis of publicly available information or information provided voluntarily by Member States for that purpose.	ACTIVITY 5
CSA	Art.7(4)d	**Supporting**. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by, at the request of one or more Member States, providing support in relation to ex-post technical inquiries regarding incidents having a significant or substantial impact within the meaning of Directive (EU) 2016/1148.	ACTIVITY 5
CSA	Art.7(6)	**Situation report**. ENISA, in close cooperation with Member States, shall prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats based on publicly available information, its own analysis and reports shared by, among others, Member States' CSIRTs or the single point of contact established by Directive (EU) 2016/1148 with the European Cybercrime Centre (EC3) and CERT-EU, both on a voluntary basis.	ACTIVITY 5
CSA	Art.7(7)a	**Assisting**. ENISA shall contribute to developing a cooperative response at the level of the Union and Member States to large-scale cross-border incidents or crises related to cybersecurity, mainly by aggregating and analysing reports from national sources that are in the public domain or shared on a voluntary basis with a view to contributing to the establishment of a common situational awareness.	ACTIVITY 5

CSA	Art.9(b)	**Analyses**. ENISA shall perform long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents.	ACTIVITY 5
CSA	Art.9(e)	**Analyses**. ENISA shall collect and analyse publicly available information regarding significant incidents and compile reports with a view to providing guidance to citizens, organisations and businesses across the Union.	ACTIVITY 5
CSA	Art.7(4)b*	**Assisting**. ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by assisting, at the request of one or more Member States, in facilitating the technical handling of such incidents.	ACTIVITY 6
CSA	Art.7(7)c	**Assisting**. ENISA shall contribute to developing a cooperative response at the level of the Union and Member States to large-scale cross-border incidents or crises related to cybersecurity mainly by, upon request, facilitating the technical handling of such incidents or crises including, in particular, by supporting the voluntary sharing of technical solutions between Member States.	ACTIVITY 6
CSA	Art.8(1)a	**Supporting**. ENISA shall support and promote the development and implementation of Union policy on the cybersecurity certification of ICT products, ICT services and ICT processes as established in Title III of this Regulation, by monitoring developments on an ongoing basis in the related areas of standardisation and by recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to point (c) of Article 54(1) where standards are non-existent.	ACTIVITY 7
CSA	Art.8(1)b	**Supporting**. ENISA shall support and promote the development and implementation of Union policy on the cybersecurity certification of ICT products, ICT services and ICT processes as established in Title III of this Regulation, by preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services and ICT processes in accordance with Article 49 the CSA.	ACTIVITY 7
CSA	Art.8(1)c	**Supporting**. ENISA shall support and promote the development and implementation of Union policy on the cybersecurity certification of ICT products, ICT services and ICT processes as established in Title III of this Regulation, by evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8) of the CSA.	ACTIVITY 7
CSA	Art.8(1)d	**Supporting**. ENISA shall support and promote the development and implementation of Union policy on the cybersecurity certification of ICT products, ICT services and ICT processes as established in Title III of this Regulation, by participating in peer reviews pursuant to Article 59(4) of the CSA.	ACTIVITY 7

CSA	Art.8(1)e	**Supporting**. ENISA shall support and promote the development and implementation of Union policy on the cybersecurity certification of ICT products, ICT services and ICT processes as established in Title III of this Regulation, by assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5) of the CSA.	ACTIVITY 7
CSA	Art.8(2)	**Secretariat**. ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group (SCCG) pursuant to Article 22(4) the CSA.	ACTIVITY 7
CSA	Art.8(3)	**Guidelines**. ENISA shall compile and publish guidelines on the development of good practices concerning the cybersecurity requirements for ICT products, ICT services and ICT processes, in cooperation with national cybersecurity certification authorities and the industry in a formal, structured and transparent way.	ACTIVITY 7
CSA	Art.8(4)	**Assisting**. ENISA shall contribute to capacity-building related to the evaluation and certification processes by compiling and issuing guidelines as well as by providing support to Member States at their request.	ACTIVITY 7
CSA	Art.48	**Request for a European cybersecurity certification scheme**. (1) The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union's rolling work programme. (2) In justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union's rolling work programme. The Union rolling work programme shall be updated accordingly.	ACTIVITY 7
CSA	Art.49(1)	**Preparation, adoption and review of a European cybersecurity certification scheme**. Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54 of the CSA.	ACTIVITY 7
CSA	Art.49(2)	**Preparation, adoption and review of a European cybersecurity certification scheme**. Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board.	ACTIVITY 7
CSA	Art.49(3)	**Preparation, adoption and review of a European cybersecurity certification scheme**. When preparing a candidate scheme, ENISA shall consult all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process.	ACTIVITY 7

CSA	Art.49(4)	**Preparation, adoption and review of a European cybersecurity certification scheme**. For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise.	ACTIVITY 7
CSA	Art.49(5)	**Preparation, adoption and review of a European cybersecurity certification scheme**. ENISA shall closely cooperate with the ECCG. The ECCG shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme and shall adopt an opinion on the candidate scheme.	ACTIVITY 7
CSA	Art.49(6)	**Preparation, adoption and review of a European cybersecurity certification scheme**. ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme prepared in accordance with paragraphs 3, 4 and 5 to the Commission. The opinion of the ECCG shall not bind ENISA nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission.	ACTIVITY 7
CSA	Art.49(7)	**Preparation, adoption and review of a European cybersecurity certification scheme**. The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services and ICT processes that meets the requirements set out in Articles 51, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).	ACTIVITY 7
CSA	Art.49(8)	**Preparation, adoption and review of a European cybersecurity certification scheme**. At least once every five years, ENISA shall evaluate each adopted European cybersecurity certification scheme taking into account the feedback received from interested parties. If necessary, the Commission or the ECCG may request ENISA to start the process of developing a revised candidate scheme in accordance with Article 48 and this Article.	ACTIVITY 7
CSA	Art.50 (1)	**Website on European cybersecurity certification schemes**. ENISA shall maintain a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity The website will include information regarding European cybersecurity certification schemes that are no longer valid so that any expired European cybersecurity certificates and EU statements of conformity may be withdrawn. ENISA will maintain links on the website to a repository of cybersecurity information provided in accordance with Article 55.	ACTIVITY 7

CSA	Art.53(3)	**Conformity self-assessment**. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.	ACTIVITY 7
CSA	Art.58(7)g	**National cybersecurity certification authorities**. The National cybersecurity certification authorities shall provide an annual summary report on the activities conducted under points (b), (c) and (d) of this paragraph or under paragraph 8 to ENISA and the ECCG.	ACTIVITY 7
CSA	Art.59(4)	**Peer review**. A peer review shall be carried out by at least two national cybersecurity certification authorities of other Member States and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review.	ACTIVITY 7
CSA	Art.62(5)	**European Cybersecurity Certification Group**. With the assistance of ENISA, the Commission shall chair the ECCG and the Commission shall provide the ECCG with a secretariat in accordance with point (e) of Article 8(1).	ACTIVITY 7
CSA	Art.5(5)a	**Supporting**. ENISA will support the development and implementation of Union policy in the field of electronic identity and trust services, in particular by providing advice and by issuing technical guidelines as well as by facilitating the exchange of best practices between competent authorities.	ACTIVITY 8
CSA	Art.5(5)c	**Supporting**. ENISA will support Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy, including by providing advice to the European Data Protection Board upon request.	ACTIVITY 8
CSA	Art.8(5)	**Facilitating**. ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services and ICT processes.	ACTIVITY 8
CSA	Art.8(6)**	**Guidelines**. ENISA shall draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148.	ACTIVITY 8
CSA	Art.8(7)	**Regular analyses**. ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union.	ACTIVITY 8
CSA	Art.9(a)	**Analyses**. ENISA shall perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity.	ACTIVITY 8

CSA	Art.11(a)	**Research**. ENISA shall advise the Union institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of cybersecurity, with a view to enabling effective responses to current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies, and with a view to using risk-prevention technologies effectively.	ACTIVITY 8
CSA	Art.11(b)	**Funding**. ENISA shall, where the Commission has conferred the relevant powers on it, participate in the implementation phase of research and innovation funding programmes or as a beneficiary.	ACTIVITY 8
CSA	Art.11(c)	**Research & Innovation**. ENISA shall contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity.	ACTIVITY 8
CSA	Art.9(d)	**Publicise**. ENISA shall, through a dedicated portal, pool, organise and make available to the public information on cybersecurity provided by Union institutions, bodies, offices and agencies and information on cybersecurity provided on a voluntary basis by Member States as well as private and public stakeholders.	EDO
CSoA (Cyber Solidarity Act)	Art.12(4)	**Coordinated preparedness testing of entities**. For the purpose of supporting the coordinated testing of entities for their preparedness as referred to in Article 11, point (a)(i), of this Regulation, the Commission shall, after consulting with the NIS Cooperation Group, EU-CyCLONe and ENISA, identify the sectors or sub-sectors concerned from the list of sectors of high criticality shown in Annex 1 to Directive (EU) 2022/2555 for which a call for proposals to award grants may be issued. The participation of Member States in those calls for proposals is voluntary.	ACTIVITY 2
CSoA	Art.12(6)	**Coordinated preparedness testing of entities**. The NIS Cooperation Group, in cooperation with the Commission, the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') and ENISA, and, within the remit of its mandate, EU-CyCLONe, shall develop common risk scenarios and methodologies for the coordinated testing of preparedness referred to in Article 11 point (a)(i) and, where appropriate, for other preparedness actions referred to in point (a)(ii) of that Article.	ACTIVITY 2

CSoA	Art.6(4)	**Cooperation and information sharing within and between Cross-Border Cyber Hubs**. Information sharing as referred to in paragraph 1 between Cross-Border Cyber Hubs shall be ensured by a high level of interoperability. To support such interoperability, ENISA shall, in close consultation with the Commission, without undue delay and in any event by 5 February 2026, issue interoperability guidelines specifying in particular information-sharing formats and protocols taking into account international standards and best practices as well as the functioning of any established Cross-Border Cyber Hubs. Interoperability requirements provided for in the cooperation agreements of Cross-Border Cyber Hubs shall be based on the guidelines issued by ENISA.	ACTIVITY 4
CSoA	Art.9(4)	**Funding of the European Cybersecurity Alert System**. The ECCC shall prepare, at least every two years, a mapping of the tools, infrastructure or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, and their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. When preparing the mapping, the ECCC shall consult with the CSIRTs network, any existing Cross-Border Cyber Hubs, ENISA and the Commission.	ACTIVITY 4
CSoA	Art.12(6)	**Coordinated preparedness testing of entities**. The NIS Cooperation Group in cooperation with the Commission, the High Representative of the Union for Foreign Affairs and Security Policy, ENISA and, within the remit of its mandate, EU-CyCLONe, shall develop common risk scenarios and methodologies for the coordinated preparedness testing referred to in Article 11 point (a)(i) and, where appropriate, for other preparedness actions referred to in point (a)(ii) of that Article.	ACTIVITY 4
CSoA	Art.21(1)	**European Cybersecurity Incident Review Mechanism**. At the request of the Commission or EU-CyCLONe, ENISA shall, with the support of the CSIRTs network and with the approval of the Member States concerned, review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident and with the aim of drawing lessons learned to avoid or mitigate future incidents, ENISA shall deliver an incident review report to EU-CyCLONe, the CSIRTs network, the Member States concerned and the Commission to support them in carrying out their tasks, in particular the tasks set out in Articles 15 and 16 of Directive (EU) 2022/2555. Where an incident has an impact on a DEP-associated third country, ENISA shall provide the report to the Council. In such cases, the Commission shall provide the report to the High Representative.	ACTIVITY 5

CSoA	Art.21(2)	**European Cybersecurity Incident Review Mechanism**. To prepare the incident review report referred to in paragraph 1 of this Article, ENISA shall cooperate with and gather feedback from all relevant stakeholders, including representatives of Member States, the Commission, other relevant Union institutions, bodies, offices and agencies, industry, including managed security services providers and users of cybersecurity services. Where appropriate, ENISA shall, in cooperation with CSIRTs and, where relevant, the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555, also cooperate with entities affected by significant cybersecurity incidents or large-scale cybersecurity incidents. Consulted representatives shall disclose any potential conflicts of interest.	ACTIVITY 5
CSoA	Art.21(3)	**European Cybersecurity Incident Review Mechanism**. The incident review report referred to in paragraph 1 of this Article shall cover a review and analysis of the specific significant cybersecurity incident or large-scale cybersecurity incident, including the main causes, known exploitable vulnerabilities and lessons learned. ENISA shall ensure that the report complies with Union or national law concerning the protection of sensitive or classified information. If the relevant Member States or other users referred to in Article 14(3) that are affected by the incident so request, the data and information contained in the report shall be anonymised. It shall not include any details about actively exploited vulnerabilities that remain unpatched.	ACTIVITY 5
CSoA	Art.21(4)	**European Cybersecurity Incident Review Mechanism**. Where appropriate, the incident review report shall draw up recommendations to improve the Union's cyber posture and may include best practices and lessons learned from relevant stakeholders.	ACTIVITY 5
CSoA	Art.21(5)	**European Cybersecurity Incident Review Mechanism**. ENISA may issue a publicly available version of the incident review report. That version of the report shall include only reliable public information, or other reliable information with the consent of the Member States concerned and, as regards information relating to a user as referred to in Article 14(3) points (b) or (c), with the consent of that user.	ACTIVITY 5
CSoA	Art.10(4)	**Establishment of the Cybersecurity Emergency Mechanism**. The actions under the Cybersecurity Emergency Mechanism shall be implemented primarily through the ECCC in accordance with Regulation EU2021/887. However, actions implementing the EU Cybersecurity Reserve as referred to in Article 11 point (b) of this Regulation shall be implemented by the Commission and ENISA.	ACTIVITY 6

CSoA	Art.14(5)	**Establishment of the EU Cybersecurity Reserve**. Without prejudice to the Commission's overall responsibility for the implementation of the EU Cybersecurity Reserve referred to in paragraph 4 of this Article and subject to a contribution agreement as defined in Article 2 point (19) of Regulation (EU, Euratom) 2024/2509, the Commission shall entrust the operation and administration of the EU Cybersecurity Reserve in full or in part to ENISA. Aspects not entrusted to ENISA shall remain subject to direct management by the Commission.	ACTIVITY 6
CSoA	Art.14(6)	**Establishment of the EU Cybersecurity Reserve**. ENISA shall prepare, at least every two years, a mapping of the services needed by the users referred to in paragraph 3 points (a) and (b) of this Article. The mapping shall also include the availability of such services, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. In mapping that availability, ENISA shall assess the skills and capacity of the Union cybersecurity workforce relevant to the objectives of the EU Cybersecurity Reserve. When preparing the mapping, ENISA shall consult with the NIS Cooperation Group, EU-CyCLONe, the Commission and, where applicable, the Interinstitutional Cybersecurity Board established pursuant to Article 10 of Regulation (EU, Euratom) 2023/2841 (IICB). In mapping the availability of services, ENISA shall also consult relevant stakeholders in the cybersecurity industry, including managed security service providers. ENISA shall prepare a similar mapping, after informing the Council and after consulting with EU-CyCLONe, the Commission and, where relevant, the High Representative, to identify the needs of users referred to in paragraph 3 point (c) of this Article.	ACTIVITY 6
CSoA	Art.14(7)	**Establishment of the EU Cybersecurity Reserve**. The Commission is empowered to adopt delegated acts in accordance with Article 23 of the supplement to this Regulation by specifying the types and the number of response services required for the EU Cybersecurity Reserve. When preparing those delegated acts, the Commission shall take into account the mapping referred to in paragraph 6 of this Article and may exchange advice and cooperate with the NIS Cooperation Group and ENISA.	ACTIVITY 6
CSoA	Art.15(6)	**Requests for support from the EU Cybersecurity Reserve**. ENISA, in cooperation with the Commission and EU-CyCLONe, shall develop a template to facilitate the submission of requests for support from the EU Cybersecurity Reserve.	ACTIVITY 6

CSoA	Art.16(4)	**Implementation of the support from the EU Cybersecurity Reserve**. To prioritise requests, in the case of concurrent requests from users referred to in Article 14(3), the criteria referred to in paragraph 3 of this Article shall be taken into account, where relevant, without prejudice to the principle of sincere cooperation between Member States and Union institutions, bodies, offices and agencies. Where two or more requests are assessed as equal under those criteria, higher priority shall be given to requests from users in Member States. Where the operation and administration of the EU Cybersecurity Reserve has been entrusted in full or in part to ENISA pursuant to Article 14(5), ENISA and the Commission shall closely cooperate to prioritise requests in accordance with this paragraph.	ACTIVITY 6
CSoA	Art.16(6)	**Implementation of the support from the EU Cybersecurity Reserve**. The agreements referred to in paragraph 5 shall be based on templates prepared by ENISA, after consulting Member States and, where appropriate, other users of the EU Cybersecurity Reserve.	ACTIVITY 6
CSoA	Art.16(7)	**Implementation of the support from the EU Cybersecurity Reserve**. The Commission, ENISA and the users of the EU Cybersecurity Reserve shall bear no contractual liability for damage caused to third parties by the services provided in the framework of the implementation of the EU Cybersecurity Reserve.	ACTIVITY 6
CSoA	Art.16(9)a Art.16(9)b	**Implementation of the support from the EU Cybersecurity Reserve**. Within two months of the end of a term of support, users that have received support shall provide a summary report about the service provided, the results achieved and the lessons learned, to: the Commission, ENISA, the CSIRTs network and EU-CyCLONe in the case of users referred to in Article 14(3) point (a); (b) the Commission, ENISA and the IICB in the case of the users referred to in Article 14(3) point (b); (c) the Commission in the case of users referred to in Article 14(3) point (c).	ACTIVITY 6
CSoA	Art.16(10)	**Implementation of the support from the EU Cybersecurity Reserve**. Where the operation and administration of the EU Cybersecurity Reserve has been entrusted in full or in part to ENISA pursuant to Article 14(5) of this Regulation, ENISA shall report to and consult the Commission on a regular basis in that respect. In that context, ENISA shall immediately send to the Commission any requests it receives from users referred to in Article 14(3) point (c) of this Regulation and, where required for the purposes of prioritisation under this Article, any requests it has received from users referred to in Article 14(3) points (a) or (b), of this Regulation. The obligations in this paragraph shall be without prejudice to Article 14 of Regulation (EU) 2019/881.	ACTIVITY 6

CSoA	Art.19(2)	**Support to DEP-associated third countries**. Within three months of the conclusion of the agreement referred to in paragraph 1 and in any event prior to receiving any support from the EU Cybersecurity Reserve, a third country associated with the Digital Europe Programme (DEP) shall provide the Commission with information about its cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant cybersecurity incidents or large-scale cybersecurity incidents as well as information on responsible national entities, including computer security incident response teams or equivalent entities, their capabilities and the resources allocated to them. The DEP-associated third country shall provide updates of that information on a regular basis and at least once a year. The Commission shall provide the High Representative and ENISA with that information for the purposes of facilitating the application of paragraph 11.	ACTIVITY 6
CSoA	Art.19(11)	**Support to DEP-associated third countries**. Upon receipt of a request for support under this Article, the Commission shall immediately inform the Council. The Commission shall keep the Council informed of the assessment of the request. The Commission shall also cooperate with the High Representative about the requests received and the implementation of the support granted to DEP-associated third countries from the EU Cybersecurity Reserve. Additionally, the Commission shall also take into account any views provided by ENISA in respect of those requests.	ACTIVITY 6
CSoA	Art.22(1)b	**Amendments to Regulation EU2021/694**. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council. However, the EU Cybersecurity Reserve shall be implemented by the Commission and, in accordance with Article 14(6) of Regulation (EU) 2025/38, by ENISA.	ACTIVITY 6

CSoA	Art.22(4)	**Amendments to Regulation EU2021/694**. When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated to the Programme in accordance with Article 10 of this Regulation. The Commission and ENISA may also act as wholesalers, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By way of derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council (*5), a request from a single third country shall be sufficient to mandate the Commission or ENISA to act. When implementing procurement procedures for the EU Cybersecurity Reserve, the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of Union institutions, bodies, offices or agencies. The Commission and ENISA may also act as a wholesaler, by buying, stocking and reselling or donating supplies and services, including rentals, to Union institutions, bodies, offices or agencies. By way of derogation from Article 168(3) of Regulation (EU, Euratom) 2024/2509, a request from a single Union institution, body, office or agency shall be sufficient to mandate the Commission or ENISA to act.	ACTIVITY 6
CSoA	Art.19	**Amendments to Regulation (EU) 2021/694**. With regard to actions supporting mutual assistance as provided in Article 18 of Regulation (EU) 2025/38, the ECCC shall inform the Commission and ENISA about requests from Member States for direct grants without calls for proposals.	ACTIVITY 6
DEP	Art.6(2)	**Implementing actions under Specific Objective 3**. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council, with the exception of actions implementing the EU Cybersecurity Reserve which shall be implemented by the Commission and, in accordance with Article 12(6) of Regulation (EU) by ENISA.	ACTIVITY 6

DEP	Art.14(2)	**Procurement procedures**. When implementing procurement procedures for the EU Cybersecurity Reserve established by Article 12 of Regulation (EU) [insert reference to Cyber Solidarity Act], the Commission and ENISA may act as a central purchasing body to procure on behalf of or in the name of third countries associated with the programme in line with Article 10. The Commission and ENISA may also act as wholesalers, by buying, stocking and reselling or donating supplies and services, including rentals, to those third countries. By derogation from Article 169(3) of Regulation (EU) ..../.... [FR Recast], the request from a single third country is sufficient to mandate the Commission or ENISA to act.	ACTIVITY 6
DEP	Art.19	**Calls for proposals no needed**. For actions specified in Article 10(1) point (c) of Regulation (EU) ..../.... [Cyber Solidarity Act], the ECCC shall inform the Commission and ENISA about requests from Member States for direct grants without a call for proposals.	ACTIVITY 6
DGA	Art.29(1)	**European Data Innovation Board**. The Commission shall establish a European Data Innovation Board in the form of an expert group, consisting of representatives of the competent authorities for data intermediation services and the competent authorities for the registration of the data altruism organisations of all Member States, EDPB, the EDPS, ENISA, the Commission, the EU SME Envoy or a representative appointed by the network of SME envoys and other representatives of relevant bodies in specific sectors as well as bodies with specific expertise.	ACTIVITY 8
DORA	Art.15	**Further harmonisation of ICT risk management tools, methods, processes and policies**. The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop draft common regulatory technical standards.	ACTIVITY 2
DORA	Art.16(3)	**Simplified ICT risk management framework**. ESAs shall, through the Joint Committee, in consultation with ENISA, develop common draft regulatory technical standards.	ACTIVITY 2
DORA	Art.32(4)c	**Structure of the Oversight Framework**. The Oversight Forum shall be composed of the Executive Directors of ESA and one representative each from the Commission, from the ESRB, from ECB and from ENISA as observers.	ACTIVITY 2
DORA	Art.49(1)	**Financial cross-sector exercises, communication and cooperation**. The ESAs, through the Joint Committee and in collaboration with competent authorities, resolution authorities as referred to in Article 3 of Directive (EU) 2014/59, the ECB, the Single Resolution Board as regards information relating to entities falling under the scope of Regulation (EU) 2014/806, the ESRB and ENISA, as appropriate, may establish mechanisms to enable the sharing of effective practices across financial sectors to enhance situational awareness and identify common cyber vulnerabilities and risks across sectors.	ACTIVITY 2

DORA	Art.18(4)	**Classification of ICT-related incidents and cyber threats**. When developing the draft common regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2) as well as international standards, guidance and specifications developed and published by ENISA including, where appropriate, specifications for other economic sectors. For the purposes of applying the criteria set out in Article 4(2), the ESAs shall consider the need for microenterprises and small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly.	ACTIVITY 2
DORA	Art.18(3)	**Classification of ICT-related incidents and cyber threats**. The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft regulatory technical standards.	ACTIVITY 5
DORA	Art.19(7)	**Reporting of major ICT-related incidents and the voluntary notification of significant cyber threats**. Following receipt of information in accordance with paragraph 6, EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority, shall assess whether a major ICT-related incident is relevant for competent authorities in other Member States. Following that assessment, EBA, ESMA or EIOPA shall, as soon as possible, notify relevant competent authorities in those other Member States accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system.	ACTIVITY 5

DORA	Art.20	**Harmonisation of reporting content and templates**. The ESAs, through the Joint Committee, and in consultation with ENISA and the ECB, shall develop: (a) draft common regulatory technical standards in order to: (i) establish the content of the reports for major ICT-related incidents in order to reflect the criteria laid down in Article 18(1) and incorporate further elements, such as details for establishing the relevance of the reporting for other Member States and whether it constitutes a major operational or security payment-related incident; (ii) determine the time limits for the initial notification and for each report referred to in Article 19(4); (iii) establish the content of the notification for significant cyber threats. When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity and the nature, scale and complexity of its services, activities and operations, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, specificities of financial sectors, without prejudice to maintaining a consistent approach to ICT-related incident reporting pursuant to this Regulation and to Directive (EU) 2022/2555. The ESAs shall, as applicable, provide justification when deviating from the approaches taken in the context of that Directive. The ESAs shall also develop: (b) common draft technical implementation standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.	ACTIVITY 5
DORA	Art.21(1)	**Centralisation of reporting of major ICT-related incidents**. The ESAs, through the Joint Committee, and in consultation with the ECB and ENISA, shall prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for major ICT-related incident reporting by financial entities.	ACTIVITY 5
DORA	Art.34(3)	**Operational coordination between Lead Overseers**. The Lead Overseers may, on an ad-hoc basis, call on the ECB and ENISA to provide technical advice, share hands-on experience or join specific coordination meetings of the JON.	ACTIVITY 5
ECCC	Art.3(2)	**Mission of the Competence Centre and the Network**. The Competence Centre and the Network shall undertake their tasks in collaboration with ENISA and the Community, as appropriate.	ACTIVITY 8

ECCC	Art.5(2)b&c	**Tasks of the Competence Centre.** The Competence Centre must carry out its agenda and multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and the Digital Europe Programme. It must ensure synergies between and cooperation with relevant Union institutions, bodies, offices and agencies, in particular ENISA, while avoiding any duplication of activities with those Union institutions, bodies, offices and agencies.	ACTIVITY 8
ECCC	Art.7(1)g	**Tasks of the national coordination centres**. Without prejudice to the competences of Member States in education and taking into account the relevant tasks of ENISA, national coordination centres must engage with national authorities regarding possible contributions to promoting and disseminating cybersecurity educational programmes.	ACTIVITY 8
ECCC	Art.8	**The Cybersecurity Competence Community**. The Community shall consist of industry, including SMEs, academic and research organisations, other relevant civil society associations as well as, as appropriate, relevant European Standardisation Organisations, public entities and other entities dealing with cybersecurity operational and technical matters and, where relevant, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges. The Community shall bring together the main stakeholders with regard to cybersecurity technological, industrial, academic and research capacities in the Union. It shall involve national coordination centres, European Digital Innovation Hubs where relevant, as well as Union institutions, bodies, offices and agencies with relevant expertise, such as ENISA.	ACTIVITY 8
ECCC	Art.10(1)	**Cooperation of the Competence Centre with other Union institutions, bodies, offices and agencies and international organisations**. To ensure consistency and complementarity while avoiding any duplication of effort, the Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies, including ENISA, the European External Action Service, the Directorate-General Joint Research Centre of the Commission, the European Research Executive Agency, the European Research Council Executive Agency and the European Health and Digital Executive Agency established by Commission Implementing Decision (EU) 2021/173(13), relevant European Digital Innovation Hubs, the European Cybercrime Centre at the European Union Agency for Law Enforcement Cooperation established by Regulation (EU) 2016/794 of the European Parliament and of the Council(14), the European Defence Agency in relation to the tasks set out in Article 5 of this Regulation and other relevant Union entities.	ACTIVITY 8

ECCC	Art.13(4)	**Tasks of the Governing Board**. Regarding the decisions set out in points (a), (b) and (c) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, in accordance with the rules of procedure of the Governing Board.	ACTIVITY 8
ECCC	Art.18(5)	**Strategic Advisory Group**. Representatives of the Commission and of other Union institutions, bodies, offices and agencies, in particular ENISA, may be invited by the Strategic Advisory Group to participate in and support its work.	ACTIVITY 8
ECCC	Art.12(7)	**Composition of the Governing Board**. A representative from ENISA shall be a permanent observer at the Governing Board. The Governing Board may invite a representative from the Strategic Advisory Group to attend its meetings.	ACTIVITY 8
eIDAS2	Art.46(c)(2)	**Single points of contact**. Each single point of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other competent authorities within its Member States.	ACTIVITY 8
eIDAS2	Art.46(e)(4)	**The European Digital Identity Cooperation Group**. ENISA shall be invited to participate as an observer in the workings of the Cooperation Group when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity certificates or standards are addressed.	ACTIVITY 8
eIDAS2	Art.47(e)(5)(c)(iv)	**The European Digital Identity Cooperation Group**. With ENISA's support, the European Digital Identity Cooperation Group will exchange views, best practices and information on relevant aspects of cybersecurity concerning European Digital Identity Wallets, electronic identification schemes and trust services.	ACTIVITY 8
NCSS (Electricity Network Code)	Art.4(2)	**Competent authority**. Member States shall, without delay, notify the Commission, Agency for the Cooperation of Energy Regulators (ACER), ENISA, the NIS Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and the Electricity Coordination Group set up under Article 1 of the Commission Decision of 15 November 2012 (17) and communicate to them the name and the contact details of their designated competent authority pursuant to paragraph 1 of this article and any subsequent changes thereto.	ACTIVITY 2

NCSS	Art.4(3)	**Competent authority**. The competent authority shall communicate the name, contact details, assigned tasks and any subsequent changes thereto of the authorities to whom a task has been delegated to the Commission, to ACER, to the Electricity Coordination Group, to ENISA and to the NIS Cooperation Group.	ACTIVITY 2
NCSS	Art.8(3)	**Terms and conditions or methodologies or plans**. ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 6(2).	ACTIVITY 2
NCSS	Art.9 (1)	**Consultation**. TSOs with the assistance of the ENTSO for Electricity and in cooperation with the EU Distribution System Operators (DSO), shall consult stakeholders, including ACER, ENISA and the competent authority in each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 6(2) and for plans referred to in Article 6(3). The consultation shall last for a period of not less than one month.	ACTIVITY 2
NCSS	Art.12 (1)	**Monitoring**. In carrying out its monitoring duties, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group and the NIS Cooperation Group about the implementation of this Regulation.	ACTIVITY 2
NCSS	Art.12 (3)	**Monitoring**. By 13 June 2025, ACER, in cooperation with ENISA and after consultation with the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for its monitoring purposes as well as the process and frequency of its collection, based on performance indicators defined in accordance with paragraph 5.	ACTIVITY 2
NCSS	Art.12 (5)	**Monitoring**. ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are related to the cybersecurity aspects of cross-border electricity flows.	ACTIVITY 2
NCSS	Art.13 (1)	**Benchmarking**. By 13 June 2025 ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide.	ACTIVITY 2
NCSS	Art.13 (5)	**Benchmarking**. Without prejudice to the confidentiality requirements in Article 47 and to the need to protect the security of entities subject to the provisions of this Regulation, the benchmarking analysis referenced in paragraphs 2 and 3 of this Article shall be shared with all NRAs, all competent authorities, ACER, ENISA and the Commission.	ACTIVITY 2
NCSS	Art.16 (1) n	**Cooperation between the ENTSO for Electricity and the EU DSO Entity**. The ENTSO for Electricity and the EU DSO Entity must cooperate in the development of guidelines for the implementation of this Regulation in consultation with ACER and ENISA.	ACTIVITY 2

NCSS	Art.16 (3)	**Cooperation between the ENTSO for Electricity and the EU DSO Entity**. The ENTSO for Electricity and the EU DSO entity shall regularly inform ACER, ENISA, the NIS Cooperation Group and the Electricity Coordination Group on the progress in implementing the Union-wide and regional cybersecurity risk assessments pursuant to Articles 19 and 21.	ACTIVITY 2
NCSS	Art.17 (2)	**Cooperation between ACER and the competent authorities**. The cooperation between ACER, ENISA and each competent authority may take the form of a cybersecurity risk monitoring body.	ACTIVITY 2
NCSS	Art.19 (5)	**Union-wide cybersecurity risk assessment**. Within three months of the receipt of ACER's opinion, the ENTSO for Electricity, in cooperation with the EU DSO entity shall notify the final Union-wide cybersecurity risk assessment report to ACER, the Commission, ENISA and the competent authorities.	ACTIVITY 2
NCSS	Art.34(1)	**Mapping matrix for electricity cybersecurity controls against standards**. Within seven months of submitting the first draft of a Union-wide cybersecurity risk assessment report pursuant to Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity and in cooperation with the EU DSO entity and in consultation with ENISA, shall develop a proposal for a matrix to map the controls set out in Article 28(1) points (a) and (b) against selected European and international standards as well as relevant technical specifications ('the mapping matrix').	ACTIVITY 2
NCSS	Art.34(3)	**Mapping matrix for electricity cybersecurity controls against standards**. Within six months of drawing up each regional cybersecurity risk assessment report pursuant to Article 21(2), the TSOs, with the assistance of the ENTSO for Electricity and in cooperation with the EU DSO Entity and in consultation with ENISA, shall propose an amendment to the competent authority for the mapping matrix.	ACTIVITY 2
NCSS	Art.36(2)	**Guidance on the use of European cybersecurity certification schemes for the procurement of ICT products, ICT services and ICT processes**. The TSOs, with the assistance of the ENTSO for Electricity and in cooperation with the EU DSO entity shall closely cooperate with ENISA in providing the sector-specific guidance included in non-binding cybersecurity procurement recommendations pursuant to paragraph 1.	ACTIVITY 2
NCSS	Art.38(2)	**CSOC capabilities**. Each high-impact and critical-impact entity shall establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), CSOC capabilities. ENISA may issue non-binding guidance on establishing such capabilities or subcontract the service to MSSPs, as part of the task defined in Article 6(2) of Regulation (EU) 2019/881.	ACTIVITY 2

NCSS	Art.41(1)	**Cybersecurity crisis management and response plans**. Within 24 months of the notification to ACER of the Union-wide risk assessment report, ACER shall in close cooperation with ENISA, the ENTSO for Electricity, the EU DSO entity, CS-NCAs, competent authorities, RP-NCAs, the NRAs and the NIS national cyber crisis management authorities, develop a Union-level cybersecurity crisis management and response plan for the electricity sector.	ACTIVITY 2
NCSS	Art.42(1)	**Cybersecurity early alert capabilities for the electricity sector**. The competent authorities shall cooperate with ENISA to develop Electricity Cybersecurity Early Alert Capabilities (ECEAC) as part of their assistance to Member States pursuant to Articles 6(2) and (7) of Regulation (EU) 2019/881.	ACTIVITY 2
NCSS	Art.42(2) c	**Cybersecurity early alert capabilities for the electricity sector**. ENISA needs to assess the information to which it has access in order to identify cyber risk conditions and relevant indicators for certain aspects of cross-border electricity flows.	ACTIVITY 2
NCSS	Art.47(7)	**Confidentiality of information. ACER, after consulting with ENISA and all competent authorities**, ENTSO for Electricity and the EU-DSO Entity, shall by 13 June 2025 issue guidelines addressing mechanisms for all entities listed in Article 2(1) to exchange information and, in particular, envisaged communication flows as well as methods to anonymise and to aggregate information for the purposes of the implementation of this Article.	ACTIVITY 2
NCSS	Art.43(5)	**Cybersecurity exercises at entity and Member State levels**. By 31 December 2026, and every three years thereafter the ENTSO for Electricity, in cooperation with the EU DSO entity, shall make available an exercise scenario template to perform cybersecurity exercises at the level of entities and Member States referred to in paragraphs 1. This template shall take into account the results of the most recently performed cybersecurity risk assessment at the entity level and at the level of Member States and shall include key success criteria. The ENTSO for Electricity and the EU DSO entity shall involve ACER and ENISA in the development of such a template.	ACTIVITY 3
NCSS	Art.44(2)	**Regional or cross-regional cybersecurity exercises**. ENISA shall support the ENTSO for Electricity and the EU DSO entity in the preparation and organisation of cybersecurity exercises at regional or at cross-regional levels.	ACTIVITY 3
NCSS	Art.44(6)	**Regional or cross-regional cybersecurity exercises**. The ENTSO for Electricity shall consult the Commission and may seek advice from ACER, ENISA and the Joint Research Centre on the organisation and execution of the regional and cross-regional cybersecurity exercises.	ACTIVITY 3

NCSS	Art.45(2)	**Outcome of cybersecurity exercises at entity, Member State, regional or cross-regional levels**. The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1), with the advice of ENISA if requested by them, and pursuant to Article 7(5) of Regulation (EU) 2019/881, shall analyse and finalise the relevant cybersecurity exercise through a report summarising the lessons learned, addressed to all participants.	ACTIVITY 3
NCSS	Art.42(3)	**Cybersecurity early alert capabilities for the electricity sector**. The CSIRTs shall disseminate the information received from ENISA to the entities concerned without delay, within their tasks defined in Article 11(3) point (b) of Directive (EU) 2022/2555.	ACTIVITY 4
NCSS	Art.42(4)	**Cybersecurity early alert capabilities for the electricity sector**. ACER shall monitor the effectiveness of the ECEAC. ENISA shall assist ACER by providing all necessary information, pursuant to Articles 6(2) and 7(1) of Regulation (EU) 2019/881.	ACTIVITY 4
NCSS	Art.37(1)(g)	**Rules on information sharing**. If a competent authority receives information related to a reportable cyberattack, that competent authority shall share a summary report with ENISA, after anonymisation and the removal of business secrets, on the cyberattack.	ACTIVITY 5
NCSS	Art.37(2)(a)	**Rules on information sharing**. If a CSIRT becomes aware of an unpatched vulnerability that is being actively exploited, it shall share it with ENISA via an appropriate secure channel for information exchange without delay, unless otherwise specified in another Union law.	ACTIVITY 5
NCSS	Art.37(8)	**Rules on information sharing**. The TSOs, with the assistance of the ENTSO for Electricity and in cooperation with the EU DSO entity, shall develop a methodology for a cyberattack classification scale by 13 June 2025. The TSOs, with the assistance of the ENTSO for Electricity and the EU DSO entity, may request the competent authorities to consult ENISA and their competent authorities responsible for cybersecurity for assistance in the development of such a classification scale.	ACTIVITY 5
NCSS	Art.37(11)(a)	**Feasibility study to assess the possibility and the financial costs necessary to develop a common tool enabling all entities to share information with relevant national authorities**. The ENTSO for Electricity in cooperation with the EU DSO entity shall consult ENISA and the NIS Cooperation Group, the national single points of contact and the representatives of main stakeholders when assessing the feasibility of developing a common tool enabling all entities to share information with relevant national authorities.	ACTIVITY 5

NIS2	Art.7(4)	**National cybersecurity strategy**. Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or an update for a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive.	ACTIVITY 1
NIS2	Art.18(1)*	**Report on the state of cybersecurity in the Union**. ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine readable data.	ACTIVITY 1
NIS2	Art.18(1)d*	**Report on the state of cybersecurity in the Union**. The report shall inter alia include an aggregated assessment of the outcome of the peer reviews referred to in Article 19.	ACTIVITY 1
NIS2	Art.18(1)e*	**Report on the state of cybersecurity in the Union**. The report shall inter alia include an aggregated assessment of the extent to which the national cybersecurity strategies of Member States are aligned.	ACTIVITY 1
NIS2	Art.18(2)*	**Report on the state of cybersecurity in the Union**. The report shall inter alia include in particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union.	ACTIVITY 1
NIS2	Art.18(3)	**Report on the state of cybersecurity in the Union**. ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1 point (e).	ACTIVITY 1
NIS2	Art.19(1)	**Peer reviews**. The Cooperation Group shall by 17 January 2025 establish, with the assistance of the Commission and ENISA and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity as well as enhancing the cybersecurity capabilities of Member States and the policies necessary to implement this Directive.	ACTIVITY 1
NIS2	Art.19(2)	**Peer reviews**. The Commission and ENISA shall participate as observers in the peer reviews.	ACTIVITY 1
NIS2	Art.19(5)	**Peer reviews: self-assessment**. The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for self-assessment by Member States.	ACTIVITY 1

NIS2	Art.19(6)	**Peer reviews: designated cybersecurity experts**. The Cooperation Group, in collaboration with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts.	ACTIVITY 1
NIS2	Art.14(4)q	**Cooperation Group**. The Cooperation Group shall establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1) as well as lay down the self-assessment methodology for Member States in accordance with Article 19(5) with the assistance of the Commission and ENISA and, in cooperation with the Commission and ENISA, shall develop codes of conduct underpinning the working methods of designated cybersecurity experts in accordance with Article 19(6).	ACTIVITY 1
NIS2	Art.19(8)	**Peer reviews**. Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of particular cybersecurity experts on substantiated grounds communicated to the designating Member State.	ACTIVITY 1
NIS2	Art.3(4)	**Essential and important entities**. The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall without undue delay provide guidelines and templates regarding the obligations laid down in this paragraph.	ACTIVITY 2
NIS2	Art.8(4)	**Competent authorities and single points of contact**. Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within that Member State.	ACTIVITY 2
NIS2	Art.18(1)e*	**Report on the state of cybersecurity in the Union**. The report shall inter alia include an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level.	ACTIVITY 2
NIS2	Art.21(5)	**Cybersecurity risk management measures**. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on draft implementing acts in accordance with Article 14(4) point (e).	ACTIVITY 2

NIS2	Art.22(1)**	**Union level coordinated assessments of security risks of critical supply chains**. The Cooperation Group, in collaboration with the Commission and ENISA, may carry out coordinated assessments of security risks of specific critical supply chains for ICT services, ICT systems or ICT products, taking into account technical and, where relevant, non-technical risk factors.	ACTIVITY 2
NIS2	Art.22(2)**	**Union level coordinated assessments of security risks of critical supply chains**. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated assessments of security risks referred to in paragraph 1.	ACTIVITY 2
NIS2	Art.27(1)	**Registry of entities**. ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.	ACTIVITY 2
NIS2	Art.27(4)	**Registry of entities**. Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2 point (f), the single point of contact of the Member State concerned shall, without undue delay, be forwarded to ENISA.	ACTIVITY 2
NIS2	Art.29(5)	**Cybersecurity information-sharing arrangements**. ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.	ACTIVITY 2
NIS2	Art.18(1)b*	**Report on the state of cybersecurity in the Union**. The report shall inter alia include an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union.	ACTIVITY 3
NIS2	Art.18(1)c*	**Report on the state of cybersecurity in the Union**. The report shall inter alia include an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises.	ACTIVITY 3
NIS2	Art.10(10)	**Computer security incident response teams (CSIRTs)**. Member States may request the assistance of ENISA in developing their CSIRTs.	ACTIVITY 4

NIS2	Art.12(2)	**Coordinated vulnerability disclosure and a European vulnerability database**. ENISA shall develop and maintain, after consulting with the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided with access to the information about the vulnerabilities contained in the European vulnerability database.	ACTIVITY 4
NIS2	Art.15(2)	**CSIRTs network**. ENISA shall provide the secretariat and shall actively provide assistance for cooperation among the CSIRTs.	ACTIVITY 4
NIS2	Art.16(2)	**European cyber crisis liaison organisation network (EU-CyCLONe)**. ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchanges of information.	ACTIVITY 4
NIS2	Art.14(3)	**Cooperation Group**. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA.	ACTIVITY 4
NIS2	Art.18(1)a*	**Report on the state of cybersecurity in the Union**. The report shall inter alia include a Union-level assessment of cybersecurity risks, taking into account the cyber threat landscape.	ACTIVITY 5
NIS2	Art.18(2)*	**Report on the state of cybersecurity in the Union**. The report shall include inter alia a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.	ACTIVITY 5
NIS2	Art.23(6)	**Reporting obligations**. Where appropriate, and in particular where a significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform without undue delay other affected Member States and ENISA of the significant incident.	ACTIVITY 5

NIS2	Art.23(9)	**Reporting obligations**. Every three months the single point of contact shall submit to ENISA a summary report, including anonymised and aggregated data on significant incidents, other incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications sent every six months.	ACTIVITY 5
NIS2	Art.37(1)	**Mutual assistance**. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA.	ACTIVITY 6
NIS2	Art.24(3)	**Use of European cybersecurity certification schemes**. Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.	ACTIVITY 7
NIS2	Art.22(1)**	**Union level coordinated assessments of security risks of critical supply chains**. The Cooperation Group, in collaboration with the Commission and ENISA, may carry out coordinated assessments of security risks relating to the supply chains of specific critical ICT services, ICT systems or ICT products, taking into account technical and, where relevant, non-technical risk factors.	ACTIVITY 8
NIS2	Art.22(2)**	**Union level coordinated assessments of security risk of critical supply chains**. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated assessment of security risks referred to in paragraph 1.	ACTIVITY 8
NIS2	Art.25(2)	**Standardisation: technical specifications relevant to the security of network and information systems**. ENISA, in cooperation with Member States and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.	ACTIVITY 8

REU (Regulation laying down measures for a high common level of cybersecurity at the Institutions)	Art.21(8)*	**Reporting obligations**. The summary report shall constitute an input to the biennial report on the state of cybersecurity in the Union adopted pursuant to Article 18 of Directive (EU) 2022/2555.	ACTIVITY 1
REU	Art.13(7)	**CERT-EU mission and tasks**. CERT-EU shall organise and may participate in cybersecurity exercises or recommend participation in existing exercises, where applicable, in close cooperation with ENISA, to test the level of cybersecurity of Union entities.	ACTIVITY 3
REU	Art.13(5)	**CERT-EU mission and tasks**. Within its competence, CERT-EU shall engage in structured cooperation with ENISA on capacity building, operational cooperation and long-term strategic analyses of cyber threats in accordance with Regulation (EU) 2019/881.	ACTIVITY 4
REU	Art.22(2)	**Incident response coordination and cooperation**. CERT-EU, where relevant in close cooperation with ENISA, shall facilitate coordination among Union entities on responses to incidents.	ACTIVITY 4
REU	Art.23(1)	**Management of major incidents**. In order to support at operational level the coordinated management of major incidents affecting Union entities and to contribute to the regular exchange of relevant information between Union entities and Member States, the IICB shall, pursuant to Article 11 point (q), establish a cyber crisis management plan based on the activities referred to in Article 22(2) in close collaboration with CERT-EU and ENISA.	ACTIVITY 4
REU	Art.13(3)e	**CERT-EU mission and tasks**. CERT-EU shall carry out the following tasks to assist Union entities in contributing to the Union's cyber situational awareness in close cooperation with ENISA.	ACTIVITY 5
REU	Art.21(8)*	**Reporting obligations**. Every three months CERT-EU shall submit to the IICB, ENISA, the EU INTCEN and the CSIRTs network a summary report including anonymised and aggregated data on significant incidents, other incidents, cyber threats, near misses and vulnerabilities pursuant to Article 20 and significant incidents notified pursuant to paragraph 2 of this Article.	ACTIVITY 5
REU	Art.22	**Incident response coordination and cooperation**. CERT-EU, in close cooperation with ENISA, shall support Union entities regarding situational awareness of incidents, cyber threats, vulnerabilities and near misses as well as sharing relevant developments in the field of cybersecurity.	ACTIVITY 5

REU	Art.5(1)	**Implementation of measures**. By 8 September 2024 the Interinstitutional Cybersecurity Board (IICB) established pursuant to Article 10 shall, after consulting ENISA and after receiving guidance from CERT-EU, issue guidelines to Union entities for the purpose of carrying out an initial cybersecurity review and establishing the internal governance of a framework for cybersecurity risk management and control pursuant to Article 6, carry out assessments of cybersecurity maturity pursuant to Article 7, take measures to manage cybersecurity risk pursuant to Article 8 and adopt the cybersecurity plan pursuant to Article 9.	EDO
REU	Art.11(o)	**Tasks of the IICB**. When exercising its responsibilities, the IICB shall, in particular, facilitate the establishment of an informal group of local cybersecurity officers in Union entities, supported by ENISA, with the aim of exchanging best practices and information in relation to the implementation of this Regulation.	EDO
Blueprint	Art 14	EU-CyCLONe, with the support of ENISA as its secretariat, should maintain an up-to-date list of national cyber crisis management authorities with contact details of EU-CyCLONe officers and executives, and make it available to EU-CyCLONe members.	ACTIVITY 4
Blueprint	Art 18	ENISA is the Union agency carrying out the tasks assigned under Regulation (EU) 2019/881 of the European Parliament and of the Council (11) for the purposes of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States and Union institutions, bodies and agencies. ENISA provides, among others, the secretariat for the CSIRTs network and EU-CyCLONe, situational awareness services, and assists Member States by regularly organising cybersecurity exercises at Union level. In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2024/2847 of the European Parliament and of the Council (12), ENISA receives information about significant cross-border incidents and actively exploited vulnerabilities and incidents affecting digital products.	ACTIVITY 4
Blueprint	Art 25	In order to enhance shared situational awareness and to facilitate assessment of the EU impact, EU-CyCLONe and the CSIRTs network with support of ENISA should use internally agreed reporting mechanism to produce an EU overview of technical and operational activities based on the information gathered at the national level	ACTIVITY 4

Blueprint	Art 26	EU-CyCLONe and the CSIRTs network should: (a)cooperate to improve information sharing between the technical and operational level and situational awareness as a whole; (b)continue to build a climate of trust between their members and between the networks; (c)make full use of the available tools for information sharing, with support of ENISA, reflect on how to improve these tools and ensure interoperability between the networks.	ACTIVITY 4
Blueprint	Art 28	ENISA, as the secretariat for the CSIRTs network and EU-CyCLONe, has a central role in supporting Member States and Union institutions, bodies and agencies to achieve a common EU situational awareness on the technical and operational level to support preparing for large-scale cybersecurity incidents and crises.	
Blueprint	Art 29	In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2019/881, Member States and relevant Union entities should coordinate with the private sector, including open-source communities and manufacturers, to improve information sharing. In particular ENISA should utilise its partnership programme in this regard. Additionally, Member States and relevant Union entities could also build on existing Information Sharing and Analysis Centres ('ISACs') at EU and national levels, to enhance cybersecurity capacity and to respond to cybersecurity incidents, including through joint meetings of the private sector with EU-CyCLONe or the CSIRTs network.	ACTIVITY 4
Blueprint	Art 30	To enhance information sharing within and between the networks, and to clarify mutual expectations for such sharing, EU-CyCLONe should, with the support of ENISA as secretariat and after consulting the CSIRTs network and the NIS Cooperation Group, within 24 months from adoption of this Recommendation, agree on a common aligned taxonomy of incident severity levels. This taxonomy should enable a comparison of the severity of incidents across Member States by considering the impact on service delivery, the number of affected entities and their respective relevance, the impact on other services and infrastructure, as well as the monetary, reputational and political damage inflicted. It should build on relevant existing scales or taxonomies, such as Reference Incident Classification Taxonomy.	ACTIVITY 4

Blueprint	Art 36	In accordance with Directive (EU) 2022/2555 and Regulation (EU) 2024/2847, ENISA receives information about significant cross-border incidents and actively exploited vulnerabilities and incidents affecting digital products. ENISA acting as the secretariat should advise the CSIRTs network and EU-CyCLONe with the objective of supporting the networks in determining whether further actions should be taken and to contribute to the shared situational awareness.	ACTIVITY 4
Blueprint	Art 40	The Commission, in coordination with the High Representative, supported by ENISA, after consulting EU-CyCLONe and the CSIRTs network, should compile an efficient annual rolling programme of cyber exercises to prepare for cyber crises and to enhance organisational efficiency. The rolling programme of cyber exercises should take account of exercises of the UCPM and other Union-level crisis response mechanisms exercises, including the exercise outlined in the EU Critical Infrastructure Blueprint. The first rolling programme should be developed within 12 months after the adoption of the Cyber Blueprint, with subsequent programmes to be completed by 31 March of each year. The rolling programme should be submitted to the Council for information.	ACTIVITY 4
Blueprint	Art 42	ENISA, in its role of secretariat of the CSIRTs network and EU-CyCLONe, should ensure the systematic collection of lessons learnt from exercises, as well as the identification and proposing ways of implementation of resulting actions, to guarantee their effective execution and positive impact on the EU common resilience, including respective SOPs.	ACTIVITY 4
Blueprint	Art 44	The NIS Cooperation Group should invite the CSIRTs network, EU-CyCLONe and ENISA to present lessons learnt from the exercises, as well as the identification and proposed way of implementation of resulting actions.	ACTIVITY 4
Blueprint	Art 45	The Council may invite the chairs of the CSIRTs network, EU-CyCLONe, the NIS Cooperation Group and ENISA, to present how lessons learnt from the exercises were implemented.	ACTIVITY 4
Blueprint	Art 46	ENISA, in cooperation with the Commission and the High Representative, is invited to organise an exercise to test Cyber Blueprint during the next Cyber Europe exercise. The exercise should involve all relevant actors, including the political level. ENISA is invited to coordinate with the Presidency of the Council of the European Union the involvement of the political level. The exercise may also include the private sector and NATO.	ACTIVITY 4

Blueprint	Art 55	In the event of a large-scale cybersecurity incident or a cyber crisis, all actors and networks should respond in close coordination as follows: (a)at the technical level: i.The affected Member States and their CSIRTs should cooperate with the affected entities to respond to incidents and provide assistance, where applicable; ii.The CSIRTs should cooperate through the CSIRTs network to share relevant technical information about the incident; the CSIRTs cooperate in their efforts to analyse the available technical artefacts and other technical information related to the incident with a view of determining the cause and possible technical mitigation measures; iii.When a CSIRT or a Member State's cyber crisis management authority becomes aware of a significant incident, they are encouraged to share within the CSIRTs network or EU-CyCLONe. iv.The CSIRTs network, with the support of ENISA, should prepare an aggregation of national reports provided by CSIRTs, which should be presented to EU-CyCLONe;	ACTIVITY 4
Blueprint	Art 60	For the purposes of preparing for large-scale cybersecurity incidents and cyber crises, Member States and, as appropriate, the Commission and CERT-EU, are invited to exchange on their communication efforts within EU-CyCLONe and the CSIRTs network, including best practices, such as advisories or awareness raising campaigns. ENISA should provide tools supporting such an exchange and ensuring an easy access	ACTIVITY 4
Blueprint	Art 74	A comprehensive list of lessons learnt from cyber crises or managed cybersecurity incidents in the past and best practices should be provided by EU-CyCLONe to the CSIRTs network, the NIS Cooperation Group, and the Council. ENISA should ensure that these lessons learnt are properly reflected in future preparedness activities and when considering the planning of future exercises.	ACTIVITY 4
Blueprint	Art 80	EU-CyCLONe, in cooperation with the CSIRT network and other main actors in the EU Cyber Crisis Management Ecosystem, supported by ENISA, should develop, within one year following the publication of the Recommendation, detailed process flow diagrams outlining the information flows between relevant actors, decision-making processes and reports developed during the management of large-scale cybersecurity incident or cyber crisis as described in this Recommendation. The flow diagrams should cover different cooperation modes and layers. They should be updated when necessary.	ACTIVITY 4

Legislative Acts, Regulations and Links

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

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

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

CSOA: Cybersolidarity Act - 2025/38 15.1.2025 REGULATION (EU) 2025/38 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) DEP: Digital Europe Programme - Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance) https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

DEP: Digital Europe Programme - Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision EU2015/2240

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

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

AIA: AI Act - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689)

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

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

eIDAS 2: Regulation EU2024/1183 amending Regulation (EU) 2014/910 as regards establishing the European Digital Identity Framework (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183)

DGA: Data Governance Act: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R0868)

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

ANNEX 16
CORPORATE STRATEGY GOALS AND INDICATORS

The table below highlights the responsible activity for each objective contained in the Corporate Strategy including the key goals and ways to measure the associated Key Performance Indicators (KPIs).

STRATEGIC DIMENSION	OBJECTIVES	ACTIVITIES 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 at the beginning of year n) by more than 5% according to annual internal procedures. 95% of Agency's staffing posts (TA, CA, SNE) are filled by the end of year according to annual recruitment results. Vacant staff posts are filled in less than 300 days according to annual recruitment results. All assignments of staff are reviewed regularly every three years according to the Agency's annual internal procedures. Aggregate loss of FTEs across the Agency due to absences (excluding long-term sick leave) is less than three FTEs annually according to annual internal process.

	Efficient talent acquisition, development and retention	Activity 11	The 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 the established competencies described in the annual recruitment process. The Agency's proficiency levels across target competencies have increased over the set period according to the results of annual appraisal exercises. 50% of the Agency's needs for its established workforce 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. A high level of staff satisfaction with the learning opportunities offered and knowledge sharing options according to the biennial staff satisfaction survey. A 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 the level of psychological safety according to the annual staff satisfaction survey. High aggregate staff satisfaction with workspace and related services according to the biennial staff satisfaction survey. The Agency obtains the EU Agency's Network Certificate of Excellence in Diversity and Inclusion by the end of 2025 according to an 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 the annual staff satisfaction survey. Staff stress level is decreasing from 2022 levels and is sustained at low levels after 2025 according to the annual staff satisfaction survey.

Service centric organisation	Ensure efficient corporate services	Activities 9 and 11	High level of satisfaction with essential corporate support services found through an annual MT survey. High level of 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 outside the Agency with other Union Entities (under SLAs, MoUs or other arrangements) found through an annual internal procedure
	Introduce digital solutions that maximise synergies and collaboration within the Agency	Activities 9 and 11	Implement (replace or develop) at least five user-centred, cloud-based, corporate solutions or tools fit for purpose and in line with ENISA's IT strategy and relevant business needs by Q4 2025. Limited disruption of continuity of services across all corporate support service areas measured by an 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 (Standard Operating Procedures 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	Activities 9 & 11	At least three SLAs signed and in operation with Union entities covering ENISA's operational services with additional resourcing from beneficiaries by 2025.

Sustainable organisation	Ensure ENISA is climate neutral by 2030	Activity 9	Acquire an Eco-Management and Audit Scheme (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 of 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 by at least 40% by 2029, by installing solar panels on the non-classified part of the building or procure a green building for the Agency by then. Offset all residual emissions generated through ENISA operations from 2024 onwards.
	Promote and enhance ecological sustainability across all the Agency's operations	Activities 9 and 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	Activities 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 be in a position to handle EUCI at the level of SECRET UE/EU SECRET and be accredited as being able to do so by Q4 2024. 20% of the total IT budget to be allocated to information security 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.

Notes

Notes

TP-01-26-001-EN-N

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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union