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

DECISION No MB/2023/10
OF THE MANAGEMENT BOARD
OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

adopting the Single Programming Document (SPD) 2024-2026, the statement of estimates for 2024 and the establishment plan for 2024

THE MANAGEMENT BOARD OF ENISA,

Having regard to

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)1, in particular Article 15.1.(c), Article 24.3., Article 24.4., and Article 29.7;
- Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council;
- Commission Opinion C(2023) 7474 on the draft Single Programming Document for 2024 – 2026 of ENISA dated 30.10.2023;
- Commission Communication C(2014) 9641 final, on the guidelines for programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies dated 16.12.2014;

Whereas:

1. The Single Programming Document 2024-2026 should be adopted by the Management Board by 30 November 2023.
2. The Single Programming Document 2024 -2026 was scrutinised by the Executive Board on 19 October 2023.
3. The Single Programming Document of the Agency should be forwarded to the Member States, the European Parliament, the Council and the Commission following adoption;

HAS DECIDED TO ADOPT THE FOLLOWING DECISION

Article 1

The Single Programming Document 2024-2026, including the Annual Cooperation Programme with CERT-EU for 2024 is adopted as set out in the Annex 1 of this decision.

[1] *OJ L 151, 7.6.2019, p. 15–69*

Article 2

The statement of estimates of revenue and expenditure for the financial year 2024 and the establishment plan 2024 is adopted as set-out in Annex 2 and Annex 3 of this decision. They shall become final following the definitive adoption of the general budget of the Union for the financial year 2024.

Article 3

Where necessary, the Management Board shall adjust ENISAs Single Programming Document 2024-2026 and ENISA's budget and the establishment plan in accordance with the general budget of the Union for the financial year 2024.

Article 4

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

Done in Athens, 16 November 2023.

On behalf of the Management Board,

[signed]

Chair of the Management Board of ENISA

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2024-2026

Including Multiannual planning,
Work programme 2024 and
Multiannual staff planning

VERSION: DRAFT V.3.2

TABLE OF CONTENTS

LIST OF ACRONYMS

ABAC	Accruals-based accounting
ACER	Agency for the Cooperation of Energy Regulators
AD	Administrator
AST	Assistant
BEREC	Body of European Regulators for Electronic Communications
CA	Contract agenda
CAB	Conformity Assessment Body
Cedefop	European Centre for the Development of Vocational Training
CEF	Connecting Europe Facility
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT-EU	Computer Emergency Response Team for EU institutions, bodies and agencies
COVID-19	Coronavirus disease 2019
CSA	Cybersecurity Act
CSIRT	Computer Security Incidence Response Team
CTI	Cyber threat intelligence
CSPO	Cybersecurity Policy Observatory
EU-CyCLO -Ne	Cyber Crisis Liaison Organisation Network
DORA	Digital Operational Resilience Act (DORA)
DSP	Digital service providers
DSO	European Distribution System Operators
ECA	European Court of Auditors
EC3	European Cybercrime Centre
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
EDA	European Defence Agency
EEAS	European External Action Service
EECC	European Electronic Communications Code
EFTA	European Free Trade Association
eID	Electronic identification
eIDAS	Electronic Identification and Trust Services (eIDAS) Regulation
ENISA	European Union Agency for Cybersecurity
ENTSO	European Network of Transmission System Operators for Electricity
ETSI	European Telecommunications Standards Institute
EUCC	European Union Common Criteria scheme
EU5G	European Union certification scheme for 5G networks
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
ICT	Information and communication technology
IPR	Intellectual property rights
ISAC	Information Sharing and Analysis Centre
IT	Information technology
JCU	Joint Cyber Unit
KDT	Key digital technologies
MFF	Multi-annual financial framework
MoU	Memorandum of understanding
NIS	Networks and Information Systems
NISD	NIS Directive
NIS2	NIS2 Directive
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
OOTS	The Once Only Technical System
SC	Secretary
SCCG	Stakeholder Cybersecurity Certification Group
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises

SNE	Seconded national expert
SOCs	Security Operation Centres
SOP	Standard Operating Procedure
SPD	Single Programming Document
TA	Temporary agent

INTRODUCTION

FOREWORD

This year ENISA will be celebrating 20 years since its establishment in 2004. As we will celebrate our joint two decades long contributions in raising resilience and cybersecurity across the Union – together with our Member States, EU partners and allies worldwide – we also need to acknowledge that the cyber threats have continued to increase globally and the world itself has become a much more unstable and unpredictable since our conception.

The threat landscape has been severely impacted over the past two years by the Russian war of aggression and other geopolitical tensions via DDoS and ransomware attacks, huge rise in information manipulation, and attacks against data to be used for extortion. The motivation of the aggressor continues to be to either to destroy critical infrastructures and render them unavailable, thus impacting our resilience, or to dissuade and manipulate our public opinion through misinformation and information manipulation. We need to keep that in mind in 2024, which is an important juncture in our Union, whose functioning is underpinned by free and fair elections.

Thus, besides building on our accumulated expertise and strengths, it is important to further enhance our pro-active capabilities at the service of our Member States in 2024. The Agency has introduced a new activity within this SPD with the aim of putting the ENISA support action on a firmer ground, enabling it to better organize its assistance to Member States. In this way ENISA can better help the Member States in their efforts to improve the capability to respond to cyber threats and incidents while providing them with knowledge and expertise and increase preparedness in key sectors. Here the Agency acknowledges the importance of the additional financial resources availed to it by the European Commission, without which this activity would not be possible.

The Agency will also strengthen its capabilities and capacities in supporting Member States with the implementation of the NIS2 directive – which will need to be fully transposed by September 2024 – including by significantly increasing its human resources dedicated to this activity (+43% compared to 2022). This despite of the strain on its human resources, which will be further put under pressure once and if legislative initiatives such as the Cyber Resilience Act or the Cyber Solidarity Act are adopted over the current multiannual programming period (2024-2026).

The Agency, through its current multiannual work program, will continue to promote a whole-of-society approach towards cybersecurity, focusing on areas which add most value to the Member States and to the community at large. As 2024 will also mark the final effective year of its current strategy, it will together of its Management Board, launch a review of ENISA Strategy. These discussions, together with the foreseen adoption of the first ever State of Cybersecurity in the Union Report under Article 18 of the NIS2 directive, will enable the Agency to adjust its programming document and organization, so it can zoom its strategic focus into areas which matter most for achieving its aspiration for a high common level of cybersecurity across the Union.

MISSION STATEMENT

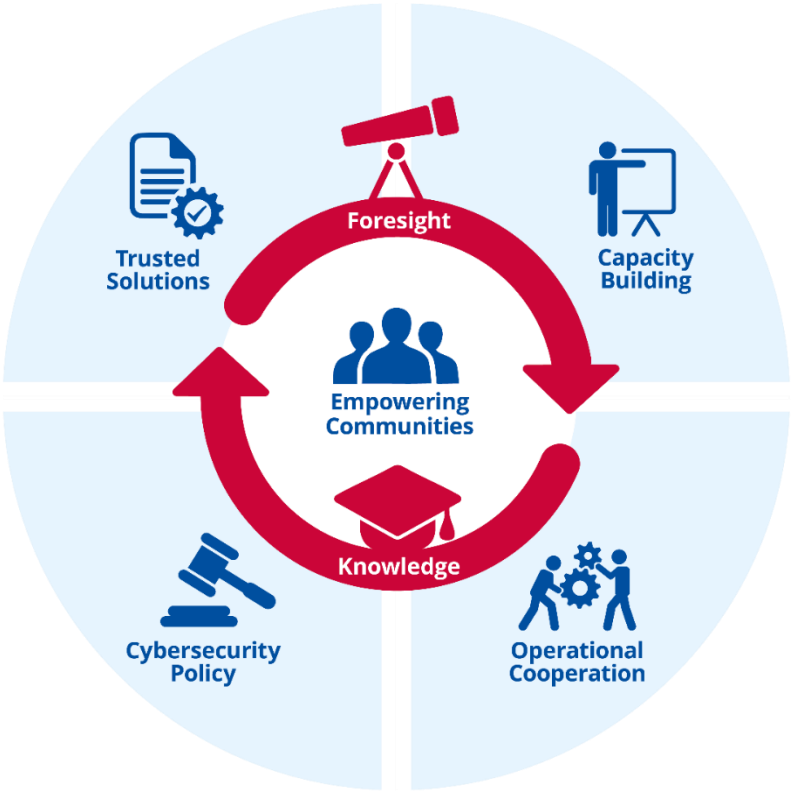
The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical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

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

STRATEGY

EMPOWERING COMMUNITIES

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



CYBERSECURITY POLICY

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

OPERATIONAL COOPERATION

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large-scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

TRUSTED SOLUTIONS

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

FORESIGHT

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

KNOWLEDGE

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

SECTION I. GENERAL CONTEXT

The results of the 2023 threat landscapes points to trends continuing in the cyber domain due to volatile geopolitical situation particularly due to the Russian invasion of Ukraine. The new paradigm is shaped by the growing range of threat actors that will need appropriate mitigation strategies to protect critical sectors, industry partners and all EU citizens.

ENISA's annual Threat Landscape (ETL)[1] for 2023 marks the 11th iteration of this flagship report and was published in October 2023. ETL 2022 looked at threats across EU and the world in the period starting July 2022 and finishing in July 2023. According to the ETL 2023, DDoS and ransomware rank the highest among the prime threats, with social engineering, data related threats, information manipulation, supply chain, and malware following. Moreover, there is a rise in threat actors professionalizing their as-a-Service programs, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises. In ETL 2023, it was observed that threat actor groups have an increased interest and exhibit an increasing capability in supply chain attacks by using employees as entry points. Threat actors will continue to target employees with elevated privileges, such as developers or system administrators. In addition, information manipulation as a key element of Russia's war of aggression against Ukraine has become prominent, whereas in 2022-2023 Internet shutdowns and complexity of DDoS attacks was at an all time high.

In terms of sectorial analysis, ETL 2023 identified public administration as the most targeted sector (~19%), followed by targeted individuals (~11%), health (~8%), digital infrastructure (~7%) and manufacturing, finance and transport (all 3 at ~6%). Almost half of the incidents had a digital impact (loss of availability, corrupted data, etc.), 20% had an economic impact, 18% societal impact and 5% had reputational and 5% a psychological impact. Only 1% of incidents had a physical impact.

It is important to highlight the inclusion of vulnerability landscape analysis and impact and motivation per sector, as well as detailed mapping of Tactics, Techniques and Procedures and targeted security measures that were part of the ETL for the first time in 2023.

ENISA continues to constantly monitor the cybersecurity threat landscape using an open and transparent methodology that was made available to the public in June 2022. This initiative aims to promote transparency in ENISA's work, build confidence and support capacity building across MS. It is in the context of such challenges that ENISA is exploring ways to improve this reporting of incidents. The NIS2 Directive is changing and harmonising the way cybersecurity incidents are notified. The new provisions will aim to support a better mapping and understanding of the relevant incidents.

NIS Investments 2023

The ENISA NIS Investments study aims at providing policy makers with evidence to assess the effectiveness of the existing EU cybersecurity framework specifically through data on how Operators of Essential Services (OES) and Digital Service Providers (DSP) identified under the NIS Directive invest their cybersecurity budgets and how the NIS Directive has influenced this investment. The present report, to be published November 2023, marks the fourth iteration of this report focusing on NIS investments. OES or DSP in the EU earmarks 7,1% of its IT investments for information security, while the average value is 7,6%. When analysing this normalised data set with historically available data, an increase of 0,4% is observed

[1] ENISA Threat Landscape 2022 — ENISA (europa.eu)

compared to the median was vs IT spending in 2021. This is still lower than the 2020 figures where the median IS vs. IT spend ratio was 7,7%. Still, any historical analysis must be done while considering the slight differences in the samples between the years of study and the differences in the macro environment.
When looking at cybersecurity skills and resources, the security domain with the most information security FTEs is Cybersecurity operations with 40% of the IS FTEs, followed by IT security architecture and engineering with 23% of the IS FTEs, and cybersecurity governance and risk management with 21%. Cybersecurity operations also comes out as the security domain with the most anticipated hires over the next two years (56%), followed by IT security architecture and engineering (42%) and cybersecurity governance and risk (36%). For organisations with a specific information security budget, the median training budget is 100k€, with an average of 333 k€, influenced by larger organisations with bigger budgets.
In 2024 the Commission will carry out an assessment and issue a recommendation to the Management Board regarding the extension of the mandate of the Executive Director. The current mandate of the Executive Director ends in October 2024.

Policy Context

Legislative measures designed to strengthen and respond to the threat landscape.
The adoption and implementation of policy frameworks is one key response area where the EU is making a difference. Indeed, the policies and initiatives being put in place in the coming years are determining how the EU faces the cybersecurity challenges of today and tomorrow.

Policy file	Status of policy file	Background and ENISA role / plans
The EU Cybersecurity Act	Amendment	On 18 April 2023, the Commission proposed a targeted amendment to the EU Cyber Security Act (ENISA Founding Regulation). The proposed targeted amendment aims to enable, by means of Commission implementing acts, the adoption of European cybersecurity certification schemes for 'managed security services'. This in addition to information and technology (ICT) products, ICT services and ICT processes, which are already covered under the Cybersecurity Act. Such security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents. There is a link between the proposed amendment to the CSA and the proposal for a Cyber Solidarity Act published by the Commission as part of the same package, as the EU Cybersecurity Reserve is envisaged to consist of trusted MSSPs.
NIS2	Adopted	The European Union (EU) Parliament and the Council approved legislation that sets clearer rules for entities in a wider range of sectors. The NIS2 directive reinforces and extends the existing approach under the NIS1, strengthening and streamlining the cybersecurity risk management and incident reporting provisions, and extending the scope by adding additional sectors, such as space or telecom (important for securing satellite communications, a vital infrastructure in remote rural areas, but also as a fail over in times of a natural disaster or military conflict). NIS2 underlines the special role of telecoms as a highly mature sector, a conduit for cyber-attacks, and a possible filter, protecting less mature and harder to protect sectors such as health care. In addition the NIS2 ambitions need to be supported for instance to improve incident reporting, to create a better situational picture, on vulnerability disclosure policies and an EU vulnerability database, on supply chain security and other coordinated Union-wide cybersecurity risk

		assessments, including expanding the scope in terms of sectors covered, and on creating the right culture and environment for essential and important entities to share cybersecurity relevant information such as cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Member States have 21 months to transpose NIS2 into national law and to implement it. In parallel, ENISA is developing its service and expertise for this with the introduction of service catalogue based on existing NIS 1 expertise that are reflected in this draft single programming document (SPD). ENISA is already invested in activities linked to the development and the implementation of the NIS2 Directive, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the implementation of the Directive in the coming years, using existing resources and building on these wherever necessary.
DORA	Adopted	In parallel with the NIS2 Directive, the European Parliament and the Council adopted in December 2022 the regulation on digital operational resilience for the financial sector (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, "DORA"). The regulation aims to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyber-attacks and other risks. The regulation aims to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyber-attacks and other risks. DORA requires financial entities to ensure that they can withstand all types of ICT-related disruptions and threats. ENISA is actively supporting the mapping of Cyber legislative initiative in the finance sector and works closely with European Commission and relevant EU Bodies on cybersecurity aspects of DORA including crisis management, incident reporting and information sharing.
Cyber diplomacy toolbox	Adopted	In addition, to support MS and EUIBAs in deterring and responding to cyber-attacks from third countries, the EU adopted a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, in the Council conclusions of 19 June 2017 [2], EEAS recently published updated implementation guidelines for the cyber diplomacy toolbox detailing specific steps Member States could take [footnote: Revised Implementing Guidelines of the Cyber Diplomacy Toolbox - 10289/23], The guidelines underline the importance of measures taken by Member States under the NIS Directive, to improve resilience, the role of ENISA in establishing information sharing channels with industry to gain situational awareness, and the importance of cooperation between EU-Cyclone, the CSIRT network, ENISA, CERT-EU and Europol, and EEAS Single Intelligence Analysis Capacity (SIAC), to ensure that internal and external EU actions are coherent.

[2] 2017 "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017.

The EU Cyber Solidarity Act	Proposal	On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the preparedness, detection and response to cybersecurity incidents across the EU. The EU Cyber Solidarity Act aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The proposal includes (a) the deployment of a pan-European infrastructure of Security Operations Centres ('European Cyber Shield') to build and enhance common detection and situational awareness capabilities; (b) the creation of a Cyber Emergency Mechanism to support Member States in preparing for, responding to, and immediate recovery from significant and large-scale cybersecurity incidents, including supporting preparedness actions, creating an EU Cybersecurity Reserve and supporting mutual assistance; (c) the establishment of a Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents. The EU Cyber Shield and the Cyber Emergency Mechanism of this Regulation will be supported by funding under Strategic Objective 'Cybersecurity and Trust' of Digital Europe Programme, whose founding regulation is amended accordingly via the Cyber Solidarity Act proposal. ENISA's proposed role in the implementation of the Cyber Solidarity Act is outlined in a number of articles. This includes ENISA being consulted in the identification of sectors/sub-sectors for which coordinated preparedness testing should be conducted. Furthermore, ENISA - in cooperation with NIS Cooperation Group, Commission and the High Representative - shall develop common risk scenarios and methodologies for the coordinated testing exercises, and that ENISA may be entrusted the operation and administration of the EU Cybersecurity Reserve, in full or in part, funded through a contribution agreement from COM. ENISA is also mentioned to play a role in preparing a mapping of the services needed, as well as a similar mapping to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve. In addition, requests for support from the EU Cybersecurity Reserve shall be transmitted to the Commission and ENISA and ENISA - in cooperation with the Commission and the NIS Cooperation Group - shall develop a template to facilitate the submission of requests for support. ENISA may also be requested to prepare agreement templates and, at the request of the Commission, the EU-CyCLONe or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident, after which ENISA shall deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks.
Artificial Intelligence Act	Proposal	With the EU's AI agenda advancing rapidly following the European Commission proposal on AI[3] and Coordinated Plan on Artificial Intelligence

[3] Proposal for a Regulation (EU) 2021/ 206 of 21 April 2021 laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts

		2021[4], the EU is addressing the major technological, ethical, legal and socio-economic challenges to put AI at the service of European citizens and the economy, for instance by considering linking high-risk AI systems to mandatory trustworthiness requirements. One of these challenges is understanding the interplay between cybersecurity and AI and how this can affect availability, safety or resilience of future AI services and applications. Building on ENISA's efforts towards securing AI / machine learning the Agency can continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2024. For this, ENISA will systematically monitor existing initiatives from the Member States in this area and continue supporting the Commission and Member States by providing good security practices and guidelines.
Cybersecurity Regulation for EUIBAs	Proposal	In March 2022, the European Commission proposed a new regulation[5] with rules to increase cybersecurity in all EU institutions, by establishing a governance framework for all EUIBAs, including the identification of specific functions and responsibilities (e.g Local cybersecurity officer), the development of a maturity assessment and a cybersecurity plan to monitor the implementation of appropriate and proportionate security measures, creating a Interinstitutional Cybersecurity Board in charge of monitoring the implementation of the regulation as well as overseeing the priorities of the CERT-EU, enabling easier information sharing on cyber threats and improving the efficiency of action to prevent and respond to cyber threats. This is expected to reduce the risk of incidents that cause material or reputational damage to EUIBAs. The proposal calls for increased cooperation with relevant bodies and stakeholders in the EU, via CERT-EU and ENISA. In addition it is proposed that ENISA will receive on a monthly basis a summary report from CERT-EU on significant cyber threats, significant vulnerabilities and significant incidents. A proposed regulation[6] on information security in the institutions, bodies, offices and agencies of the Union was also put forward earlier in 2022 to create a minimum set of information security rules and standards for all EU institutions, bodies, offices and agencies to ensure an enhanced and consistent protection against the evolving threats to their information. These new rules will provide a stable ground for a secure exchange of information across EU institutions, bodies, offices and agencies and with the Member States, based on standardised practices and measures to protect information flows. The regulation will also be applicable to ENISA and will require that the Agency takes measures to further enhance its own cybersecurity posture.
Cyber Resilience Act (CRA)	Proposal	In her State of the Union 2021 address, President von der Leyen underlined that the EU should strive to become a leader in cybersecurity, announcing in that context a new European Cyber Resilience Act. The act would add in particular to the existing baseline cybersecurity framework of the NIS

[4] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review
[5] Cybersecurity – uniform rules for EU institutions, bodies and agencies (europa.eu)
[6] Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union | European Commission (europa.eu)

		Directive 2 and the Cybersecurity Act. The Act with its EU cybersecurity certification framework propose the establishment of common European cybersecurity requirements for products with digital elements that are placed on the internal market by introducing mandatory essential requirements for products with digital elements as well as obligations for manufacturers, importers and distributors (e.g. vulnerability handling. Products with digital elements create opportunities for EU economies and societies. However they also lead to new challenges – when everything is connected, a cybersecurity incident can affect an entire system, disrupting economic and social activities. The CRA aims to address market needs and protect consumers from insecure products by introducing common cybersecurity rules for manufacturers, importers and distributors of tangible and intangible products with digital elements. The CRA proposal was published on the 15th September 2022. The scope proposed currently includes to all products connected directly or indirectly to another device or network. Open-source software and products and services covered by other existing rules, such as medical devices, aviation and cars, are explicitly excluded. The CRA proposal foresees a role for ENISA in the implementation of the Regulation. ENISA's proposed role includes receiving notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products, preparing a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements, at the request of the Commission conducting evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, proposing joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this regulation of products and submitting information relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level to the European cyber crisis liaison organisation network (EU CyCLONe). Depending on the tasks assigned to ENISA based on the final adopted text of the CRA, significant additional resources may be required. ENISA has provided expert opinion in the preparation process for the CRA proposal, including, through its Cybersecurity Policy Observatory (CSPO), in support of the Impact Assessment that accompanied the proposal and will also provide support in later stages (post-Impact Assessment) by contributing to elements of the legislative proposal such as risk categorisation, security requirements and notably to the preparation of the standardisation process, as well as in relation to the interplay between the CRA and certification schemes based on the Cybersecurity Act.
Electricity Network Code for Cybersecurity	Proposal	The Network Code on Cybersecurity aims to set sector specific rules for the cybersecurity of cross-border electricity flows across EU member states. It includes rules on cyber risk assessment, common minimum requirements, cybersecurity certification of products and services, monitoring, reporting and crisis management. It is part of Commission's request to ENTSO-E pursuant to Regulation (EU) 2019/943 and ENISA has been actively involved in defining risk assessment approaches, common minimum cybersecurity requirements and appropriate technical and organizational measures. The

		code contains many references to and foresees new leading and supporting tasks for ENISA amongst others, facilitation of an Early Warning System, support ACER in monitoring the implementation of the code and support ENTSO-E and EU.DSO entity with organising sector specific exercises.
Horizontal Rule – Part IS	Adopted	This sectorial legislative initiative consists of a new Implementing Regulation and a new Delegated Regulation regarding information security management systems for organisations and competent authorities (Horizontal Rule Part-IS). It also introduces amendments (through one implementing act and one delegated act) to the already existing Commission Regulations (EU) No 748/2012, No 1321/2014, 2017/373, 2015/340, No 139/2014, No 1178/2011, No 965/2012 and 2021/664. The purpose of these amendments is to introduce requirements to comply with the information security management requirements introduced in the new Implementing and Delegated Regulations, and to add the elements necessary for the competent authorities to perform their certification and oversight activities. The objective is to efficiently contribute to the protection of the aviation system from information security risks, and to make it more resilient to information security events and incidents. Specifically, the Horizontal Rule introduces additional rules to fill in existing gaps in the policy framework in order to address the safety impact of information security risks in a comprehensive and standardised manner across all civil aviation domains. ENISA is currently contributing to the Activities of the working groups established to support the implementation of the Regulation, e.g. concerning the development of acceptable means of compliance (AMC) and guidance material (GM).
Other: • eIDAS 2 • Delegated Regulation on cybersecurity under the Radio Equipment Directive • Data Act • Chips Act • DSA • DMA • European Health Data Space		**eIDAS 2** Digital identity and trust services are crucial for the EU digital market, because they allow citizens and businesses to carry out transactions online in a safe and trusted way. In 2020 the Commission reviewed the Electronic Identification and Trust Services for electronic transactions in the internal market (eIDAS) Regulation and identified factors hindering adoption of electronic identification mechanisms. In June 2021 the Commission made a proposal for a revised Regulation establishing a European Digital Identity framework and a European Digital Identity Wallet, to be available for all EU citizens, on a voluntary basis and that will be usable for online transactions with government entities, but also with businesses. In the 2024-2026 period, ENISA will support Member States and the Commission with the development of the European Digital Identity Framework and the European Digital Identity Wallets, as set out in Regulation establishing a Framework for a European Digital Identity in addition to promoting the exchange of good practises and capacity building of relevant stakeholders. The Regulation establishing a Framework for a European Digital Identity also expands the list of qualified trust services with electronic attestations of attributes, distributed ledgers and electronic archiving and management of remote devices for the creation of electronic signatures and seals. The NIS2 Directive foresees that the cybersecurity obligations laid down in this Directive should be considered complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014 (eIDAS Regulation). ENISA will support Member States and the Commission with this transition, to ensure

		that the trust service providers and the national authorities can benefit from the NIS Directive ecosystem. **Delegated Regulation on cybersecurity under the Radio Equipment Directive** The European Commission adopted Delegated Regulation (EU) 2022/30 under the Radio Equipment for certain categories of radio equipment to increase its level of cybersecurity (protection of networks, privacy and protection from fraud). The Commission has issued a standardisation request to CEN and CENELEC to develop relevant harmonised standards in support of the EU requirements on cybersecurity of radio equipment. In this respect, it has been established that the aforementioned European standardisation organisations will have to ensure coherence of the developed harmonised standards with the EU cybersecurity certification schemes developed by ENISA, since they can have the same scope, such as IoT devices or 5G network equipment. Therefore, a cooperative work between ENISA and the standardisation organisations is envisaged. **Chips Act** On 8 February 2022, the European Commission proposed a comprehensive set of measures for strengthening the EU's semiconductor ecosystem, the European Chips Act [7] In this package, the Commission has adopted a Communication, outlining the rationale and the overall strategy, a proposal for a Regulation for adoption by co-legislators, a proposal for amendments to a Council Regulation establishing the KDT Joint Undertaking, and a Recommendation to Member States promoting actions for monitoring and mitigating disruptions in the semiconductor supply chain. Supply chain security, including cybersecurity aspects is an important cross cutting issue for stakeholders.

Non legislative policy developments

ENISA Cybersecurity Support Action

During the course of 2023 ENISA has developed and implemented the cybersecurity support action to support Member States in the short term in view of the immediate and elevated threat of malicious cyber activities due to the on-going Russian war of aggression against Ukraine. This mechanism aims to complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats by assisting Member States in their efforts to improve the capability to respond to cyber threats and incidents. It provides them with knowledge and expertise and increases preparedness in key sectors. The Commission has indicated that ENISA would continue the Cybersecurity Support Action with a further contribution agreement of 20MEUR in 2023, with an

[7] COM(2022) 45. Communication from the Commission: A Chips Act for Europe. 08/02/2022
COM(2022) 46. Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act). 08/02/2022
COM(2022) 782. Commission Recommendation on a common Union toolbox to address semiconductor shortages and an EU mechanism for monitoring the semiconductor ecosystem. 08/02/2022

agreement for implementation and finalising by 31st December 2026[8]. The work programme now includes a specific activity earmarked to undertake the Cybersecurity Support Action, highlighting the objectives, outputs and resourcing foreseen during 2024 and taking into account lessons learned from the implementation in 2023.

EU crisis management framework

The EU cybersecurity eco-system does not yet have a common space to work together across different communities and fields which allow the existing networks to tap their full potential. The recent geopolitical situations confirmed the need for a joint response between the Member States and the Union institutions, bodies, offices and agencies in responding to incidents and cyber-attacks and builds on the work started in the Recommendation of 23.6.2021 on building a Joint Cyber Unit 4520 (2021) for a coordinated response to incidents and crises and Council conclusions 19.10.2021 (13048/21) - the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises Commission recommendation 1584'(Blueprint) of 2017.

ENISA will contribute in enhancing the EU cyber crisis management framework following the NIS2 and latest Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure 15623/22 of 9 December 2022, and taking into consideration both the Blueprint and the Joint Cyber Unit recommendations, along the lines and according to the roles defined in the on-going discussions amongst Member States and EU operational actors

Cyber Defence Policy

In November 2022 the Commission and the High Representative Josep Borrell put forward a Joint Communication[9] on an EU Cyber Defence policy and an Action Plan to enhance cooperation and investments in cyber defence to better protect, detect, deter, and defend against a growing number of cyber-attacks. Areas under consideration requiring potential support by ENISA such as building preparedness and response actions across the EU, including the testing of essential entities operating critical infrastructure for potential vulnerabilities based on EU risk assessments, as well as incident response actions to mitigate the impact of serious incidents and to support immediate recovery and/or restore the functioning of essential services. Council Conclusions 22.05.2023 (9618/23) on the EU Policy on Cyber Defence emphasizes the importance of establishing mutual beneficial cooperation between this centre and other EUIBAs, in particular ENISA and CERT-EU and invites Member States to exchange information on best practices to develop skilled cybersecurity professionals with the support and expertise of ENISA.

Cybersecurity Skills Academy

On 18th of April 2023, as part of a Cyber Package, the Commission adopted a communication on the Cybersecurity Skills Academy inviting actors to take action to close the cybersecurity workforce skills gap. The Academy aims at fostering knowledge generation through education and training by working on a common language on cybersecurity role profiles and associated skills namely ECSF, also and including pilots for attestation schemes for cybersecurity competences; ensuring a better channelling and visibility over available funding opportunities for skills-related activities in order to maximise their impact; calling on stakeholders to take action by making concrete cybersecurity pledges and integrating cybersecurity skills in their national strategies; defining indicators to monitor the evolution of the market and to address better the needs on one hand, and on the other, the offer of trainings, as well as to better direct funds towards the needs. ENISA plays a key role in the implementation of the Academy tasks outlined, all in collaboration with relevant stakeholder namely the ECCC, the NCCs, the NIS Cooperation Group and others.

[8] Contribution Agreement is being finalized. Dates and amount are currently estimated.
[9] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_6642/IP_22_6642_EN.pdf

Implementation of the EU cybersecurity certification framework

ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework by preparing the candidate schemes and supporting their maintenance once adopted.. In this task ENISA is supported by area experts and operates in collaboration with the National Cybersecurity Certification Authorities (NCCA) in the Member States. It is expected that the draft candidate cybersecurity certifications schemes proposed by ENISA will be adopted by Commission implementing Regulations. The adopted schemes will allow for the conformity assessment of digital products, services and processes in the Digital Single Market under those schemes, which can contribute to increasing the level of stakeholders trust of digital solutions in the Union. Currently, ENISA has prepared a candidate cybersecurity certification scheme on Common Criteria (EUCC) which is currently being considered for voting in committee of the dedicated Implementing Act by the Commission and the Member States, likely by Q4. Following up, the draft candidate cybersecurity certification scheme on Cloud Services (EUCS) will be submitted to the ECCG for its opinion and adoption in committee will likely follow. Furthermore, an ad hoc working group has been supporting ENISA in drafting the candidate certification cybersecurity certification scheme for 5G network. Finalizing the candidate schemes for specialized product categories under the EU Common Criteria (EUCC) scheme and for cloud services is just the first step and it will likely bring about benefits in terms of recognition and trust across public services, business and citizens during the time period starting 2024.

In relation to the digital identity framework ENISA continues supporting the development of a certification strategy matching the expectations of Article 6a of the Regulation which requires Member States to issue a European Digital Identity Wallet based on common technical standards following mandatory conformity assessment and the voluntary nature of certification within the European cybersecurity certification framework, as stipulated in the Cybersecurity Act. This strategy shall make best reuse of existing relevant cybersecurity certification schemes under development and seeks to identify potential new certification iterations of schemes likely to contribute to the certification of the EU Digital Identity wallet. ENISA is currently responding to a request of the Commission to support it with respect to the EUDIW.

ENISA will also support the development of certification means that would allow to demonstrate compliance with certain requirements of Article 21 of the NIS 2 Directive, as this regulation stipulates that Member States may require, entities to use particular ICT products, services and processes, either developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.

In terms of the Union Rolling Work Programme which has been pending publication by the Commission, ENISA stands ready to support the Commission with the current as well as future editions of the URWP. The adopted schemes will also be mapped with the requirements of the CRA to provide the means for the conformity assessment of digital products, services and processes in the Digital Single Market, in a way that compliance with the CRA requirements can also be attested. This approach sets the stage to for other legal instruments on cybersecurity to use the synergetic effects of the cybersecurity certification framework. ENISA is currently responding to a request of the Commission to support it with respect to CRA.

SECTION II. MULTI-ANNUAL PROGRAMMING 2024 – 2026

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA adopted a new strategy for the Agency in June 2020, which builds on the Cybersecurity Act (CSA), and outlines how the Agency will strive to meet the expectation of the cybersecurity ecosystem in a medium to long-term perspective, in a manner that is open, innovative, agile as well as being socially and environmentally responsible. The strategy sets out a vision of "A trusted and cyber secure Europe" in which all citizens and organisations of Europe not only benefit but are also key components in the effort to secure Europe. Most importantly, the ENISA strategy outlines seven strategic objectives which are derived from the CSA and set the expected medium to long-term goals for the Agency.

1. Multi-annual work programme

The following table maps the strategic objectives stemming from ENISA's strategy[10], against the respective articles of the CSA. It furthermore integrates the activities of the Work Programme showing how the progress in the achievement of the objectives is monitored. These objectives shall be reviewed if applicable through the ENISA Management Board as from 1 July 2024.

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

STRATEGIC OBJECTIVE	ACTIONS TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	INDICATOR
SO1 **Empowered and engaged communities across the cybersecurity ecosystem**	Activities 1 to 10	Art.5 to Art.12	Empowered ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure An EU-wide, state of the art body of knowledge on cybersecurity concepts and practices, that builds cooperation amongst key actors in cybersecurity, promotes lessons learned, EU expertise and creates new synergies	The % gap between demand and supply of cybersecurity skilled professionals General level of cybersecurity awareness and cyber hygiene among citizens and entities[11]
SO2 **Cybersecurity as an integral part of EU policies**	Activities 1 & 2	Art.5	Cybersecurity aspects are considered and embedded across EU and national policies	Uptake of policy recommendations adopted within the biennial report on the state of cybersecurity in the Union[12] Effectiveness of EU relevant policy initiatives taking cybersecurity into consideration
			Consistent implementation of Union policy and law in the area of cybersecurity EU cybersecurity policy implementation reflects sectorial specificities and needs Wider adoption and implementation of good practices	Level of maturity of cybersecurity capabilities and resources across the Union at sector level[13]

[11] Article 18(1)c in NIS2
[12] As part of the report of the state of cybersecurity in the Union ENISA shall include policy recommendations with a view to addressing shortcomings and increasing the level of cybersecurity across the union [Art 18(2) of NIS2]
[13] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e

SO3 **Effective cooperation amongst operational actors within the Union in case of massive[14] cyber incidents**	Activities 4, 5a & 5b	Art.7	All communities (EU Institutions and MS) use streamlined and coherent set of SOPs for cyber crises management Efficient, tools and methodologies for effective cyber crisis management	Level of cooperation and availability, utilisation and trust of Union level networks, tools and databases.
			Member States and institutions cooperating effectively during large scale cross border incidents or crises Public informed on a regular basis of important cybersecurity developments Stakeholders aware of current cybersecurity situation	Risk level due to cyber threats is understood and decision makers are able to prioritize resources to manage the risk
			Improve MS capabilities to respond to cyber threats and incidents	Union Level of preparedness and response to large-scale cross-border incidents
SO4 **Cutting-edge competences and capabilities in cybersecurity across the Union**	Activities 3 & 9	Art.6 and Art.7(5)	Enhanced capabilities across the community Increased cooperation between communities	Aggregated assessment of the level of cybersecurity capabilities in the public and private sectors across the Union[15]. Aggregated assessment of the level of maturity of national cybersecurity capabilities and resources as well as the extent to which MS national cybersecurity strategies are aligned[16]

[14] large scale and cross-border
[15] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)b
[16] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e

		Art.10 & Art.12	Greater understanding of cybersecurity risks and practices Stronger European cybersecurity through higher global resilience.	The % gap between demand and supply of cybersecurity skilled professionals General level of cybersecurity awareness and cyber hygiene among citizens and entities
SO5 **High level of trust in secure digital solutions**	Activities 6 & 7	Art.8	Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework versus schemes' requests and schemes' adopted Smooth transition to the EU cybersecurity certification framework Certified ICT products, services and processes are preferred by consumers / industry and where relevant, Operators of Essential Services or Digital Service Providers under NIS1, and entities in scope of NIS2.	Citizens trust in ICT certified and non-certified solutions in the EU market
			Contribution towards understanding market dynamics A more competitive European cybersecurity industry, SMEs and start-ups	Monitor metrics such as number of certificates issued under an EU scheme; number of companies interested in EU certification; growth observed in the number of CABs / or EU certification functions thereof recorded in the MS.
SO6 **Foresight on emerging and future cybersecurity challenges**	Activity 10 & 8	Art.11 & Art. 9	Research and development of cybersecurity technology reflecting the needs and priorities of the Union. Funding the development of cybersecurity technologies that meet the Union's ambition to become more resilient, autonomous and competitive.	Overall EU investment in R&I activities addressing emerging cybersecurity challenges

SO7 **Efficient and effective cybersecurity information and knowledge management for Europe**	Activity 8	Art.9	Decisions about cybersecurity take into consideration information and knowledge concerning the current and evolving cybersecurity threat landscape Stakeholders receive relevant and timely information for policy and decision making	Union level cybersecurity risk assessment and cyber threat landscape [adopted in accordance of Article 18(1)a]

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

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

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

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

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

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

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

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

ENISA Corporate Strategy

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

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

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

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

The table below highlights the responsible activity for each corporate objective from the Corporate Strategy including the key goals and means to measure the associated KPIs. In addition to these principles for resourcing the objectives have been taken into consideration when developing the budget.

Strategic dimension	**Objectives**	Activity's to achieve objectives	**Key goals (KPIs/means to measure the KIs**
People centric organisation	Effective workforce planning and management	Activity 13	• Agency's internal workforce needs for the year n until n+2 are defined and presented to the MB together with the first draft SPD for those years as per annual/internal procedures. • Effective FTEs used for SPD activities (as reported in AAR by end of year n) do not diverge from planned FTEs in SPD (as endorsed by MB in the beginning of year n) by more than 5% according to annual/internal procedures. • 95% of Agency's staffing posts (TA, CA, SNE) are fulfilled by the end of year according to its annual recruitment results. • Vacated staff posts are fulfilled in less than 300 days according to its annual recruitment results. • All assignments of staff are reviewed regularly every three years during the Agency's annual/internal procedures. • Aggregate loss of FTE across the Agency due to absences (excluding long-term sick leave) is less than three FTEs annually during its annual/internal process.
	Efficient talent acquisition, development and retainment	Activity 13	• Agency has established clear competency targets in line with its established needs and has reviewed them in an annual appraisal exercise. • All selection criterions used for the published as well as internal vacancies are solely based on established competencies described in the annual/recruitment process. • Agency's proficiency levels across target competencies have increased over the set period according to annual appraisal exercises. • 50% of Agency's established workforce needs are addressed through internal talent development (including internal mobility, competitions and appointment) according to its annual internal process.

			• Jobholder satisfaction with the guidance and support received from their Reporting Officers in achieving learning and development goals is high according to the biennial staff satisfaction survey. • High level of staff satisfaction for learning opportunities offered and knowledge sharing options according to the biennial staff satisfaction survey. • High level of positive peer-review assessments in CDR reports in annual internal process.
	Caring and inclusive modern organisation	Activity 13	• High aggregate staff satisfaction with psychological safety level according to annual staff satisfaction survey. • High aggregate staff satisfaction with workspace and related services according to biennial staff satisfaction survey. • Agency obtains EU Agency's Network Certificate of Excellence in Diversity and Inclusion by the end of 2025 according to external audit and certification process. • High level of satisfaction with Agency's workplace integration, wellness and health programmes, engagement and community mindset for staff according to annual staff satisfaction survey. • Staff stress level is decreasing from 2022 levels and is sustained at low levels after 2025 according to annual staff satisfaction survey
Service centric organisation	Ensure efficient corporate services	Activity 11 & 13	• High satisfaction with essential corporate support services found through an annual MT survey. • High satisfaction with demand driven or optional corporate support services found through an annual MT survey. • Number of procurement procedures merged, combined or used in interinstitutional FWCs found through an annual internal procedure. • The percentage of staff (measured in FTEs) engaged in shared corporate service activities within the Agency found through an annual internal procedure. The percentage of staff (measured in FTEs) engaged in shared corporate service activities beyond the Agency with other EUIBAs (under SLAs, MoUs or other arrangements) found through an annual internal procedure
	Introduce digital solutions that maximise synergies and collaboration within the Agency	Activity 11 & 13	• Implement (replace or develop) at least five user-centered, cloud-based, corporate solutions or tools fit for purpose and in line with ENISA's IT strategy and relevant business needs by Q4 2025. • Limited disruption of continuity of services across all corporate support service areas measured by annual assessment. • To have IT support service standards as technical KPIs in place by Q2 2025 and to have them continuously monitored and observed, to support the maintenance and development of operational IT systems through an annual review. • All on-premises systems are maintained within risk levels established by the business owners and all corrective measures recommended by periodic risk assessments are implemented as found in an annual review.
	Continuous innovation and service excellence	Activity 11	• The percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have not been reviewed less than three years ago as found by an annual review. Percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have been last reviewed more than four years ago as found in an annual review.

	Developing service propositions with additional external resourcing	Activity 11 & 13	• At least three SLAs signed and in operation with EUIBAs covering ENISA's operational services with additional resourcing from beneficiaries by 2025.
Sustainable organisation	Ensure ENISA is climate neutral by 2030	Activity 11	• Acquire an EMAS certificate23 by Q4 2023. • 50% of participants in ENISA's organised events and meetings to participate online by 2025, rising to 75% by 2030. • 50% of ENISA events and meetings to be organised as hybrid or online by 2025, rising to 75% by 2030. • Initiate and by end 2024 agree a tripartite MoU with the Hellenic Authorities and the landlord of ENISA HQ building to reduce the climate impact of the HQ building at least 40% by 2029, by installing solar panels on the non-classified part of the building or procure a green building for the Agency by then. • Offset all residual emissions generated through ENISA operations from 2024 onwards
	Promote and enhance ecologic sustainability across all the Agency's operations	Activity 11 & 13	• Recycle all ENISA residual waste created in its HQ and local offices by 2025. • Implement ecological sustainability and climate neutrality criteria for procuring event management and support and for facilities management and support services from external contractors by 2025. • Implement ecological sustainability and climate neutrality criteria for all ENISA tenders for corporate service contractors by 2027 and by 2029 for operational activities. • Understand best practices in sustainable IT solutions, define an agency-wide approach and include it in the IT Strategy.
	Develop efficient framework for continuous governance to safeguard high level of IT and physical security	Activity 11 & 13	• Review the Agency's IT strategy and align it with the objectives of the corporate strategy by Q3 2024. • Set in place a relevant policy for security compliance for IT and for physical security (including for required EUCI levels) for all relevant internal and external services with a high level of adherence to this KPI from 2025 onwards. • The Agency in a position to handle EUCI at the level of SECRET UE/EU SECRET and be accredited as being able to do so by Q4 2024. • 20% of the total IT budget to be allocated to information security proportional to the level of risks across various IT systems within the Agency by Q4 2024. Implement relevant security requirements and criteria for all relevant ENISA tenders for corporate services by Q1 2025.

2. HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2024 – 2026

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

The Agency has taken a number of actions to manage and balance the resources allocated to it, and adjust to the ever increasing demand for ENISA services by Member States and stakeholders. The actions undertaken to address the effective and efficient use of resources include:

2.1.1. Recruiting new talent and increasing operational capacities

The Agency has taken significant strides to improve the fulfilment of its Establishment Plan with an increase from 77% in 2019 to 87% in 2022 to 96% as of 01/09/2023, with the rate expected to increase to 100% by the end of 2023 (not including possible resignations)[17]. This despite the increasing competition for cybersecurity talent[18] and – compared to private sector and the living standard of more economically advanced Member States – uncompetitive overall salary and support package which the Agency can offer.

In parallel the Agency has also taken persistent measures over the past 3 years to rebalance the allocation of posts towards operational units in expense of corporate units. This follows the reorganisation of the Agency under the direction of the Management Board decision No MB/2020/9, according to which all support and corporate functions (including administrative and secretarial support etc) where concentrated to corporate units from 01.01.2020 onwards, leaving in operational units only the posts which purpose is entirely linked with operational tasks and functions (Title II Chapter II in the Cybersecurity Act).

Though the rebalancing has achieved in creating more capabilities in delivering its operational tasks, it has reached to its limits. Further internal adjustment and reallocation at the expense of corporate activities, would mean significant erosion of the Agency's administrative capacity including sustaining security (including IT and physical), legal, financial & procurement, compliance functions and other corporate support systems (please see table below).

Allocated staff policy plan posts	01.01.2021	%	01.01.2022	%	01.01.2023	%
Operational units	70	**59,3**	78	**61,9**	90	**70,3**
Corporate units	44	37,3	37	29,4	36	28,1
unallocated[19] (of which reserve)	4(2)	3,4	11(9[20])	8,7	2(0)	1,6
TOTAL	118	100	126	100	128	100

2.1.2. Utilising internal and external synergies

[17] Individual set of KPIs have been introduced since 01.01.2023 to all managers to ensure rapid fulfillment of all open posts allocated to the unit.

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

[19] Including 2 posts held by the Executive Director and the Accounting Officer.

[20] Includes posts which became available after the adoption of the NIS2 directive late November 2022.

Building on the outcomes of strategic discussions with the Agency's Management Board, the Agency developed service packages in key areas of its mandate. The purpose of the service package is to integrate ENISA's various outputs across different activities, help the agency to prioritize its actions, build and make use of internal synergies, and ensure that adequate resources are reserved across the Agency in a transparent manner.

Identifying priorities and de-prioritisation of actions in 2024 work programme. The Agency sought guidance from the Management Board for its 2024 work programme during strategic discussions at the MB meeting in June 2023. The Management Board members were requested to identify what areas of its work programme ENISA should do more versus those that it should do less, based on the lessons learned from the annual activity report 2022. The current draft of the work programme has taken the strategic guidance from the Management Board into consideration and resources have been allocated according to the feedback received. The negative priorities of reduced scope, suppressed outputs and / or postponed projects amount to a shortfall in resources of 3.8 million euros and 15 FTEs for the 2024 work programme.

Shared operational functions and partnerships. Structured cooperation with CERT-EU was put in place already in 2020 with the drafting of an annual cooperation plans to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation. A service level agreement has been signed on 13 July 2023 with European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA) which covers support services offered by ENISA to EU-LISA on the planning, execution and evaluation of upcoming annual exercises. An MoU was signed in 2023 with ECCC and EDPS to coordinate the implementation of operational tasks of the Agency.

Shared administrative and corporate services and partnerships. On 20 December 2022 the Agency signed a service level agreement to create synergies with the European Cybersecurity Competence Centre (ECCC) in the field of research and innovation as well as in administration, namely, accounting, data protection and information security. Shared service agreements are currently in place with the European Union Intellectual Property Office (EUIPO) and with the European Centre for the Development of Vocational Training (CEDEFOP) to streamline procurement, shared financial services, human resources, IT solutions and in the area of data protection. The Agency will continue build up on its shared services strategy and further build upon the partnership model with other EUIBAS.

2.1.3. Current resource gaps and challenges

Although the Agency has taken considerable steps to internally build and create synergies and efficiencies in 2021-2022 there is a limit to what can be done internally and externally. All these measures are, in the end of the day, mitigation actions which point to a persistent gap in resourcing which does not allow the Agency to fully undertake the implementation of its mandate, not to tackle efficiently new challenges.

New challenges and expectations. In 2022, the Agency was able to raise to the challenge posed by the Russian war of aggression in Ukraine partially thanks to additional budgetary resources allocated by the European Commission in response to the call of the informal council in Nevers to establish and expand dramatically ENISA Support Services. However, the additional funds did not include any additional posts to its Establishment Plan or Staff Policy Plan, forcing ENISA to internally reallocate its human resources. To meet these challenges, the Agency was also forced to suppress outputs foreseen in the original draft SPD 2023-2025, postpone projects and/or reduce the scope of projects in 2023, due to budgetary shortfall of more than 3 million.

Budget implementation	2020[21]	%	2021[22]	%	2022	%
Voted budget	21 149 120	100.00	22 833 060	100.00	24 207 625	100.00
Additional budget	-	-	-	-	15 000 000	63.57
Total budget	21 149 120	100.00	22 833 060	100.00	39 207 625	163.57

[21] ENISA Annual Activity Report 2020: https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2020

[22] ENISA Annual Activity Report 2021: https://www.enisa.europa.eu/publications/corporate-documents/enisa-annual-activity-report-2021.pdf

	Implemented budget	20 588 320	97.35	22 721 149	99.51	39 179 406	100.00

In 2022 the Agency did received few additional FTEs to address new tasks. Firstly, for tasks foreseen in NIS2, the resources which were approved constituted a slight increase of budget 610 kEUR per year and some (5) new posts (4% increase). It should be noted, however, that most MS have responded to NIS2 by significantly increasing the staff numbers of their National Cybersecurity Agencies and though ENISA does not fulfil the regulatory duties like national agencies do, the allocated appropriations fall far short to the initial needs which the Agency put forward during consultations with the Commission (10-12 posts). Nor were the final additional resources qualitatively fit for purpose - the Agency requested higher grades of posts, given the high level of new tasks requiring specialised expertise. However, the new posts were graded as entry level.

Secondly, recognising its growing need to have increased capabilities to support operational cooperation, resilience and capabilities at the Union level, and expand the scope of relevant services which ENISA offers to the Member States, Commission has taken two steps. Firstly, allocated 2 additional SNE posts to ENISA to facilitate operational cooperation with Member States and in 2023, injected an additional 15 MEUR to ENISA to scale up and expand its ex-ante and ex-post services to the Member States (tasks related to Articles 6 and 7 of CSA) in response to the higher threat due to Russian aggression. Both these steps should be acknowledged and welcomed. However, both in terms of human resources and in terms of budget, those additional resources are insufficient compared to the scale of the task or the level of demand for ENISA services. Preliminary lessons learned from the implementation of the Cybersecurity Support Action were presented to the Management Board during the MB meeting in June, highlighting that the actual FTE allocation for ENISA Support Action 2023 was 20% to 30% higher than originally estimated (~15 FTEs) and as such adequate resourcing will need to be reflected in the potential continuation of the Cybersecurity Support Action within and beyond 2024.

2.2. OUTLOOK FOR THE YEARS 2024 – 2026

The multi-annual financial framework 2021-2027 laying down the EU's long term budget could not foresee the cumulative effect the rapidly deteriorating cybersecurity threat landscape – including due to Russian war of aggression which increased the Union's attack surface and brought new challenges to manage supply-chain security – or new legislative initiatives such as NIS2 Directive, the proposed Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA), etc. – will have on ENISA's ability to serve the ever-increasing demands with its limited resources.

The Agency was only able to fulfil its operational mandate in response to Russian aggression partially thanks to additional budgetary resourcing stemming from the Cybersecurity Support Action, but did not receive any significant additional posts to its Establishment Plan. Thus with the long term outlook of the Union threat landscape remaining bleak, the Agency cannot, under its current normal budgetary and human resource limits, maintain even this minimum level of support going forward, without jeopardising its other priorities, like increasing assistance to the Union and Member States to support transposition of NIS2 or support actual deployment of new certification schemas.

Secondly, though welcome in substance, no new resources have been given to the Agency within legislative proposals of the Commission that nevertheless give new tasks for ENISA. For example, within the CRA proposal, which is currently undergoing co-decision procedures, despite that the Commission estimated that ENISA would need about 4,5 FTEs to fulfil these new tasks, the Commission suggested they be reallocated from existing resources e.g. that ENISA would deprioritise other activities. In parallel, in the Cyber Solidarity Act proposal, the Commission again estimates that new assignments need about 7 FTEs to be implemented and again propose that these 7 FTEs are reallocated from existing resources of ENISA, which should be then deprioritised. In addition, numerous sectorial proposals or commitments (DORA) referring to ENISA 14 times, the Electricity code referring to ENISA 32 times regarding tasks, declarations with

3rd countries[23] etc.) rightly try to leverage on ENISA expertise in upgrading the cybersecurity posture of other sectors, policies or partners. However, those proposals do not acknowledge that even this would mean that the Agency must then dedicate time and expertise – e.g. human capital – to fulfil these expectations, putting a further strain on the Agency's limited resources.

Acknowledging ENISA's exceptional operational mandate, the Commission has indicated its desire that ENISA would continue the Cybersecurity Support Action with a further contribution agreement of 20MEUR in 2024 with an agreement for implementation for finalising on 31st December 2025. While ENISA in the short term demonstrated the required agility and flexibility to perform, such new tasks, if potentially they become permanent ENISA should be also entrusted with additional resources, in the form of allowing it to temporarily surpass the CA post levels foreseen in the Staff Policy Plan, in order to execute the Support Action efficiently without drastically deprioritising resources from other activities.

The human resource requirements forecasted in the current draft of the SPD are well above those foreseen by the current establishment plan. While ENISA remains committed to the continuous improvement of its administrative and operational efficiency, the Agency has almost exhausted all possible internal and external actions that it can take to resolve the insufficient allocated resources. Therefore unless further resources are allocated, or ENISA is allowed to temporarily go beyond the current CA posts foreseen in the Staff Policy Plan, ENISA would need to de-prioritise and limit the scope of its services within the existing tasks as well as within new tasks in its operational mandate.

2.3 RESOURCE PROGRAMMING FOR THE YEARS 2024 – 2026

2.3.1 Financial Resources

The current total appropriations in EU Budget for 2024 amount to 25.8 million euros. As noted above, this level is not sufficient for the Agency to fulfil its mandate in full, given the increased legislative and policy expectations and demands for its services in response to the heightened threat level. The Agency's needs, which are estimated on the basis of the development of the 2024 work programme, far exceed the Agency's means. The total amount of budget that the Agency foresees that it requires to fulfil its mandate and by extension the demands of stakeholders amount to additional 3.8 million EUR, and this is without the operational budgetary resources which would be necessary to maintain or expand ENISA Support Action (ex-ante and ex-post services to Member States under Article 6 and 7 of CSA) and without the additional costs which it would entail on ensuring corporate and administrative support. Discussions on Support Action fund activities for 2024 including financial and human resources are ongoing and are expected to be concluded by Q3 2023.

In developing the first budgetary estimates of the first draft 2024 work programme, the Agency has taken into account its imperative needs and priorities, requirements set in the Corporate Strategy (please see under part 2.4. 'efficiency gains') as well as other factors such as the inflationary environment, which has had an additional detrimental effect on budgeting, and which is expected to continue into 2024. Also, costs for achieving the goals of climate neutrality of the Agency by 2030 (including by ensuring the energy efficiency of its buildings) and staff development costs are expected to increase over the coming years.

These factors mean that the Agency's operational budget (Title III) without the potential additional funds for Support Action, will not be maintained at 2023 level and will decrease approximately 16.93% (from 2023 level). The identified impact are detailed under each activity in the draft SPD.

[23] Paragraph 26 Tirana declaration 6th December 2022 - As cyber threats know no borders, we will work together to enhance our collective cyber security. Recent large scale cyber-attacks demonstrate the need for enhanced engagement, building on existing programmes and on cooperation with the EU Agency for Cybersecurity (ENISA)

2.3.2 Human Resources

The Management Board has mandated the Agency to highlight in its SPD those parts of the conclusions of the Annual Activity Report 2022 (AAR 2022), which together with the recent Commission's legislative initiatives, indicate significant resource constraints which the Agency will face in the multiannual programming period. The current establishment plan foresees no change in the number of posts allocated to ENISA (82 posts) although the Agency has been entrusted and is foreseen to be further entrusted with new and enhanced tasks. As such the Agency has undertaken a thorough assessment of its internal human resourcing needs for the programming period of 2024-2026, taking into account the near-term foreseen legislative and political developments, as well as the heightened level of threat of the cybersecurity landscape[24]. Whilst the Agency acknowledges that this overall initial assessment of a 44.5 FTE gap compared to existing resources due to new tasks and developments should be further clarified, it points out that the critical and highly critical FTE needs related to current additional tasks reflected in its AAR 2022 and new legislative tasks within the programming period (2024-2026) amount to the equivalent of 21 FTEs.

As highlighted in the AAR2022 adopted by the Management Board, a total of 10.5 FTEs were transferred from other work program activities to deliver the support action in preparation for its implementation in the course of 2023. This represented 15,9% from the total operational human resource used by ENISA in 2022. As a result, ENISA had to deprioritize and/or scale down other activities in 2023 and the expected continuation of the support action into 2024 and 2025 would result in ENISA needing to keep deprioritising its operations in other areas for the duration of the multiannual programming period, to be able to retain the human resourcing the support action requires.

The outcome of legislative process might also put further strain on ENISA human resources in the forthcoming multiannual programming period and would require the Agency to scale down its current operational activities even further, as noted above in section 2.2 outlook for the years 2024-2026

The Agency has already addressed some of the critical needs through reallocating posts to respond to highest criticality needs including by restructuring functions, using internal mobility, assignments to permanent teams, rotation to sensitive functions etc.

Thus there is almost no room left to use internal reallocation of posts to increase the Agency's operational human capacity, without deprioritising further its existing tasks and functions. Furthermore, due to already existing shortfall in terms of FTE needs, there are only limited budgetary resources which could be used to explore further outsourcing of some administrative and corporate functions, in order to liberate additional staff posts for operational purposes. However, the Agency has developed a cost model under which operational budget lines contribute into outsourcing some technical tasks now performed by operational staff (project administration and support), liberating some additional FTE's. Also, in this vein some of the additional funds reallocated to ENISA through continuation of ENISA support action could be used to explore options to increase temporarily the number of Contract Agents the Agency employs for supporting relevant operational tasks, without exposing the Union budget to any financial obligations in the long term.

Though the Agency has actively pursued and will continue to pursue number of avenues to build and exploit efficiency gains internally and also externally by developing joint operational and administrative services with other EUIBAs (CERT-EU, ECCC, EU-LISA, CEDEFOP and EUAN), the efficiencies actually gained from these joint approaches – in

[24] Following the decision of the Management Team of ENISA to conduct the internal workforce needs assessment for the period 2023-2025, the Heads of Units (HoU) and permanent Team Leaders (TL) were requested to put forward their initial analysis in three parts. Firstly, by indicating main challenges which affect their unit/team in implementing the annual and multiannual objectives and priorities enshrined in the draft Single Programming Document of 2023-2025, and if relevant linking those challenges with reported gaps or shortcomings within the adopted Annual Activity Report 2021 or the comments from MB members during the discussion in June 2022. Secondly, they were requested to define the medium and long-term needs of their units and teams by outlining main legislative, political and cybersecurity developments and trends and how these overall challenges will change the tasks and responsibilities of the unit/team for the coming years (2023, 2024, 2025), and assessing the overall human resources needs in the long term (n+3) perspective including key competences (max 5) that the unit should develop/strengthen (on the basis of existing ENSIA competencies map). Finally, they were requested to define additional functions which the unit/team should be able to perform in short term perspective (n+1), indicating the competencies (and their level) which are intrinsic to those functions. They were also requested to indicate whether to fulfill new functions via internal mobility or recruitment and put forward proposals how to restructure or suppress existing functions within the unit/team if the additional resource requests cannot be addressed by the Agency.

terms of liberated FTEs – will, and also in the future, cover only a fraction of the assessed shortfalls in additional FTE needs.

Its Establishment Plan implementation rate is foreseen to reach close to 100% by end of 2023 (currently at 96% as of September 2023), and thus any unexploited resource means are not nearly sufficient for the Agency to meet its current foreseen workforce needs. The Agency's means will become even more inadequate as new legislative proposals get adopted – e.g. the criticality and priority of related workforce needs increases – during the end of the current programming period of 2024-2026.

Thus, by the end of 2024, if the already announced legislative and political expectations towards the Agency will materialise ENISA's budgetary and human resource means shall be drawn to their absolute limits. Unless the FTE needs stemming from potential new tasks are addressed, the Agency will need to limit and deprioritise its existing operational activities in 2025 and 2026 within the programming period of 2024-2026, in order to reallocate FTEs to new emerging tasks. This will in turn limit ENISA's ability to deliver its overall mandate and objectives in their entirety.

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 2024 and may use this option in the future to offset long-term absences and part-time work with short term contracts of CA.

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

Given the current constraints of its resources but also in order to fulfil its strategic corporate objectives – including setting the pace of its staff development and greening objectives – ENISA will remain committed to the continuous improvement of its efficiency across its operational and corporate / administrative tasks.

2.4.1. Strategy to achieve operational efficiency gains

Within the programming period 2024-2026 ENISA will continue develop and review its operational service packages, to ensure internal alignment and synergies between its structural entities (operational units and teams) and prioritise its resources. In order to handle the new challenges and tasks given to the Agency, or those that may arise once the legislative proposals are agreed and adopted, , ENISA might need to pursue targeted structural adjustments to consolidate capacity across some operational units and permanent teams to be able to provide its key services.

Beyond and on top of further elaborating and updating the service packages and internal structures, ENISA aims to build partnerships and strengthen synergies with a number of EU institutions, agencies and bodies. This includes by proposing joint operational objectives and KPIs in the respective work programs, thus further utilising external support and mobilising external resources for the benefit of ENISA operational objectives when those are aligned with the objectives of prospective partners. The main current and possible partnerships and/or prospective cooperation frameworks across its operational activities shall include:

Activity 1: leveraging ENISA's existing participation in the OECD Working Party on Security in the Digital Economy (SDE) to identify good practices among OECD members and assess their relevance for EU policy initiatives under development.

Activity 2: the MoU with the **European Railway Agency** (ERA) is planned for signing in Q4 2023 and an extension of the current MoU with the **European Banking Authority** (EBA) and others to align ENISA's support for MS under the critical sectors of NIS2 with the activities of the Union bodies in these sectors exchanging of good practices with OECD nations and other EU policy initiatives under implementation.

Activity 3: further utilise **structured cooperation with CERT-EU** in developing and deploying exercises and trainings for EUIBAs, and in view of the resource constraints also develop cost-based training and exercises services for EUIBAs, to address demands for ENISA support for which currently there are no additional resources, building on the example of SLA with **EU-Lisa.** In addition, an MoU with the **European Security and Defence College** was signed in 2023 establishing strategic cooperation in areas of common interest with a view to addressing common concerns such as the cybersecurity training and education, development of e-learning material, cyber capacity building, a skills certification framework, the Cyber Skills Academy.

Activity 4 & 5: develop further the **structured cooperation with CERT-EU** (including carrying out the mandatory review of the existing MoU) by exploring further the possibilities of joint products which contribute to achieving of the objectives of the activities. Cooperating with the **European Commission's Cyber Situation and Analysis Centre** to utilise synergies in order to serve ENISA mandate under article 7 of the CSA. In addition, ENISA cybersecurity support action synergises with Article 6 and 7 of the CSA.

Activity 6 & 7: formalised a cooperation arrangement with **CEN-CENELEC** and ETSI anda joint cybersecurity market observatory with **European Cybersecurity Competence Centre** (ECCC)

Activity 8: Working together with the 3 DORA European Supervisory Authorities (EBA, ESMA, EIOPA) concerning the implementation of incident reporting under DORA and its alignment with the corresponding NIS2 requirements. In the context of the EU-US cyber dialogue, relevant workstream on incident reporting with US counterparts (DHS, CISA) to map relevant initiatives. Regular discussions with Eurostat and European Commission concerning the implementation and operationalisation of the EU cybersecurity index and its comprising qualitative and quantitative indicators.

Activity 9: developing joint objectives (with relevant programming KPIs) with **ECCC** to help to tackle skills gap in cybersecurity b under European Cybersecurity Skills Framework as foreseen in the Commission's communication on "European Cybersecurity Skills Academy". In addition, utilise the new cooperation arrangements with **CISA**, **NATO** and **Ukraine** to enrich EU cybersecurity knowledge and information.

Activity 10: formalised the structured cooperation with **ECCC** via an MoU to coordinate research initiatives with other work programme activities.

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

2.4.2. Strategy to achieve corporate and administrative efficiency gains

ENISAs strategy for achieving efficiency gains has been formalised in its Corporate Strategy, which shall encompass its human resources strategy, greening and digital strategy and service modelling, which was approved by the MB in June 2023.

The Corporate Strategy (including HR strategy) presents a vision for a contemporary, flexible and values-driven organisation that empowers staff to deliver outstanding results for people across the EU and beyond. This strategy addresses ENISA's ambition to perform at the highest level in the interests of Europeans and the needs of its staff members to have an attractive workplace and a fulfilling career where excellence and effort are rewarded. Founded on European Commission strategies and practices[25], ENISA will strive to maximise the efficiency of its resources by maintaining its focus on developing a flexible, highly skilled and fit-for-purpose workforce that would support ENISA's goals to enhance its capabilities in future-readiness and continue its path towards an agile, knowledge-based and matrix way of working. 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. This strategy also aims to enhance personal accountability, responsibility and growth, and sets out a common vision in which all staff will work in a trust-based environment through the introduction of new technologies that facilitate modern and flexible work practices.

As ENISA aspires to become a trusted partner at EU level, it will continue to provide customer-focused, multi-disciplinary teams that demonstrate a customer centric, can-do and agile attitude. Open and dynamic workspaces,

[25] People first – Modernising the European Commission; Towards a Next Generation Digital Commission; Commission welcomes political agreement on the European Year of Skills – Employment, Social Affairs & Inclusion – European Commission; and 2021-2027 Strategy for the EU Agencies Network

matrix type operational set ups and collaborative IT tools will enable an integrated culture that will be able to act rapidly to increasingly complex policy challenges beyond the remit of a single service or unit. While the strategy reflects ENISA's broader corporate and long-term vision, it is also aligned with and supported by ENISA's Internal Control Framework (ICF), which is designed to provide reasonable assurance regarding the achievement of objectives set out in ENISA's Financial Regulation and retain credibility with the European Commission and Member States. While implementing the path in this direction ENISA will need to review and redesign its processes, policies and SOPs, promote self-service functionalities and build on collaborative ways of working, while redesigning job roles and investing in staff development. The founding principles of the strategy will be implemented via the SPD and annual work plans.

In order to enable the achievement of the above, the Corporate Strategy sets the following benchmarks which affect the Agency's budgetary and human resource planning in 2024-2026:

- the Agency's investment into talent development is a minimum 4% of expenditure foreseen for the salaries of staff in active employment;
- the Agency's welfare (excluding medical) expenditure is at a maximum of 5% of expenditure foreseen for the salaries of staff in active employment;
- the Agency's expenditure on movable property and related costs for retaining a modern workplace is at a maximum of 1% of expenditure foreseen for the salaries of staff in active employment;
- corporate overhead which shall be budgeted from the expenditure of all operational activities to ensure technical support for essential corporate services shall not be higher than 7% of the aggregated operational budget (Title III);
- the Agency dedicates at least 20% of its total investments to core, corporate and operational IT systems in order to ensure the cybersecurity of these systems;
- starting from 2024, the Agency offsets 100% of its CO2, CH4 and N2O emissions (Approximately 150t) which will be generated across all its activities and as a result of its operations in the relevant budgetary period.

Beyond setting these benchmarks the Corporate Strategy aims to ensure that the Agency acts in the right way and exhaust efficiency gains before reinforcing areas of work with extra resources. Such initiatives should be seen as a holistic package and cover different pillars such as: activity and resources/service categorisation, capitalisation on shared services, strategic workforce planning, business and service optimisation among a few.

Strategic Workforce Planning

In 2022, ENISA has taken steps to shift from a traditional headcount methodology to strategic workforce planning. This will enable a forward looking, proactive, flexible and integrated approach in anticipating and addressing staffing gaps in order to build agile workforce needs and allocate resources where priorities are. To do so, ENISA is revamping its internal strategic workforce planning framework, with the aim to consolidate 'hard' workforce data with 'soft' competency aspects, adopt a new staffing strategy aligned with organisational priorities.

While continuing to monitor the staff allocation between operational and administrative units in order to ensure thresholds of MB decision MB/2020/9 are met, ENISA aims to identify the level of in-house resources in terms of numbers of staff and their skills and competences, review its job evaluation and job framework, and general redesign its staffing policy while determining future workforce needs not only based on workload indicators and workforce plans but also competency investments and shortages to address the gaps in skills and expertise. This is of particular importance, considering the highly changing and competitive 'niche' market of cybersecurity and in order to maintain ENISA's added value in the EU cyber eco-system.

The HR strategy which is part of the Corporate Strategy is based on the multi-annual planning of human resource needs and will be activity driven. Efficiency gains through the introduction of new tools, business process reviews or better organisation of the workload will be exhausted first before supplementing an area of work with extra resources. With the priority given to operational work, ENISA will ensure that its workforce is flexible and multi-skilled and can be redeployed swiftly to meet increasing or changing organisational needs. Emphasis is placed on competencies and demonstrating transferrable skills and competencies that are needed in order to meet broad operational needs. At the same time, ENISA will invest in the skills and experience of its current workforce and will endeavour to retain and develop its solid performers with the right skills and competencies. To do so, ENISA will introduce modern HR practices to support talent development as outlined in the Corporate Strategy, in particular prioritise change & revision of some

key MB decisions such as L&D, middle management, appraisal and reclassification. It will further invest on building partnerships with accredited providers in and invest in competency development for both technical and soft skills. In parallel, ENISA would further proceed with its pilot of 2023 in linking L&D with the results of multi-source feedback evaluation and provide and introduce a job complexity and job grade standards.

Business process review and service optimisation

ENISA also intends to assess and analyse sustainability of existing processes, explore alternative models for providing indirect support and propose actions to ensure operational efficiency without compromising the activities of the operational units. Within the context of its Corporate Strategy, the overall operating business model of the support units would continue to be reviewed in order to ensure that the MB 2020/09 thresholds and requirements of the Corporate Strategy are met.

Digitalisation of services, self-service functionalities and service optimisation will be also at the core of the future way of working and ENISA's corporate strategy to build an agile workforce. ENISA will continue to review and explore possibilities to reengineer its processes, with a view to optimising service quality and cost-effectiveness, for instance by:

- Exploring and piloting changes in service levels and modalities, to improve added-value and cost-efficiency, such as shifting from owned to leased solutions, from manual entries to centrally managed solutions;
- Identifying activities and services that may be downsized and discontinued if needed;
- Continuously streamlining and automating administrative workflows to improve staff's productivity, by removing redundant steps and capitalising on new technologies such as making use of DIGIT services and tools,
- Reviewing ICT infrastructure and related technologies to reduce duplication of components and optimise maintenance and capital replacements such as for storage or move towards cloud-based solutions;

Besides the above, most of ENISA's administrative tasks are supported by EU Tools such as accrual-based accounting (ABAC), Sysper for human resource management and for missions and document approvals and registry. In the course of 2023, ENISA onboarded Advanced Record System (ARES) Missions Integrated Processing System (MIPS+),Public Procurement Management Tool (PPMT) ServiceNow as a key ticketing & service management tool, an online recruitment platform, Allegro, as well as continue on progressing on onboarding Sysper Modules and switched to web-based ABAC platform and expanded the usage of ABAC functionalities The Agency has started also exploring to introduce new modules on contract management as ABAC LCK and redesign financial workflows via PPMT/ARES.

In 2023 the Agency has continued supporting the EU Agencies network in relation to the implementation of cybersecurity requirements proposed in the draft regulation on common binding rules on cybersecurity for EUIBAs, namely though a concept of shared services on cybersecurity risk management, such as the concept of a virtual CISO. This concept is developed in close cooperation with CERT-EU and another six EU agencies[26] that volunteered to join this initiative.

In its corporate functions, ENISA further seeks to rationalise its internal processes to improve its overall efficiency and to benchmark its activities with the best practices implemented by other EU Institutions and Agencies. In area of facility management and security, in 2023 ENISA completed the chartography of facility and security service. In applying further efficiencies in the area, as of 2024 onwards, the Agency aims to merge and simplify its administrative expense

[26] EU-LISA, European Training Foundation (ETF), European Maritime Safety Agency (EMSA), European Public Prosecutor's Office (EPPO), European Institute of Innovation & Technology (EIT), CEDEFOP, CERT-EU and The Trans European Services for Telematics between Administrations (TESTA) system.

as a result of using multitude of contracts and reduce the usage of framework contracts via applying integrated service models for soft services (security and facility management and AV). This will be further supported by exploring additional modules of ServiceNow and integrating facility management and security requests via all-inclusive service packages.

As a priority, in 2023, the Agency conducted an independent analysis of its financial procedures and processes which resulted with options for further simplifications in the execution of its budget implementation, and more flexible application of the budget expenditure in full compliance with the legal and financial framework. In 2024, priority will be given in business redesign and implementing revised financial business model decisions and service model, explore insourcing/outsourcing options as well as on redesigning and streamlining key HR processes which are quite outdated, in line with its corporate and HR strategy.

Capitalising on shared services

In line with the call for agencies to promote the use of shared services, ENISA will continue to seek efficiency gains and build partnerships through initiatives such as:

- Sharing services with other agencies and/or the Commission, including e.g. interagency and inter-institutional procurements, common services with CEDEFOP and European Cybersecurity Competence Centre (ECCC) and use of Commission ICT solutions such as those for human and financial resources management; namely sharing accounting and data protection with ECCC as of January 2023.
- Explore further synergies with other EUIBAS in running joint calls and competitions of HR and engage in shaping job-sharing or secondment regimes with other EUIBAS;
- Prioritise the introduction of modern HR information systems and join forces with EC on the new HR Transformation roadmap and other modern cloud-based solutions.
- Explore further synergies with PMO on reimbursement of experts and EPSO of running calls and accessing reserve lists;
- Contributing to further promoting shared services among agencies through the different networks, particularly in the areas of procurement, HR, ICT and risk and performance management, data protection, information security, accounting etc;
- Contributing to the improvement and piloting of IT services with DG HR, and DIGIT in the area of HR and financial management;

SECTION III. WORK PROGRAMME 2024

This is the main body of the Work Programme describing, per operational and corporate activity, what the agency aims to deliver in the respective year towards achieving its strategy and the expected results. In total eleven operational activities and three corporate activities have been identified to support the implementation of ENISA's mandate in 2024.

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

Stakeholders and engagement level
Stakeholders' management is instrumental to the proper functioning and implementation of ENISA' work programme. On 29 March 2022 Management Team adopted the ENISA's Stakeholders Strategy. This Strategy lays down the main principles and approach towards stakeholders' engagement at Agency-wide level. The implementation of the Stakeholders Strategy is linked with the implementation of the Single Programming Document (SPD) via the activities. Each activity includes a list of stakeholders and the expected or planned engagement level for each stakeholder. The engagement level refers to the degree of the stakeholder's interest and influence in the activity for stakeholders classified as either partner or involve / engage, Stakeholders classified as "Partner" refers to stakeholders with high influence and high interest, usually business owners and others with significant decision-making authority. They are typically easy to identify and to engage with actively. Whilst stakeholders classified as involve / engage have a high influence and low interest. These are typically stakeholders with a significant decision-making authority but lacking the availability or the interest to be actively engaged.

KPIs / metrics
In 2020 the Agency developed and introduced a new set of key performance indicators and related metrics for measuring performance of the activities. These metrics are inscribed in the Single Programming Document for each activity and are made up of both quantitative and qualitative metrics. Quantitative metrics are those that measure a specific number through a certain formulae. Where as qualitative metrics are those that are more of a subjective opinion based on the information received, however even these are quantified in order to be interpreted and measured. The work programme for 2024 includes indicators for measuring strategic objectives, indicators and targets for measuring the activity objectives and indicators at the output level to measure the performance of the outputs. Many of the proposed indicators have been taken from the cybersecurity index pilot run by ENISA in 2022 and will eventually be superseded by the NIS2 directive indicators to monitor high level progress towards general objectives.

3.1 OPERATIONAL ACTIVITIES

Activity 1 Providing assistance on policy development

OVERVIEW OF ACTIVITY

The activity seeks to bolster policy initiatives on novel/emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. ENISA will support the EC and MS on new policy initiatives[27] through evidence-based inputs into the policy development process. ENISA, in coordination with the EC and Member States will also conduct policy monitoring to support them in identifying potential areas for policy development based on technological, societal and economic trends, identify gaps, overlaps and synergies among policy initiatives under development, as well as develop monitoring capabilities and tools to regularly and consistently be able to provide advice on the effectiveness of the existing Union policy and law in accordance with the EU's institutional competencies in the area via the Cybersecurity Policy Assessment (CSPA) service.

This activity also contributes to the service package INDEX by providing data used in the cybersecurity index (Activity 8), by providing input that can be used for future certification schemes (CERTI service package) and by providing findings and recommendations for the service packages offered to critical NISD sectors (Activity 2).

The added value of this activity is to support the decision makers in evidence-based policy making, in a timely manner and to inform them on developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework. Given the cross-cutting nature of cybersecurity across the policy landscape, the activity will provide an up-to-date risk- based analysis of cybersecurity not only in the areas of critical infrastructure and sectors, but also by providing advice across the field in an integrated and holistic manner.

The legal basis for this activity is Article 5 of the CSA.

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO2. Cybersecurity as an integral part of EU policies	1. Uptake of policy recommendations adopted within the biennial report on the state of cybersecurity in the Union[28]. 2. Effectiveness of EU relevant policy initiatives taking cybersecurity into consideration

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
1. A Improve the effectiveness and consistency of EU cybersecurity policies	Art.5 CSA	2026	Assessment of ENISA advice and its influence on EU policy (stakeholder centric survey)	75% stakeholder satisfaction from ENISA's advice and influence (among EU policy makers)

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
1.1 Advise the EC and Member States in reviewing the effectiveness of current cybersecurity policy frameworks	Stakeholders will use evidence to understand how implemented policies have affected the targeted entities	DG CONNECT NIS CG NLOs	Stakeholder satisfaction[29]	Biennial (Survey)	93%	>90%
			Number of contributions to policy development activities	Annual (Internal report)	21	30

[27] Policy initiatives such as the Cyber Resilience Act and the Cyber Solidarity Act as well as initiatives on Artificial Intelligence (AI), 5G, , Data Governance Act / big data,data spaces, digital resilience and response to current and future crises

[28] As part of the report of the state of cybersecurity in the Union ENISA shall include policy recommendations with a view to addressing shortcomings and increasing the level of cybersecurity across the union [Art 18(2) of NIS2]

[29] Stakeholder satisfaction conducted every two years to measure the take up of results / outcome, added value, duplication of ENISA work etc by stakeholders

			(reports, papers, opinions, participation in workshops etc.)			
1.2 Advise the EC and MS on new policy development, as well as carrying out preparatory work	Stakeholders will use ENISA's advice to develop effective and consistent EU cybersecurity policies	DG CONNECT and other DGs or EUIBAs depending on policy file owner.	Stakeholder satisfaction	Biennial (Survey)	93%	>90%
			Number of EU policies supported by ENISA	Annual (Internal report	7	5
			Number of contributions to policy development activities (reports, papers, opinions, participation in workshops etc.)	Annual (Internal report)	21	30
1.3 Monitor and analyse new and emerging policy areas	Stakeholders are informed in a timely manner about gaps, overlaps and inconsistencies across EU policy initiatives under development	NLOs NIS CG DG CONNECT and other DGs or EUIBAs depending on policy file owner	Stakeholder satisfaction	Biennial (Survey)	93%	>90%

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: DG CNECT, other DGs and Agencies, NIS Cooperation Group and relevant work streams, ENISA National Liaison Officers

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

Resource forecast

Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 1.1	INDEX, SITAW, NIS, CERTI	0,95	300.000	0,00	7.135	0,10	0	1,05	307.135
Output 1.2	NIS, CERTI	2,00	8.000	0,25	7.000	0,10	0	2,25	15.000
Output 1.3	NIS, CERTI	0,7	18.000	0,25	17.000	0,00	0	0,95	35.000
Activity total	FTE: 4.25 Budget: 357.135								
Actual resources used in previous year (2022)	FTE: 4,8 Budget: 354 406								

Activity 2 Supporting implementation of Union policy and law

OVERVIEW OF ACTIVITY

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

Under this activity ENISA provides support to the NIS Cooperation Group, its workstreams, and the implementation of its work program. In this period the focus is on supporting the NIS2 transposition, the NIS2 implementing acts, and the implementation of new tasks under the NIS2, like the EU registry for digital infrastructure entities. Under this activity ENISA also supports the Union risk evaluations processes (Nevers, Council Cyber risk posture[30]), follows up on the 5G toolbox (a previous union risk evaluation), delivers a methodology for Union risk evaluations and the building of sectorial risk scenarios, delivers sectorial situational awareness, and runs a yearly NIS360 for assessing maturity and criticality of sectors across the board.

Besides the horizontal outputs, which address sector-agnostic cross-cutting issues, this activity has a sectorial output, which addresses sector-specific issues, with a focus on increasing cybersecurity in the NIS sectors, via targeted service bundles ('sustain', 'build', 'involve', 'prepare'). Currently, we focus our limited resources on low-medium maturity and/or high criticality sectors like telecoms, digital infrastructures (e.g. core internet), energy-electricity, health, and rail. Very limited preparatory work is ongoing in a few sectors, like gas, public administrations and space. This sectorial output also provides relevant sectorial input to other SPD activities, such as cyber exercises (Activity 3), situational awareness (Activity 5), knowledge and information (Activity 8), and awareness raising (Activity 9), allowing these activities to better target sectorial stakeholders.

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

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

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO2. Cybersecurity as an integral part of EU policies	Level of maturity of cybersecurity capabilities and resources across the Union at sector level[31]

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

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

			reporting and security measures) and DORA provisions in survey of JC-DOR and NISCG	say NIS2 and DORA are aligned on these topics

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
2.1 Support Member States and the EC in the implementation of the NIS CG work program and the NIS directive	Member States will use ENISA advise to implement the NIS Directive.	DG CNECT, NIS CG	Stakeholder satisfaction[32]	Biennial (Survey)	94%	>90%
			EU register for digital entities is used by all MS	Biennial (Survey)	n/a	Used by all MS
			CVD guidance is implemented by MS and all MS are on the CVD map	Biennial (Survey)	n/a	Used by all MS
2.2 Support Member States with union-wide risk evaluations and union toolboxes scenarios	Support Union-wide risk evaluations and risk scenarios Follow-up of previous union-wide risk assessments (5G, Nevers) Sectorial situational awareness reporting	DG CNECT, NIS CG	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of stakeholders involved in the NIS360	Annual (Internal count)	n/a	120
			Number of sectorial situational awareness reports	Annual (Internal count)	6	12
2.3 Improve cybersecurity and resilience of the NIS sectors	Stakeholders use the NIS service packages to improve security and resilience of the sectors	DG CNECT, NIS CG, sectorial DGs, sectorial EU agencies	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)	Annual (Internal count)	3	4
			Number and frequency of services delivered to NIS sectors according to	Annual (Internal count)	21	24

[32] Results / outcome taken up, added value, duplication of existing work etc and effectiveness of ENISA guidance to help MS implement their tasks and deliver the NIS CG work program

			the maturity of the sector			

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

Involve / Engage: NLOs, Operators of essential services and digital service providers under NIS1 and overall entities in scope of NIS2 and industry associations/representatives

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 2.1	NIS, SITAW	4,00	183.268	0.25	39.500	0,25	-	4,50	222.768
Output 2.2	NIS, SITAW, TREX	3,75	167.500	0,25		0,25	-	4,25	167.500
Output 2.3	NIS, SITAW, CERTI, TREX	3,00	330.000	0,50		-	-	3,50	330.000
Activity total	FTE: 12.25 Budget: 720.268								
Actual resources used in previous year (2022)	FTE: 9,75 Budget: 780 925								

Activity 3 Capacity Building

OVERVIEW OF ACTIVITY

This activity seeks to improve and develop the capabilities of Member States, Union Institutions, bodies, and agencies, as well as various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the Union. This is achieved through the development of frameworks (Risk management, strategies, etc.) that are based on lessons learnt from MSs through the implementation and development of their National Cyber Security Strategies.

Actions to support this activity includes the organisation of large scale exercises, sectorial exercises and trainings and others[33]

In addition the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem including cross-border, and assist in reviewing and developing national and Union level cybersecurity strategies.

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

The legal basis for this activity is Articles 6 and 7(5) of the CSA.

Compared to the outputs under Act3 of previous years, in 2024 due to reduced funds it was decided to supress

- Output 3.4. Following the development of the RM framework by ENISA the next steps are following an iterative to review the framework and update it. This process may obviously also be carried out on a less frequent than annual basis.
- Output 3.5. In 2022 and 2023 the main role of ENISA was to support the EC in launching the initiatives in support of SOCs. This activity now is taken over mainly by the ECCC.

Regarding Output 3.6 the addition of private sector sponsors supproting the activities of Team Europe allowing ENISA to reduce the amount of spending in this domain .

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO4: Cutting-edge competences and capabilities in cybersecurity across the Union	Aggregated assessment of the level of cybersecurity capabilities in the public and private sectors across the Union[34]. Aggregated assessment of the level of maturity of national cybersecurity capabilities and resources as well as the extent to which MS national cybersecurity strategies are aligned[35]

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
Objective 3.A. Increase the level of alignment and cooperation within and between Member States as well as sectors, EU institutions, bodies and agencies	Art.6 CSA Art.9 CSA	2024	Number of MS that use ENISA support and tools on the implementation review and update of their NCSS.	All MS that have reviewed their NCSS use ENISA support and tools.
Objective 3.B Prepare and test capabilities to respond to cybersecurity incidents	Art.6 CSA	2024	Proportion of beneficiaries who take part in relevant ENISA exercises and trainings Added-value of ENISA exercises and trainings	All MS participate in Cyber Europe 2024 >80% of EUIBs have participated in JASPER exercises over 3 years (number of

33 CSIRT trainings and Capture the Flag (CTF) and Attach Defence (AD) competitions.
34 As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)b
35 As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e

				participants in 2024 increases compared to 2023) 90% participants see positive added value
Objective 3.C Increase skill sets and align cybersecurity competencies	Art.6 CSA	2024	Assessment of average level of cybersecurity technical competences of participants in European cybersecurity challenge finals Number of participants that take part in national competitions improving cybersecurity skills and capabilities Level of alignment of cybersecurity competences across the Union	A relevant metric is in the process of being developed in the ENISA security index. More than 10.000 participants take part in the annual CTF competitions that are organised prior to the ECSC final MS national competence frameworks are aligned with European Cybersecurity Skills framework

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
3.1 Assist MS to develop, implement and assess National Cybersecurity Strategies	Increase the level of preparedness and cooperation Prepare capabilities to respond to cybersecurity incidents Increase skill sets Align cybersecurity competencies Improved national cybersecurity strategies	NLO subgroup on National Cybersecurity Strategies	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Maturity of national cybersecurity strategies, ISACs, SOCs etc	Annual (Report)	N/A	N/A
3.2 Organise large scale biennial exercises and sectorial exercises	Increase the level of preparedness and cooperation Prepare and test capabilities to	NLO Network (as necessary) CSIRTs Network (as applicable)	Stakeholder satisfaction	Biennial (Survey)	91%	90%

	respond to cybersecurity incidents Stakeholder test and improve capabilities and increase capacity	EU-CyCLONe members (as applicable) NIS Cooperation Group (as applicable) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as applicable)	Evaluation of capacity building actions by participants in exercises and trainings	Annual (Report)	40% high usefulness 53.5% medium usefulness 6.5% low usefulness	>50% high usefulness
			Number of participants in trainings and organized by ENISA	Annual (Report)		>500 (incl online exercises)
3.3 Organise trainings and other activities to support and develop maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS cooperation group (NIS CG), EU-CyCLONe and work streams, information sharing and analysis centers (ISACs) and other communities	Increase the level of preparedness Prepare capabilities to respond to cybersecurity incidents Increase skill sets Stakeholders improve capabilities and skill set	NLO Network (as necessary) CSIRTs Network (as applicable) EU-CyCLONe members (as applicable) NIS Cooperation Group (as necessary) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as necessary)	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Number of participants in trainings and challenges organized by ENISA	Annual (Report)	N/A	>1.000 (incl online trainings)
3.4 Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)	Align cybersecurity competencies Increase skill sets	ECSC Steering Committee (NLO Subgroup)	Stakeholder satisfaction	Biennial (Survey)	91%	90%

STAKEHOLDERS AND ENGAGEMENT LEVELS

Involve / Engage: Cybersecurity professionals, Private industry sectors (operators of essential services such as health, transport etc. or generally entities in scope of NIS2), EU Institutions and bodies, CSIRTs Network and related operational communities, European ISACs, EU-CyCLONe members, NISD Cooperation Group, Blueprint stakeholders, SOCs, including National and Cross-border SOCs.

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 3.1	TREX, INDEX	2,00	70.000	0,00	0	0,00	0	2,00	70000

Output 3.2[36]	TREX, NIS	3,35	500.000	0,00	0	0,00	0	3,35	500.000
Output 3.3	TREX	4,30	546.591	0,00	0	0,00	0	4,30	546.591
Output 3.4	TREX	2.3	120.000	0,00	0	0,50	0	2,8	120.000
Activity total	FTE: 12,45 - Budget: €1.236.591[37]								
Actual resources used in previous year (2022)	FTE: 10.32 Budget: 1 921 221[38]								

[36] By the end of 2023 ENISA expects to sign a new multi annual Service Level Agreement with eu LISA to provide support on exercises.
[37] In addition 120.000 from SLA with EU-LISA see annex XI
[38] Carried over into 2023: EUR 328 339

Activity 4 Enabling operational cooperation

OVERVIEW OF ACTIVITY

The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities.. The main goal of the activity is to provide support and assistance in order to ensure efficient functioning of EU operational networks and cyber crisis management mechanisms. ENISA, as mandated by the NIS2, provides the organizational support and tools for both the technical(EU CSIRTs Network) and operational layer (EU CyCLONe - Cyber Crises Liaison Organisation Network) of Union operational cooperation networks. Under this activity ENISA is supporting operational communities through helping to develop and maintain secure and highly available networks / IT platforms and communication channels in particular ensuring maintenance, deployment and uptake of the MeliCERTes platform[39] and the EU Vulnerability Database. . As such, this activity could also frame prepare some of ENISA's proposed tasks in coordinating information and notification about vulnerabilities at the Union level as outlined in the Commission's legislative initiative on CRA.

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

ENISA will contribute to the next steps in enhancing the EU cyber crisis management framework following the NIS2 and the 2022 Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises'. In addition, this activity supports the ENISA Cybersecurity Support Action[40].

This activity contributes to the Situational Awareness, INDEX and NIS service packages.

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

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO3: Effective cooperation amongst operational actors within the Union in case of massive cyber incidents	Level of cooperation and availability, (disruptions) and utilisation and trust of Union level networks, tools and databases.

GENERAL ACTIVITY OBJECTIVE	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
4.A. Enable trust and effective cooperation and operations of CSIRTs Network and EU-CyCLONe members.	Article 7 & NIS2	2024	Satisfaction with scalable ENISA support Maturity of operational communities	80% of satisfaction of stakeholders Average overall level of maturity increases year by year
4.B. Ensure a high level of coordination of the Vulnerability Disclosure Services within the Union.	Article 7 & NIS2	2026	EU vulnerability database usage and added-value	EU Vulnerability Disclosure Services are gradually available (Numbering Services in place) and aligned with

					national mechanisms . EU vulnerability database functional and aligned with national mechanisms
4.C. Robust and secure tools/ platforms are established, and actively utilised to facilitate seamless operational collaboration at the Union level.		Article 7 & NIS2	2024	Continuous operations and use of secure communication tools and platforms for EU-CyCLONE and CNW including the use of regular checks and controls.	No significant disruption or incidents in the working of operational tools and platforms recorded against standard checks and controls Beneficiaries use the tools

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs Network and EU-CyCLONe members.	Enhanced Information Sharing and cooperation among the CSIRTs Network and EU-CyCLONe members.	CSIRTs Network and EU-CyCLONe members.	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)	N/A	
4.2 Design and architect processes and tools to build an EU Vulnerability Database in close cooperation with the Member States	ENISA provides numbering services for Common Vulnerabilities and Exposures with a view to gradually establishing EU Vulnerability Database.	CSIRTs Network and NIS Cooperation Group.	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)		
	Usage of the available tools		Stakeholder satisfaction	Biennial (survey)	89%	>90%

4.3. Operate, maintain and promote operational cooperation infrastructure for the Union Cyber security communities.		CSIRTs Network and CyCLONe members.				
			Number of users, both new and recurring, and usage per platform/tool/ SOP provided by ENISA	Annual (report)		>5% increase
			CSIRTs active users % increase year on year		19%	
			CSIRTs number of exchanges/i nteractions % increase year on year		104%	
			EU-CyCLONe active users % increase year on year		2%	
			EU-CyCLONe number of exchanges/i nteractions % increase year on year		548%	

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

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

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 4.1	NIS, SITAW	3,50	144.567	0	299.557	0	0	3,50	444.124
Output 4.2	NIS, SITAW	3,5	266.474	0	0	0	0	3.5	266.474

Output 4.3	SITAW, NIS	3,5	786.908	0	278.988	0	0	3.5	1.065.896
Activity total	FTE: 10,50 - Budget: €1.776.494								
Actual resources used in previous year (2022)	FTE: 5 Budget: €1 682 555[41]								

[41] Carried over into 2023: EUR 602 393

Activity 5a Contribute to cooperative response at Union and Member States level through effective situational awareness

OVERVIEW OF ACTIVITY

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

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

The activity supports the Union institutions, bodies, offices and agencies in public communication to incidents and crises. The activity also supports Member States with respect to operational cooperation within the CSIRTs Network and EU-CyCLONe by providing at their request advice to a specfic cyber threat, assisting in the assessment of incidents, facilitating technical handling of incidents, supporting cross-border information sharing and analyzing vulnerabilities, including through the EU Vulnerability Database (under development in Output 4.2).

This activity implements the structured cooperation with CERT-EU (please see Annex XIII Annual Cooperation Plan 2024) including general oversight over the cooperation, provides primary point of contact for the Cyber Crisis Task Force, and implement the agreements between ENISA and DG CONNECT for the contribution to the Commission Situation Center.

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

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

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

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO3: Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents	Risk level due to cyber threats is understood by the cybersecurity communities at Union level and decision makers are able to prioritize actions to manage the risk

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

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

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
5a.1 Collect, organise and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, operational and technical levels[42]	Establishment of a Threat Information Management Platform. Production of briefings, reports, and summaries of incidents, threats, and vulnerabilities Increased understanding and timely access to information regarding latest threats, incidents and vulnerabilities	CSIRT Network, EU CyCLONe, , EUIBAs, National Authorities within MSs subscribed to the products	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Timeliness and Accuracy of reports	Annual (survey)	N/A	
5a.2 Provide analysis and risk assessment jointly with other operational partners including EUIBAs, Member States, industry partners, and non-EU partners	Union joint assessment and reports, sectorial analysis, threat and risk analysis[43] Recipients receive accurate and timely assessment of threat actors and associated risk to the EU Internal Market	CSIRT Network, EU CyCLONe, EUIBAs, HWPCI, Management Board	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Number of contributing MSs and relevant EUIBAs	Annual (report)	N/A	
5a.3 Maintain, develop and promote ENISA Cyber Partnership programme aiming at information exchange to support the Agency's understanding of threats, vulnerabilities incidents and cyber security events	Establishment and operationalisation of the Cyber Partnership Programme	CSIRT Network, EU CyCLONe, EUIBAs, HWPCI, MB	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Number of new and total partners in the	Annual (report)	N/A 6	10/4

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

	ENISA Situational Awareness leverage private sector partnership to augment context and understanding of threats, vulnerabilities and incidents		ENISA partnership program			
			Percentage of RFI answered by members of partnership program	Annual (report)	N/A	80%

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

Involve / Engage: Other type of CSIRTs and PSIRTs

Resource forecast 2024									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 5a.1	SITAW, INDEX,NIS	4	1.280.459[44]	0	0	0	0	4	1.280.459
Output 5a.2	SITAW, INDEX,NIS	4		0	0	0	0	4	
Output 5a.3	SITAW	1,25	37.000	0	0	0	0	1,25	37.000
Activity total	FTE: 9.25 - Budget: 1.317.459[45]								
Actual resources used in previous year (2022)	FTE: 7,35 Budget: 842 992[46]								

[44] Includes allocation of 450.000 from Contribution Agreement related to Cybersecurity Support Action, refer to annex XI for further information and activity 5b
[45] Includes allocation of 450.000 from Contribution Agreement related to Cybersecurity Support Action, refer to annex XI for further information and activity 5b
[46] Carried over into 2023: EUR 276 749

Activity 5B: Contribute to cooperative response at Union and Member States level through ex-ante and ex-post services provision

OVERVIEW OF ACTIVITY

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

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

The types and level of services are agreed with single point of contact within each EU Members States and final beneficiary entities.

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

This activities is resourced through the use of 10 Contract Agents to be absorbed as direct cost of the programme and financed through Commission contribution agreement. ENISA will not be able to resource this activity with the current establishment plan. The budget for this activity is to be intended for 2024 through 2025[47]

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

Link to strategic objectives (ENISA STRATEGY)	Indicator of strategic objective
SO3: Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents	Level of preparedness and response to large-scale cross-border incidents

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET Target
5b.A Enhanced preparedness and effective incident response	Article 7	2025	Ability of ENISA to support EU Member States to further develop preparedness and response capabilities through implementation and delivery of ex-ante and ex-post services delivery	>4[48]

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
5b.1 Pentest and Threat Hunting services towards selected entities within EU Member States[49]	Pentest and Threat Hunting services are delivered timely and accurately to MSs	MSs, CNECT, Beneficiaries	% of MSs requesting the service Satisfaction score	Annual	N/A	50% >4
5b.2 Customized Exercise and Training for selected entities within EU Member States[50]	Customize Exercise and Training services are delivered timely	MSs, CNECT, Beneficiaries	% of MSs requesting the service Satisfaction score		N/A	50% >4

[47] Information on FTE calculation and Budget amount are pending final determination of the Contribution Agreement between Commission (DG CONNECT) and ENISA
[48] Target response to qualitative survey regarding ENISAs ability to support MS with a scale of 1 to 5, with 5 being the highest rating
[49] Beneficiaries of the Act5B services are specified in the [Contribution Agreement]
[50] Beneficiaries of the Act5B services are specified in the [Contribution Agreement]

	and accurately to MSs.					
5b.3 Risk Monitoring and Assessment for selected entities within EU Member States[51]	ENISA is able to provide regular risk monitoring towards specific targets or at national level, including by leveraging commercial of-the-shelf platforms, as well provide specific risk assessment and threat landscape as requested by MSs	MSs, CNECT, Beneficiaries	% of MSs requesting the service Satisfaction score		N/A	50% >4
5b.4 Support Incident Response and Incident management of selected entities within EU Member States[52]	ENISA provides 24/7 support for Incident Response to MSs	MSs, CNECT, Beneficiaries	% of MSs requesting the service Support was provided timely Satisfaction Score		N/A	50% >4

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States, Selected Beneficiary Entities, Commission

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

Resource forecast 2024

Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)[53]*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 5b.1	SITAW, NIS, INDEX, TREX	3,5[54]	19,55m[55]						19,55m
Output 5b.2	SITAW, NIS, INDEX, TREX								
Output 5b.3	SITAW, NIS, INDEX, TREX								
Output 5b.4	SITAW, NIS, INDEX, TREX								
Activity total	3,5 FTE and 19.550.000 Budget[56]								

[51] Beneficiaries of the Act5B services are specific in the [Contribution Agreement]
[52] Beneficiaries of the Act5B services are specific in the [Contribution Agreement]
[53] Cyber Support Action Programme
[54] This activity is resources through the use of 10 Contract Agents to be absorbed as direct cost of the programme and financed through Commission contribution agreement. The actual resources count will be available after finalization of the Contribution Agreement between Commission (DG CONNECT) and ENISA. The FTE represent the contribution of ENISA based on the current establishment plan.
[55] Information on FTE calculation and Budget amount are pending final determination of the Contribution Agreement between Commission (DG CONNECT) and ENISA. The budget for this activity is to be intended for 2024 through 2025. In addition 450.000 allocated to activity 5a
[56] Minus 450.000 allocated to activity 5a, please refer to annex XI for further details regarding contribution agreement

Activity 6 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

This activity encompasses actions that seek to establish and support the EU cybersecurity certification framework by preparing and reviewing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the Union Rolling Work Program. Actions also include maintaining and evaluating adopted cybersecurity certification schemes and participating in peer reviews. In addition, in this activity, ENISA assists the Commission with regard to the European Cybersecurity Certification Group (ECCG), co-chairing and providing secretariat to the Stakeholder Cybersecurity Certification Group (SCCG); ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Article 50 of the CSA. As from 2024, ENISA seeks to gradually support the cybersecurity certification stakeholders with an online platform that has been set up by the Commission. Furthermore, ENISA contributes to the cybersecurity framework by analysing pertinent aspects of certification along the lines of legislation adopted notably, NIS2, DGA as well as legal instruments in the legislative process that include the amendment to the CSA, CRA, EUDI Wallet, AI Act, Chips Act, Data Act, AI Act, amendment of CSA regarding managed security services certification etc.

The work under taken under output 7.4 has been absorbed within output 6.2

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

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

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO5 High level of trust in secure digital solutions	Citizens trust in ICT certified and non-certified solutions in the EU market

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
6.A Improve the certification requirements concerning security posture management of certified products, services, processes and gradually of managed security services	Article 8 and Title III	2025	Monitor ENISA take up of technical standards and technical specifications in support of EU legislation (document monitoring)	Applicable standards cybersecurity requirements have been considered by ENISA to promulgate better cybersecurity certification schemes
6.B Efficient and effective implementation of the European cybersecurity certification framework	Article 8 and Title III	2025	Number of stakeholders (public and private) in the internal market, implementing the cybersecurity certification framework for their digital solutions	A scheme is timely implemented across all relevant market sectors
6.C Increase use and uptake of European cybersecurity certification	Article 8 and Title III	2024	Number of schemes and additional requests addressed to ENISA by the Commission Number of schemes and additional requests processed by ENISA Uptake of certified digital solutions (products, services,	High number of private and public entities and/or market sectors relevant to a given scheme taking up certification after the entry into force of the implementing act

			processes and gradually managed security services) using certification schemes under the CSA framework as well as other directly applicable instruments i.e. CRA, EUDIW etc.	
6.D Increase trust in ICT products, services and processes	Article 8 and Title III	2025	Number of certificates issued and published under an EU certification scheme; high utilisation rate in the market.	High degree of visibility and utilisation of EU cybersecurity certificates

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
6.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes	Scheme meets stakeholder requirements, notably of the Member States and the Commission Take up of schemes by stakeholders Timely delivery of all schemes requested in cooperation with the Commission Statutory Bodies and ad hocWorking Groups actively involved	Ad hoc working groups on certification ECCG European Commission	Stakeholder satisfaction	Biennial (survey)	82%	75%
			Number of opinions of stakeholders managed	Annual (report)	n/a	100 opinion items per scheme
			Number of people/organizations engaged in the preparation of certification schemes	Annual (report)	N/A	At least 20 ad hoc Working Group Member from third-party Experts; at least 15 Member States joining ad hoc Working Groups
6.2 Implementing and maintaining of the established schemes including evaluation of adopted schemes, participation in peer reviews etc. monitoring the dependencies and vulnerabilities of ICT products and services	Review of schemes to improve efficiency and effectiveness Take up of schemes by stakeholders	Ad hoc working groups on certification ECCG European Commission	Stakeholder satisfaction	Biennial	82%	75%
			ENISA response to consolidated monitoring and maintenance requirements of schemes adopted	Triennial (survey)	N/A	75%
			Satisfaction of ENISAs role in NCCA peer reviews	Triennial (survey)	n/a	75%

6.3 Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks		ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			Feedback from statutory bodies including NCCAs on ENISAs role	Annual (survey)	N/A	75%
6.4 Developing and maintaining the necessary provisions and tools and services concerning the Union's cybersecurity certification framework (incl. certification website, support the Commission in relation to the core stakeholders service platform of CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework etc.)	Supporting in transparency and trust of ICT products, services and processes Stakeholders engagement promotion of certification	ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			Users satisfaction concerning the certification website services	Annual (survey)	N/A	75%
			Usage of certification website	Annual (report)	N/A	75%

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. National Cybersecurity Certification Authorities, ECCG), European Commission, EU Institutions, Bodies and Agencies Selected stakeholders as represented in the SCCG

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

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 6.1	CERTI, NIS	4,65	400 000	0,7		0,5	0	5,85	400 000
Output 6.2	CERTI	1,9	53 000	0	-	0	0	1,9	53 000
Output 6.3	CERTI	0,5		0		0	0	0,5	-
Output 6.4	CERTI	1,1	118896	0,15		0	0	1,25	118896
Activity total	FTE: 9,5 Budget: 571.896								
Actual resources used in previous year (2022)	FTE: 8,35 Budget: 959 343[57]								

[57] Carried over into 2023: EUR 277 604

Activity 7 Supporting European cybersecurity market and industry

OVERVIEW OF ACTIVITY

This activity seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence from outside and increase the capacity of the Union and to reinforce supply chains to the benefit of internal market. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation. As such, this activity also seeks to lay the ground for a robust role of ENISA in the CRA notably in terms of market analysis, preparation of market sweeps and reporting of exploited vulnerabilities etc. Actions to support this activity include producing analyses and guidelines as well as good practices on cybersecurity requirements, facilitating the establishment and take up of European and international standards across applicable areas such as for risk management as well as performing regular analysis of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein. Platforms for collaboration among the cybersecurity market players, improve visibility of trustworthy and secure ICT solutions in the digital single market.

Output 7.4 has been absorbed within output 6.2, whilst output 7.4 has been merged with Activity 6.

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

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO5 High level of trust in secure digital solutions	Monitor metrics such as number of certificates issued under an EU scheme; number of companies interested in EU certification; growth observed in the number of CABs / or EU certification functions thereof recorded in the MS.

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
7.A Foster a robust European cybersecurity industry and market	CSA Article 8 and Title III CRA proposal	2024	Stakeholders' satisfaction with of the ENISA survey State of the EU cybersecurity industry and market for products and services (index) Industry perception of the internal market (survey)	Improved ability of ENISA and the EU to analyse the EU cybersecurity market
7.B Improve the conditions for the functioning of the internal market	CSA Article 8 and Title III CRA proposal	2025	Better informed choices by users of products in market niches analysed	Improve the understanding of stakeholders on the cybersecurity market conditions in the EU

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
7.1. Market analysis on the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes	Improved understanding of the market / industry	Ad hoc working groups cybersecurity market analysis ECCG (as necessary) SCCG Advisory Group	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Cybersecurity market analysis; cybersecurity product and services	Annual (report)	N/A	All reports produced as planned (Y out of Y reports)

		NLO (as necessary)	analysis; analysis on vulnerabilities and dependencies in ICT products and services as appropriate; analysis if other relevant market areas			
7.2. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification	Alignment with standards	SCCG Advisory Group NLO (as necessary)	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification.	Annual (report)	N/A	All reports produced as planned (Y out of Y reports)

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. entities with an interest in cybersecurity market monitoring e.g. NCCA, National Standardisation Organisations) , European Commission, EU Institutions, Bodies and Agencies, European Standardisation Organisations (CEN, CENELEC, ETSI), Private sector or ad hoc Standards Setting Organisations European Cybersecurity Competence Centre.

Involve / Engage: Private Sector stakeholders with an interest in cybersecurity market and/or standardisation, International Organisation for Standardisation / International Electrotechnical Committee, Consumer Organisations

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 7.1	CERTI, INDEX, CERTI	4,15	130 000	0,1	0	0	0	4,25	130.000
Output 7.2	CERTI, NIS	2,75	136.666		0	0	0	2,75	136.666
Activity total	FTE: 7- Budget: 266.666								
Actual resources used in previous year (2022)	FTE: 4,35 Budget: EUR 366 473[58]								

[58] Carried over into 2023: EUR 105 230

Activity 8 Knowledge on emerging cybersecurity challenges and opportunities

OVERVIEW OF ACTIVITY

This activity delivers on ENISA's strategic objectives SO7 (efficient and effective cybersecurity knowledge management for Europe) and supports SO6 (foresight on emerging and future cybersecurity challenges). In particular, work under this Activity shall provide strategic long-term analysis, guidance, foresight and advice on current emerging and future cybersecurity challenges and opportunities.

These activities leverage on expertise of relevant legal, regulatory, economic and society trends and data by aggregating and analysing information. The strategic goal is to provide timely, reliable and useful information and knowledge (across the past-present-future timeline) to different target audiences as per their needs and contribute to the improvement of the state of cybersecurity across the Union.

Under this activity the Agency will map **threat landscapes** and provide topic-specific, as well as general, assessments on the expected societal, legal, economic, technological and regulatory impact, with targeted recommendations to Member States and Union institutions, bodies, offices and agencies.

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

In terms of knowledge management, ENISA will work towards consolidating data, information and indicators concerning the status of cybersecurity across MS and the EU.

Effforts in developing and maintaining the EU cybersecurity index and developing, reviewing and following up on the biennial report on the state of cybersecurity in the Union under Art.18 of NIS2 will continue.

This activity leads ENISA's efforts towards delivering the cybersecurity index (INDEX) service package, while in parallel contributing to the delivery of the NIS, TREX and situational awareness (SITAW) service packages

The legal basis for this activity is Article 9 and Article 5(6) of the CSA and Articles 18, 23(9) of the NIS2.

Compared to annual work programme of 2023, work related to the development of the infohub is suppressed and all existing and completed outcomes will be merged with the ENISA website.

Link to strategic objectives (ENISA STRATEGY)	Indicator for strategic objectives
SO6. Foresight on emerging and future cybersecurity challenges SO7. Efficient and effective cybersecurity information and knowledge management for Europe	Union level cybersecurity risk assessment and cyber threat landscape [adopted in accordance of Article 18(1)a]

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
8.A Knowledge and uptake of future challenges and opportunities by MS and Union actors.	Art.9 CSA	2025	Cybersecurity index indicator "emerging technology threats are considered by national risk assessments" Level of the acceptance of the report of the state of cybersecurity in the Union	European Parliament positive adoption] High take-up of the report by MS and Union actors All MS have considered at least 1/3 of the mapped emerging technology threats in assessing risk at national level
8.B Increase understanding of the state of cybersecurity	Art.9 CSA & eIDAS Art.10	2025	Use of Cybersecurity index by MS	All MS give input to cybersecurity index 2/3 of MS are using the

				index to inform their national cybersecurity strategies
8.C Deliver relevant and timely information	Art.9 CSA	2024	Usage of knowledge management portals, i.e. index, CIRAS, , etc. Value and usability of knowledge management portals	2/3of targeted stakeholders use the portals regularly 2/3 of Stakeholders are satisfied with the portals

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
8.1 Develop and maintain EU cybersecurity index	Measuring maturity Stakeholders can better prepare for future challenges based on indication of maturity	NISD CG, NLO, CSIRTs Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Uptake of the cybersecurity index	Biennial (survey)	N/A	20 MS representatives 60% satisfaction rate Agreement by all validating bodies
8.2 Collect and analyse information to report on the cyber threat landscapes	Mapping threats Generate recommendations for stakeholders to take up	NLO, AG and Cybersecurity Threat Landscape AhWG CSIRTs Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357	±5% compared to 2023
			Uptake of reports generated in activity 8	Annual (report)	N/A	±5% compared to 2023
8.3 Analyse and report on incidents as required by Art 5(6) of CSA as well as other sectorial legislations (e.g. DORA, eIDAS Art. 10, etc.)	Analysing incidents Generate recommendations for stakeholders to take up	WS3 of the NISD CG, ECASEC and eIDAS Art.19 groups	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			EU incident reporting maturity	Annual (report)	N/A	EU Average >50%

			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)		±5% compared to 2023
			Uptake of reports generated in activity 8	Annual (report)		±5% compared to 2023
8.4 Foresight on emerging and future cybersecurity challenges and recommendations.	Identifying future challenges and opportunities Generate recommendations for stakeholders to take up	Foresight AhWG, NLO and AG	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357	±5% compared to 2023
			The influence of foresight on the development of ENISA work programme	Biennial (ENISA SPD)	N/A	>2 emerging areas identified
			Uptake of reports generated in activity 8	Annual (report)	N/A	±5% compared to 2023

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: NISD CG WS3, ECASEC, eIDAS Art. 19 Group, Foresight ahWG, CTL ahWG, Index NLO subgroup

Involve / Engage: NLO/AG, CSIRTs Network

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 8.1	INDEX	2,75	181.982	0	0	0	0	2,75	181.982
Output 8.2	INDEX, SITAW, NIS	2	136616	0,25	0	0,15		2,35	136616
Output 8.3	INDEX, SITAW, NIS	1,2	178.791		0	0	0	1,2	178.791
Output 8.4	INDEX	1,1	207.257	0	0	0,1	7000	1,2	214.257
Activity total	FTE: 7,50 - Budget: 711646								
Actual resources used in previous year (2022)	[59]FTE: 10,9 Budget: EUR 1 043 564[60]								

[59] Activity 10 outputs and thus resources were undertaken within activity 8 in 2022.
[60] Carried over into 2023: EUR 81 543

Activity 9 Outreach and education

OVERVIEW OF ACTIVITY

The activity seeks to raise the overall awareness of cybersecurity risks and practices. in cooperation with Member States, Union institutions, bodies, offices and agencies and EU's international partners, it aims to build an empowered European community, with an allied global community which can counter risks in line with the values of the Union. Under this activity the Agency will be organising regular outreach campaigns, providing guidance on best practices and support coordination across MS on awareness and education. Moreover, the Agency will facilitate the exchange of best practices and information on cybersecurity in education between MS.

The added value of this activity comes from building communities of stakeholders which improve and enhance current practices in cybersecurity by harmonizing and amplifying stakeholder actions.

The activity will also seek to contribute to the Unions efforts to cooperate with third countries and international organisations on cybersecurity.

Based on the MB strategic discussions in June, the actions on the European cybersecurity Month have been suppressed and ENISA will only maintain coordination of the group of national coordinators going forward. In addition, the tasks stemming from the recently published EC Communication on the Cybersecurity Skills Academy are undertaken within this Activity; such as the implementation and uptake of EU cybersecurity skills framework and its review on a biennial basis; the consolidation of mapping of education institutions (CyberHEAD) and of the repositories of existing trainings and of cybersecurity certifications; the pilots for an attestation scheme for skills; the development of indicators and KPIs to measure the progress towards closing the cyber talent gap and collect associated data. The Agency will collaborate with all relevant actors while undertaking these tasks.

This activity contributes to the NIS, CERTI and TREX service packages. The legal basis for this activity are Articles 10 and 12 and Article 42 of the CSA.

Link to strategic objectives (ENISA STRATEGY)	Indicator
SO1. Empowered and engaged communities across the ecosystem SO4. Cutting edge competences and capabilities in cybersecurity across the Union	The % gap between demand and supply of cybersecurity skilled professionals General level of cybersecurity awareness and cyber hygiene among citizens and entities

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
9.A Increase awareness of cybersecurity risks and improve cyber-secure behaviour	Article 10	2025	Cybersecurity indicator "ENTERPRISES: STAFF AWARENESS Cybersecurity indicator "SME culture of cybersecurity" Number of cybersecurity incidents with human error as root course Cybersecurity index indicators "National culture of cybersecurity"	1% - 2% increase of Cybersecurity indicator "SME culture of cybersecurity" increases year by year Number of cybersecurity incidents in critical sectors with human error as root course decreases year by year in relative percentages 1% - 2% increase of Cybersecurity index "National culture of cybersecurity"

9.B Increase the supply of skilled professionals to meet market demand	Article 10 and 6 EU priority on skills shortage EC Communication on Cybersecurity Skills Academy	2025	Increase in cybersecurity indicator "cybersecurity graduates in higher education" Number of professionals trained under cybersecurity skills academy	"cybersecurity graduates in higher education" At least 200 000 professionals trained by 2025
9.C Foster EU cybersecurity values and priorities	Article 42 of the CSA	2024	Ability to support the Union external objectives Coherence of ENISA International Engagement with the Agency's strategy	ENISA is seen as key contributor to foster EU cybersecurity values and priorities where engaged ENISA activities are judged aligned with its International Strategy

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
9.1 Develop activities to enhance behavioural change by essential entities[61]	Targeted awareness campaigns to improve behaviour Take up of best practices by stakeholders	Awareness Raising AHWG, NISD WS	Stakeholder satisfaction	Biennial (survey)	91 %	>1% increase (from previous year – decrease in duplication)
			Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics	Annual (report)		>5% increase
			Total social media impressions		27 278 491	
			Total social media engagement		19 301	

[61] Defined by NIS 2

			Total video views		6 602 355	
			Total website visits		300 530	
			Total participation at events		40	
			Number of download of materials and overall utilisation of AR tools (i.e. AR-in-a-Box and SME tool)	Annual (ENISA website)	N/A	>4000 per semester
9.2 Promote cybersecurity topics and good practices[62]	Recognise threats and risks and how to act cyber secure Better informed stakeholder	AR AHWG, ECSM coordinators group	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)
			Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics	Annual (report)		>5% increase
			Total social media impressions		27 278 491	
			Total social media engagement		19 301	
			Total video views		6 602 355	
			Total website visits		300 530	
			Total participation at events		40	
			Number of download of materials and overall	Annual (ENISA website)	N/A	>4000 per semester

[62] Including based on stakeholder strategy

			utilisation of AR tools (i.e. AR-in-a-Box and SME tool)			
9.3 Implement ENISA international strategy and outreach	EU values recognised by international stakeholders International cooperation support ENISA objectives	MT, EEAS, COM and (MB as required)	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)
			Staff satisfaction with international coordination	Annual (survey)	N/A	>80%
			Number of international engagements	Annual (report)	N/A	
9.4 Support the implementation and uptake of EU cybersecurity skills framework	Promoting cybersecurity skills courses Greater number of participants in cybersecurity courses	AHWG on Cybersecurity Skills, ECCC WG on Skills	Stakeholder satisfaction	Biennial (survey)		1% increase (from previous year – decrease in duplication)
			Number of cybersecurity programmes (courses) and participation rates	Annual (cyberhead platform)		1-2% increase
			Total number of students enrolled in the first year of the academic programmes		5 205	
			Student gender distribution (% female: % male)		19% female 81% male	
			Total number of cybersecurity programmes		122	
			Number of postgraduate programmes		5%	
			Number of master's degree programmes		80%	
			Number of bachelor's		15%	

			degree programmes			
			Number of entities included in ECSF registry (i.e. # of MS adopted ECSF, #of ECSF implementations/pledges)	Annual (register of activities)	N/A	30% of MS to adopt ECSF, At least 15 orgisations to have endorsed ECSF
9.5 Implement the Cybersecurity in Education roadmap[63]	Influence education to include cybersecurity Greater awareness and interest in cybersecurity as a career path	AR AHWG	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: ECSM Coordination Group, National Competent Authorities through the NIS Cooperation Group Work Streams, AHWG on Awareness Raising and Education, Enterprise Security AHWG (SMEs), AHWG on Skills, EEAS, DG NEAR, DG CONNECT

Involve / Engage: ENISA National Liaison Officers (NLOs), DG CONNECT, NIS Operators of Essential services / entities in scope of NIS2,, European Cybersecurity Competence Center, International partner

Resource forecast

Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 9.1[64]	NIS	1,75	50.000	0,6	50.000	0	0	2,35	100.000
Output 9.2	INDEX, TREX	1	50.000	0,5	49.315	0	0	1,50	99.315
Output 9.3	SITAW, TREX	1	-	0,75	20.000	0	0	1,75	20.000
Output 9.4*	INDEX, TREX, NIS	1,5	70.000	1	30.000	0	0	2,50	100.000
Output 9.5	INDEX	0,5	60.000	0,5	30.000	0	0	1	90.000
Activity total	FTE: 9.1 - Budget: €409.315.								

Actual resources used in previous year (2022)	FTE: 5.22 Budget: EUR 415 122[65]

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

[65] Carried over into 2023: EUR 125 341

Activity 10 Advise on Research and Innovation Needs and Priorities

OVERVIEW OF ACTIVITY

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

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

ENISA will also conduct regular consultations with relevant user groups, projects (including EU funded projects), researchers, universities, institutes, industry, start-ups and digital innovation hubs to consolidate information and identify gaps, challenges and opportunities in research and innovation from the different quadrants of the community.

This activity contributes to the delivery of ENISA NIS service package.

The ENISA R&I Roadmap (output 10.1) has been supressed from the 2024 work programme due to the change of the periodicity of this report to biennial.

The legal basis for this activity is Article 11 of the CSA.

Link to strategic objectives (ENISA STRATEGY)	Indicators
SO6. Foresight on emerging and future cybersecurity challenges	Overall EU investment in R&I activities addressing emerging cybersecurity challenges

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
10.A EU R&I funding programmes address emerging cybersecurity challenges identified by ENISA.	Art.11, EU Research Agenda	2024	Assessment of ENISA contribution to EU R&I funding programmes work programmes	50%[66]
10.B EU R&I funding programmes focus in the development of solutions made in the EU.	Art.11, EU Research Agenda	2025	Assessment of EU funded projects transitioning from research into deployment of new cybersecurity solutions	10
10.C EU cybersecurity R&I community generates knowledge on emerging cybersecurity challenges identified by ENISA.	Art.11	2024	Number of research articles and papers generated by the community reviewing emerging cybersecurity challenges identified by ENISA	10

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

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
10.1 Collect and analyse information on new and emerging information and communications technologies in order to identify gaps, trends, opportunities and threats (research & innovation observatory).	Identifying current and emerging R&I needs and funding priorities	Academia, Industry and National R&I Entities (including NCCs) and EUIBAs	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Evaluation of the trends, wild cards and week signals on emerging cybersecurity challenges leading to R&I needs and priorities	Annual (annual work programme)	N/A	3
10.2 Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment.	Advising EU Funding programmes including the ECCC	EC including CNECT and JRC, ECCC and NCCs	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Number of contributions to EU funding programmes	Annual (reports)	N/A	5
STAKEHOLDERS AND ENGAGEMENT LEVELS						
Partners: EC-Joint research centre, National and EU R&I Entities, Academia and Industry, European Cybersecurity Competence Centre and National Cybersecurity Centre's.						

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 10.1	NIS	0.6	0	1,15	85.510	0,00	0	1.75	85.510
Output 10.2				1.8	35.490	0,20	5.000	2	40.490
Activity total	FTE:3.75 Budget: 126000								
Forecasted resources in previous year	N/A[67]								

[67] Activity 10 outputs were undertaken under activity 8 in 2022

3.2 CORPORATE ACTIVITIES

Activities 11, 12 and 13 encompass enabling actions that support the operational activities of the agency.

Activity 11: Performance and sustainability

OVERVIEW OF ACTIVITY

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

Under this activity ENISA will seek to achieve key objectives of the Agency's Corporate Strategy (service-centric and sustainable organisation), including by establishing a thorough quality assessment framework, ensuring proper and functioning internal controls and compliance checks, as well as maintaining a high level of cybersecurity across all Agency's corporate and operational activities. In terms of resource management, the budget management committee ensures that the Agency adheres to sound financial management. In the area of IT systems and services, the IT management committee oversees and monitors the comprehensive application of the Agency's IT strategy and relevant policies and procedures.

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

Annual					
ACTIVITY OBJECTIVES	**Link to corporate objectives**	**Activity indicators**	**Frequency(data source)**	**Latest result**	**Target**
11.A Maintain corporate performance and coordinate strategic planning	Ensure efficient corporate services	Proportion of SPD KPIs meeting targets	Annual	13 metrics were unchanged, 21 underperformed and 58 outperformed	>80 of indicators outperformed
	Continuous innovation and service excellence	Results of Internal control framework assessment	Annual	Effective (Level 2)	Effective level 1/2
	Developing service propositions with additional external resourcing	High satisfaction with essential corporate services in the area of compliance and coordination	Annual	N/A	>60%
11.B Increase corporate sustainability	Ensure climate neutral ENISA by 2030	EU Eco-Management and Audit Scheme (EMAS) established	Annual	N/A	Adopted by end 2024
	Develop efficient framework for ENISA continuous governance to safeguard	Agency IT strategy aligned with corporate strategy Proportion of total IT budget allocated to	Annual	N/A N/A	Revised IT strategy by 2024 20% by 2024

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

OUTPUTS	How output expected to contribute to activity objective for the year	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
11.1 Coordinate the implementation of the Agency's performance management framework, including Agency wide budget management and IT management processes, environmental management and regulatory compliance	Unified day to day practices across the agency upon implementing SPD Annual risk assessment and internal controls assessment performed and reported Legal and regulatory compliance are monitored; issues and areas of improvement identified Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy; reports from ITMC Streamlined budget management across the Agency; reports from BMC A plan to reduce CO2 emissions at ENISA's HQ	MT & relevant committees External and internal audits Statutory bodies	Efficiency and effectiveness of project management procedures and tools (survey)	Annual	N/A	>80%
			Number of high risks identified in annual risk assessment		3	<= 3
			Percentage of identified internal controls deficiencies addressed within timelines		N/A	100% for critical, 80% for major, 60% for moderate
			Number of complaints filed against ENISA/number of identified legal or regulatory breaches		3	<=3
			% of revised and up to date corporate rules (MBD, EDD, policies, processes)		N/A	60% corporate rules which have not been reviewed less than 3 years ago; 80% corporate rules which have not been reviewed less than 4 years ago
			MoU with Hellenic authorities for CO2 reduction in ENISA HQ in place		N/A	MoU process initiated by end 2024
			Efficiency and effectiveness of ITMC/BMC processes (survey)		N/A	> 60%
	Compliance with new Regulation on a high	MT and relevant	Percentage of identified high	annual	NA	90%

11.2 Maintain and enhance ENISA's cybersecurity posture	common level of cybersecurity within EUIBAs Timely identification and response to cybersecurity risks Continuous monitoring of IT systems cybersecurity and timely identification of issues and areas of improvement (first level and second level controls)	committees External and internal audits Statutory bodies	risk mitigation measures addressed within timelines			
			Cybersecurity trainings for staff and managers	annual	NA	At least two trainings per year
11.3 Provide support services in the EU Agencies network and in key areas of the Agency's expertise	Cybersecurity advisory in implementation of the new Regulation on a high common level of cybersecurity within EUIBAs and in co-operation with CERT-EU Shared services in the area of data protection, legal services and accounting	MT, BMC EUAN (Agencies receiving ENISA's support)	Satisfaction within the EU Agency network with ENISA support services	annual	NA	>80%
11.4 Ensure the implementation of single administration processes across the Agency	Streamlined document management practices	MT, Staff committee	Percentage of staff considering that the information they need to do their job is easily available/accessible within ENISA	Annual	29%	55%
			Response timeliness to external parties (internal reporting)	Annual	NA	48h

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

Resource forecasts							
Outputs	***Supporting service packages***	CORE		ESSENTIAL		ON-DEMAND	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 11.1	All service packages	4,2	132882	0		0	0
Output 11.2	All service packages	2.	134882	0	20% IT investment –	0	0

					cybersecurity[68]		
Output 11.3		0,6	0	0		0	0
Output 11.4	All service packages	4,2	0	0	203125	0	0
Total	FTEs 11 (of which 0,6 reserve) Budget 470888[69]						
Actual resources used in previous year (2022)	[70]FTE: 16.5 Budget: EUR 829 614[71]						

[68] Budget allocated from across the Agency operational activities for IT cybersecurity (as per corporate strategy KPI 20% of IT spent allocated to cybersecurity). Although internal cybersecurity is centrally co-ordinated by Activity 11, this amount is not included in the budget of activity 11 because it is counted within the budget of the different operational activities.
[69] In addition 54.604 SLA with ECCC, see annex XI for additional information
[70] The current SPD Activity 11 and 12 were undertaken within activity 11 in 2022
[71] Carried over into 2023: EUR 174 087

Activity 12: Reputation and Trust

OVERVIEW OF ACTIVITY

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

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

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

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

Annual

ACTIVITY OBJECTIVES	Link to corporate objectives	Activity indicators	Frequency (data source)	Latest result	Target
12.a Protect and grow the Agency's brand and reputation	Ensure efficient corporate services	Level of trust in ENISA (as per Biannual Stakeholder Survey)	Biennial	95%	95%
12.b Supports the activities implementing the core mandate by improving knowledge sharing	Ensure efficient corporate services	High satisfaction with essential communication and assistants services High satisfaction with demand driven communication and assistants services	Annual (MT survey Annual (MT survey)	N/A N/A	60 % 60%
	Developing service propositions with additional external resourcing	Limited disruption of continuity of internal and external communications	Annual (Business Continuity Plan)	N/A	Target set in business continuity plan and agreed response time objectives (RTO)

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
12.1 Implement the multiannual communications and stakeholders' strategies	Increase transparency and outreach Engaged communities Increased impact of ENISA activities Relevant and easily accessible information	Management Team and agency stakeholders	Number & types of activities at each engagement level (stakeholder strategy implementation)	Annual (Internal report)	N/A	

	is provided to stakeholders		Number of social media engagement	Annual (Media monitoring)	75k	>80k
			Stakeholder satisfaction with ENISA outreach	Biennial (survey)	N/A	>80%
			Number of total ENISA website visits	Annual (website analytics)	2.03 million	>2.5 million
12.2 Implement internal communications strategy	Engaged staff	Management Team and staff committee	Staff satisfaction with the quality and timing of ENISA internal communications	Annual (survey)	36%	>50%
12.3 Manage and provide the secretariat for the statutory bodies	Support the operation and organisation of ENISA statutory bodies Support effectiveness of implementation of work programme (validation of operational outputs) Providing administrative support for the day to day working of the Management board decisions and recommendations from NLO & AG	Statutory bodies, Management Team and Committees	Number of feedback received per NLO consultation	Annual (Internal report)	N/A	>2
			Number of feedback received per AG consultation	Annual (Internal report)	N/A	>2
			Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA	Annual (Survey)	N/A	>80%
			Satisfaction of statutory bodies with ENISA portals	Annual (Survey)	N/A	>80%

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

Involve / Engage: All ENISA stakeholders

Resource forecasts							
Outputs	***Supporting service packages***	CORE		ESSENTIAL		On Demand	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 12.1	All service packages	2,5	430000	0	0	0	0
Output 12.2	All service packages	1	5000	0	0	0	0

Output 12.3	All service packages	2	50000	0	0	0	0
Total	FTE: 5,50 Budget: 485.000						
Actual resources used in previous year (2022)	N/A[72]						

[72] Activity 12 output were undertaken within activity 11 in 2022

Activity 13 Effective and efficient corporate services

OVERVIEW OF ACTIVITY

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

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

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

In parallel, ENISA will continue to **enhance** secure operational **environment** at the highest level, strive excellence in its infrastructure services based on best practices and agile frameworks. It will also explore cloud-enabled services that are fit for purpose and provide services in accordance with recognised european and international standards and ENISA IT strategy. Besides that, ENISA will strive to promote and foster eco-system solutions, explore opportunities for shared services with other EU Agencies, leverage standard technologies where possible, and support flexible ways of working. As ENISA aspires to become a trusted partner it will continue by providing customer focused, multi-disciplinary teams that demonstrate a customer centric, can-do and agile attitude.

ACTIVITY OBJECTIVES	Link to corporate objectives	Activity indicators	Frequency (data source)	Latest result	Target
13.a Enhance people centric services by implementing the Corporate and HR strategy	Effective workforce planning and management	Implementation of SWP/SWR decisions	Annual	Fully implemented	Fully implemented
	Efficient talent acquisition, development and retainment	Implementation of the Corporate and HR strategy	Annual	N/A	Actions implemented according to the timelines
	Caring and inclusive modern organisation	High participation in staff satisfaction survey	Annual	69 %	75 %
13.b Ensure sustainable and efficient corporate solutions and promote continuous improvement	Ensure efficient corporate services	Understand best practices in sustainable IT solutions	Annual	N/A	IT strategy updated accordingly
	Introduce digital solutions that maximise synergies and collaboration in the Agency	Limited disruption of continuity of corporate services	Annual	N/A	BCP for corporate IT, facilities, financial and HR services ensured
	Developing service propositions with additional external resourcing	Handling EUCI at the level of SECRET UE/EU SECRET	By Q2 2024	N/A	Has been accredited
	Promote and enhance ecologic sustainability across all Agency's operations				
	Develop efficient framework for ENISA continuous governance to safeguard high level of IT and physical security				

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results 2022	Target 2024
13.1 Manage and provide horizontal, recurrent, quality support services in the area of resources for ENISA staff and partners	Implement payroll and recurrent administrative services Implement annual recruitment plan Implement annual L&D plan and staff performance Implement annual procurement plan via PPMT Implement insource mission service support Implementation of the ED decision on strategic workforce review [adopted in May 2023] Follow up on FIA centralisation and implementation of results of external analysis on simplification of ENISA financial procedures Analyse procurement services and tenders and propose simplifications Explore further synergies with PMO SLA (e.g. reimbursement of experts)	Management Team IT Management Committee Budget Management Committee Staff Committee	Turnover rates	Annual	4%	3 %
			Establishment plan posts filled		89%	>95%
			Time spent from vacancy announcement to candidate selection		n/a	<300 days
			Percentage of the implementation of approved Recruitment plan		n/a	>90%
			Percentage of the implementation of approved Procurement Plan		n/a	>90%
			Percentage of procurement procedures launched via e-tool (PPMT)		n/a	>90%
			Percentage of budget implementation		100%	>95%
			Average time for initiating a transaction (FIA role)		n/a	<7 days
			Average time for verifying a transaction (FVA role)		n/a	<3 days
			Number of budget transfers		4	<4
			Late payments		n/a	<8%
13.2 Implement Agency's Corporate strategy including HR strategy with emphasis on initiatives in talent development, growth and welfare, innovation and inclusiveness areas	Establish / review corporate costing models and mechanisms to forecast, anticipate and timely manage emerging needs Revision of HR related MB decisions on middle management staff, on SNEs, on the framework for learning and development, on the appraisal of TA staff and CA staff, on reclassification of TA staff and CA	Management Board Management Team Staff Committee EUAN BMC	Number of policies/IR revised or adopted	Annual	n/a	>1
			Number of processes reviewed/redesigned		n/a	>1
			Percentage of staff satisfaction survey with talent development		43%	>50%

	staff indicated in the corporate strategy Set up of key HR policies in the area of learning and development and review staff welfare and mission policies Introduce modern digital solutions in managing talent that give real time input to managers Modernize the selection process by introducing automated IT tool in the process		Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time		n/a	>95%
			Number of implemented competency driven training and development activities		n/a	>1
			Number of multisource feedback evaluations implemented and followed up		n/a	>5
13.3 Manage and provide horizontal, recurrent, quality support services in the area of facilities, security and corporate IT for ENISA staff and partners	Implement annual IT project plan Implement annual FM plan, maintenance and upgrades, including physical security service provision Upgrade infrastructure to improve working conditions and create a conducive work environment to ensure sustained productivity and employee satisfaction Align the lifecycle of IT services and equipment (servers, used equipment) with objectives Ensure timely implementation of requirements to maintain EUCI at relevant level Review ENISA's geographically disperse IT solutions and systems and propose cost benefit solutions that would maximise ENISA's corporate resilience Follow up on the ServiceNow implementation and explore further synergies for integrating further services (HR, FM, EDO, etc) Follow up on AV implementation and upgrade of meeting rooms	Management Team IT Management Committee Budget Management Committee Staff Committee	Satisfaction survey for working environment	Annual	n/a	80 %
			Safety and security incidents reported at workplace in any of the 3 ENISA offices		n/a	<3
			Average time for dealing with facilities management requests		n/a	<3 days
13.4 Enhance operational excellence and digitalisation through modern, safe and secure and streamlined ways of working and introducing self-service functionalities	Explore synergies between FM and Security service provision by integrating services via one service provider, hence reducing FWC numbers and provide all-inclusive services Implementation of an Identity and Access Management Solution to increase the Cybersecurity posture of the organisation Equipment renewal (laptops/mobiles) to ensure business continuity through updated technology, enhanced security measures and improved equipment performance Implement an effective backup solution (SAN) to enhance business continuity by safeguarding critical data, mitigating the risk of data loss and ensuring a swift operation recovery in the event of system failures, disasters or cyber-attacks Implement new A/V and conference equipment to bolster business continuity by facilitating seamless remote collaboration to ensure high-quality communication and	Management Team IT Management Committee	Resilience and quality of ENISA IT systems and services (automated or via surveys) [specific KPIs will be defined for each expected result of the output and will be monitored separately] – as generic indicators – • Critical systems uptime//downtime • Staff satisfaction with resolution	Annual	100 % 84 %	99 % 85 %

	collaboration, which is essential to maintain productivity and operational efficiency Implement of a cloud-based platforms and solutions automate IT delivery services, assure service availability, improve self-service functionalities and provide critical IT-related metrics enabling secure access and sharing of information or device from any location Upgrade physical security measures to ensure high standards for the other ENISA offices to get EUCI accreditation Further development of Athens data centre for high availability purposes to ensure the business continuation and minimisation of downtime risks					

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

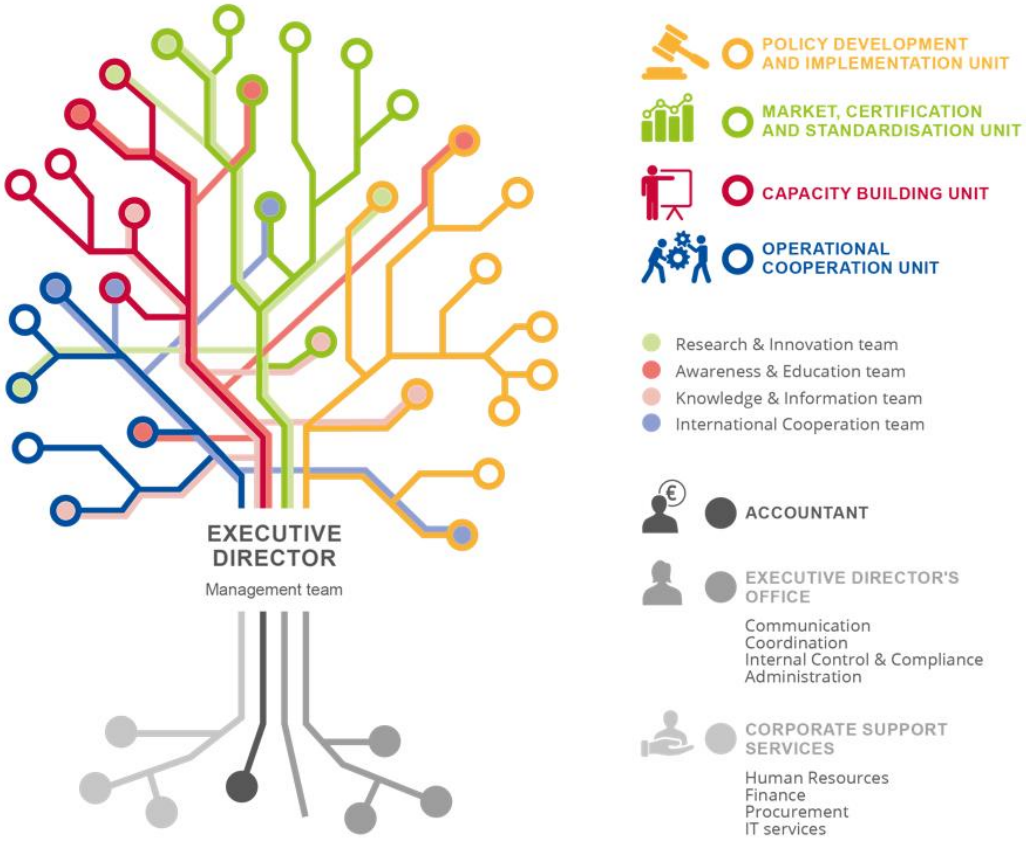
Involve / Engage: Private Sector and International Organisations

Resource forecasts							
Outputs	***Supporting service packages***	CORE		ESSENTIAL		On Demand	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 13.1				8,25	428.250		
Output 13.2				4,75	858.601		
Output 13.3				3,75	2.612.060		
Output 13.4				2,75	362.000		
Total	FTE 19.50 Budget 4.260.911						
Actual resources used in previous year (2022)	FTE: 15 Budget: 1 229 738[73]* *Direct costs only: staff learning and development, staff welfare, books and newspapers, consultancy and travel expenditures linked to Activity 13						

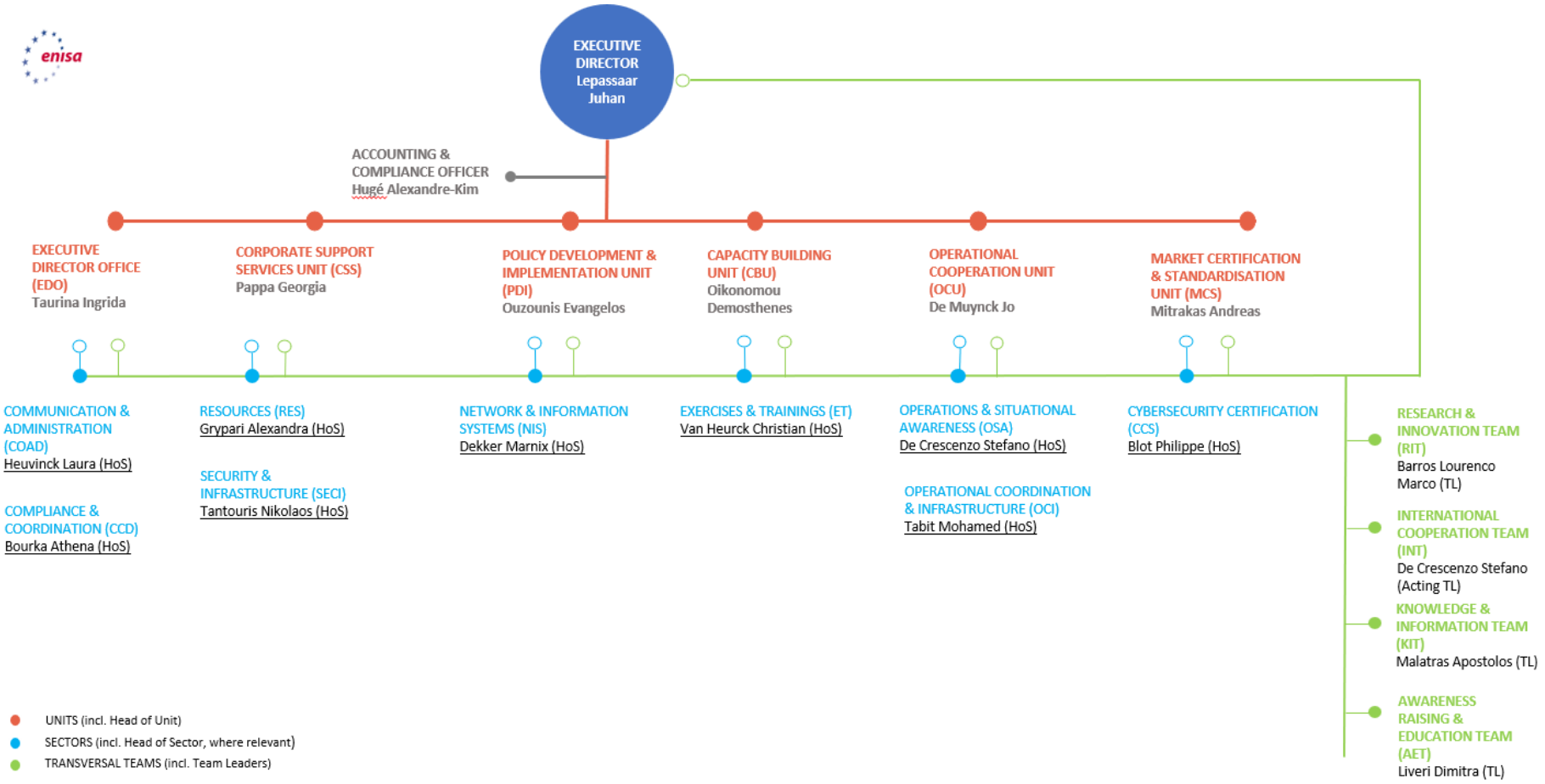
[73] Carried over into 2023: EUR 444 812

ANNEX

I. ORGANISATION CHART AS OF 01.12.2022



Administrative Organigramme



II. RESOURCE ALLOCATION PER ACTIVITY 2024 - 2026

The indicative allocation of the total 2024 financial and human resources following the activities as described in part 3.1 in Section III and the corporate activities as described in part 3.2 in Section III will be presented in the table below. The allocation will be done following direct budget and FTEs indicated for each activity with indirect budget being assigned based on causal relationships.

The following assumptions are used in the simplified ABB methodology:

- Budget allocation of each activity includes Direct and Indirect budget attributed to each activity.
- Direct Budget is the cost estimate of each of the 10 operational activities as indicated under Section 3.1 of the SPD 2024-2026 (carried out under Articles 5-12) in terms of goods and services to be procured.
- Indirect Budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs, attributable to each activity. The indirect budget is allocated to activities based on different drivers. Main driver for costs allocation was number of foreseen direct FTEs for each operational activity in 2024.
- In order to estimate full costs of operational activities, both corporate activities (Activities 11-13) shall be distributed accordingly to all operational activities based on respective drivers

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2024)	Activities as referred to in Section 3	Direct and Indirect budget allocation (in EUR)	FTE allocation
Providing assistance on policy development	Activity 1	1.038.153	4,96
Supporting implementation of Union policy and law	Activity 2	2.670.232	14,21
Building capacity	Activity 3	3.152.259	13,96
Enabling operational cooperation	Activity 4	3.280.613	10,96
Contribute to cooperative response at Union and Member States level through effective situational awareness	Activity 5a	2.165.802	9,46
Contribute to cooperative response at Union and Member States level through ex-ante and ex-post services provision	Activity 5b	509.538	3,71
Development and maintenance of EU cybersecurity certification framework	Activity 6	1.904.535	9,71
Supporting European cybersecurity market and industry	Activity 7	1.256.347	7,21
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	1.804.214	7,96
Outreach and education	Activity 9	1.467.587	7,71
Research and innovation	Activity 10	635.538	3,71
Performance and sustainability	Activity 11	1.874.064	11,21
Reputation and trust	Activity 12	1.046.543	4,96
Effective and efficient corporate services	Activity 13	3.031.048	18,21
TOTAL		**€25.836.475**	**128**[74]

[74] Includes three posts equally distributed across all activities (Executive Director, Accountant and Advisor)

III. FINANCIAL RESOURCES 2024 - 2026

TABLE 1: REVENUE

Revenues	2023	2024
EU contribution	24.475.757	24.953.071
Other revenue (EFTA)	707.738	883.404
Other revenue (SLAs, Annex XI)	p.m.	174.604
TOTAL	**25.183.495**	**26.011.079**

REVENUES	2023 Adopted budget	VAR 2024 / 2023	Draft Estimated budget 2024	Envisaged 2025	Envisaged 2026
1 REVENUE FROM FEES AND CHARGES					
2 EU CONTRIBUTION	24.475.757	1,95%	24.953.071	25.439.933	25.936.532
- of which assigned revenues deriving from previous years' surpluses	*320.868*		*0*	*0*	*0*
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	707.738	24,82%	883.404	735.989	750.539
*- of which EEA/EFTA (excl. Switzerland) ** *	*707.738*	*24,82%*	*883.404*	*735.989*	*750.539*
- of which Candidate Countries					
4 OTHER CONTRIBUTIONS	*	N/A	*	*	*
5 ADMINISTRATIVE OPERATIONS					
- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)					
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT ***	p.m.		174.604	174.604	174.604
7 CORRECTION OF BUDGETARY IMBALANCES					
TOTAL REVENUES	**25.183.495**	**3,29%**	**26.011.079**	**26.350.526**	**26.861.675**

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

** - for the purpose of calculation of EFTA funds for 2025-2026 same surplus as indicated under 2023 is included with 2,93% EFTA proportionality factor

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

Table 2: Expenditure

EXPENDITURE	2023		2024 (*)	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	12.719.412	12.719.412	14.739.106	14.739.106
Title 2	3.519.470	3.519.470	3.666.898	3.666.898
Title 3	8.944.613	8.944.613	7.430.471	7.430.471
Total expenditure	**25.183.495**	**25.183.495**	**25.836.475**	**25.836.475**

EXPENDITURE (in EUR)	Commitment and Payment appropriations					
	Amended budget 2022 (**)	Adopted Budget 2023 Agency	Draft estimated budget 2024 (*)	VAR 2024 / 2023	Envisaged in 2025	Envisaged in 2026
Title 1. Staff Expenditure	**11.917.868**	**12.719.412**	**14.739.106**	**16%**	**14.932.752**	**15.224.351**
11 Staff in active employment	9.862.695	11.019.993	13.058.316	18%	13.229.880	13.488.226
12 Recruitment expenditure	405.780	404.684	517.889	28%	524.693	534.939
13 Socio-medical services and training	1.101.619	923.735	754.501	-18%	764.413	779.341
14 Temporary assistance	547.774	371.000	408.400	10%	413.766	421.845
Title 2. Building, equipment and miscellaneous expenditure	**3.236.767**	**3.519.470**	**3.666.898**	**4%**	**3.715.075**	**3.787.621**
20 Building and associated costs	1.065.153	1.357.750	1.000.719	-26%	1.013.867	1.033.665
21 Movable property and associated costs (***)	64.285	0	0	n.a.	0	0
22 Current corporate expenditure	480.593	472.650	516.125	9%	522.906	533.117
23 Corporate ICT	1.626.737	1.689.070	2.150.054	27%	2.178.302	2.220.839
Title 3. Operational expenditure	**9.052.990**	**8.944.613**	**7.430.471**	**-17%**	**7.528.094**	**7.675.099**
30 Activities related to meetings and missions	551.000	438.600	387.000	-12%	392.085	399.741
37 Core operational activities	8.501.990	8.506.013	7.043.471	-17%	7.136.010	7.275.358
TOTAL EXPENDITURE	**24.207.625**	**25.183.495**	**25.836.475**	**0**	**26.175.921**	**26.687.071**
(*) Does not amounts (total of EUR 174 604) for possible revenue under SLAs with ECCC and EU-LISA, ref. Annex XI						
(**) Does not include the additional EUR 15 000 000 granted for Support Assistance Fund						
(***) As from 2023, "Movable property and associated costs" have been included in Chapter 21 and 22 for streamline purpose						

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

In addition to the EU contribution, ENISA is expected to execute in 2024 an additional amount of EUR 20 174 604 stemming from a contribution agreement under discussion – please refer to Annex XI for the breakdown.

Table 3: Budget outturn and cancellation of appropriations

Budget outturn	2020	2021	2022
Revenue actually received (+)	21.801.460	23.058.211	39.227.392
Payments made (-)	-15.050.421	-17.989.374	-20.396.780
Carry-over of appropriations (-)	-6.200.614	-5.082.548	-18.836.095
Cancellation of appropriations carried over (+)	180.023	209.385	248.745
Adjustment for carry-over of assigned revenue appropriations carried over (+)	10.403	125.622	33.743
Exchange rate difference (+/-)	-1.291	-428	-17,88
Total	**739.560**	**320.868**	**276.988**

Budget 2022 outturn amounts to EUR 276 988.

With more than double budget increase from EUR 24,2 million to EUR 39,2 million during 2022 a commitment rate of 99,93 % (99,51 % in 2021) of appropriations of the year (C1 funds) at year end has been reached which shows the already proven capacity of the Agency to fully implement its annual appropriations.

In 2022 commitment appropriations were cancelled for an amount of EUR 111 911 representing 0,49 % of the total budget.

The payment rate for the full budget of EUR 39,2 million was 52,02 %, while payment rate for usual ENISA operations (without EUR 15 million Assistance Fund which was committed late December 2022) reached 84,11 % (in 2021 – 77,40 %). The total amount including the Assistance Fund carried forward to 2023 is EUR 18 782 626.

No payment appropriations were cancelled during 2022.

The appropriations of 2021 carried over to 2022 were utilised at a rate of 95,07 % (automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 5 048 805 carried forward, the amount of EUR 248 745 was cancelled (or 4,93 %). This cancellation represents 1,09 % of the total budget 2021 of EUR 22 721 149 (fund source C1).

IV. HUMAN RESOURCES - QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2024 - 2026

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

Statutory staff and SNE

STAFF	2022			2023	2024	2025	2026
ESTABLISHMENT PLAN POSTS	Authorised Budget	Actually filled as of 31/12/2022	Occupancy rate %	Adopted	Envisaged staff	Envisaged staff	Envisaged staff
Administrators (AD)	63	55	87%	63	63	63	63
Assistants (AST)	19	18	94%	19	19	19	19
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	82	73	90%	82	82	82	82
EXTERNAL STAFF	FTE corresponding to the authorised budget 2022	Executed FTE as of 31/12/2022	Execution Rate %	Adopted FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)[75]	32	27	84%	32	32	32	32
Seconded National Experts (SNE)	12	10	83%	14	14	14	14
TOTAL External Staff	44	37	84%	46	46	46	46
TOTAL STAFF[76]	126	110	87%	128	128	128	128

[75] 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 2024 and may use this option in the future to offset long-term absences and part-time work with short term contracts of CA.
[76] Refers to TAs, CAs and SNEs figures

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

Human Resources	2021	2022	2023	2024	2025	2026
	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	n/a	n/a	n/a	10	10	10
Seconded National Experts (SNE)	n/a	n/a	n/a	n/a	n/a	n/a
TOTAL	n/a	n/a	n/a	10	10	10

Other Human Resources

- Structural service providers

	Actually in place as of 31/12/2021	Actually in place as of 31/12/2022
Security	5	7
IT	5	7
Facilities management	2	2

- Interim workers

	Actually in place as of 31/12/2021	Actually in place as of 31/12/2022
Number	10	10

Table 2: Multi-annual staff policy plan Years 2022-2026[77]

Function group and grade	2022				2023		2024[78]		2025		2026	
	Authorised budget		Actually filled as of 31/12/2022		Authorised		Envisaged		Envisaged		Envisaged	
	Perm. Posts	Temp. posts	Perm. Posts	Temp posts	Perm. posts	Temp. posts	Perm. Posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts
AD 16												
AD 15		1				1		1		1		1
AD 14				1								
AD 13		2		1		2		2		2		2
AD 12		4		4		4		4		4		4
AD 11		2		2		2		3		4		4
AD 10		4		1		4		4		3		3
AD 9		11		12		11		14		15		15
AD8		22		8		25		15		24		24
AD 7		8		11		10		13		8		8
AD 6		9		15		4		7		2		2
AD 5												
AD TOTAL		63		55		63		63		63		63
AST 11												
AST 10												
AST 9										2		2
AST 8		2		2		2		3		4		4
AST 7		3		1		4		2		4		4
AST 6		8		5		7		7		6		6
AST 5		5		4		5		4		4		4
AST 4		1		4		1		2		0		0
AST 3				1				1				
AST 2				1								
AST 1												
AST TOTAL		19		18		19		19		19		19
AST/SC 6												
AST/SC 5												
AST/SC 4												
AST/SC 3												
AST/SC 2												
AST/SC 1												
AST/SC TOTAL												

[77] The change in the number of establishment plan up to 10% requested for year 2022 is modified as per Art 38 of the ENISA Financial Regulation. In 2022, ENISA will review its staffing strategy and will update a forecast for reclassification also in line with job mapping.
[78] To be updated after the 2024 EU budget has been adopted

Function group and grade	2022				2023		2024[78]		2025		2026	
	Authorised budget		Actually filled as of 31/12/2022		Authorised		Envisaged		Envisaged		Envisaged	
	Perm. Posts	Temp. posts	Perm. Posts	Temp posts	Perm. posts	Temp. posts	Perm. Posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts
TOTAL		82		73		82		82		82		82
GRAND TOTAL	82		73		82		82		82		82	

External personnel

Contract Agents

Contract agents	FTE corresponding to the authorised budget 2022	Executed FTE as of 31/12/2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026
Function Group IV	30	19	30	30	30	30
Function Group III	2	7	2	2	2	2
Function Group II	0	0	0	0	0	0
Function Group I	0	1	0	0	0	0
TOTAL	32	27	32	32	32	32

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2022	Executed FTE as of 31/12/2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026
TOTAL	12	10	14	14	14	14

Table 3: Recruitment forecasts 2024 following retirement / mobility or new requested posts

JOB TITLE IN THE AGENCY	TYPE OF CONTRACT (OFFICIAL, TA OR CA)	TA/OFFICIAL	CA
		Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication *	**Recruitment Function Group (I, II, III and IV)**

	Due to foreseen retirement/ mobility	New post requested due to additional tasks[79]	Internal (brackets)	External (brackets)	
Expert		8 TAs & 2 SNEs	n/a	n/a	n/a
Officer		4 TAs	n/a	n/a	n/a
Assistant		1 TAs	n/a	n/a	n/a

[79] Posts stemming from the resource shortfall identified for 2024 work programme (15 FTEs)

V. HUMAN RESOURCES - QUALITATIVE

A. Recruitment policy

Implementing rules in place:

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

B. Appraisal and reclassification/promotions

Implementing rules in place:

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

Table 1: **Reclassification of TA/promotion of official**

	AVERAGE SENIORITY IN THE GRADE AMONG RECLASSIFIED STAFF							
Grades	**Year 2017**	**Year 2018**	**Year 2019**	**Year 2020**	**Year 2021**	**Year 2022**	**Actual average over 5 years**	**Average over 5 years (According to decision C(2015)9563)**
AD05	-	-	-	-	-	-	-	2.8
AD06	1	2	3	-	1	1	3,8	2.8
AD07	-	-	-	1	-	2	3	2.8
AD08	1	1	1	2	1	3	4,1	3
AD09	-	1	-	-	-	-	10	4
AD10	-	-	-	-	-	2	10,5	4
AD11	-	-	-	-	-	-	-	4
AD12	-	-	-	-	1	-	10	6.7
AD13	-	-	-	-	-	-	-	6.7
AST1	-	-	-	-	-	-	-	3
AST2	-	-	-	-	-	-	-	3
AST3	1	1	1	-	-	1	5,2	3
AST4	1	1	1	1	-	-	4,33	3
AST5	-	1	-	-	1	-	5,5	4
AST6	-	-	-	1	1	-	3,5	4
AST7	-	-	-	-	1	1	4	4
AST8	-	-	-	-	-	-	-	4
AST9	-	-	-	-	-	-	-	N/A
AST10 (Senior assistant)	-	-	-	-	-	-	-	5
	There are no AST/SCs at ENISA: n/a							
AST/SC1								4
AST/SC2								5
AST/SC3								5.9
AST/SC4								6.7
AST/SC5								8.3

Table 2: Reclassification of contract staff

FUNCTION GROUP	GRADE	STAFF IN ACTIVITY AT 31.12.2022	HOW MANY STAFF MEMBERS WERE RECLASSIFIED IN YEAR 2022	AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS	AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS ACCORDING TO DECISION C(2015)9561
CA IV	17	1	-	-	Between 6 and 10 years
	16	4	-	-	Between 5 and 7 years
	15	6	1	4	Between 4 and 6 years
	14	7	1	5,8	Between 3 and 5 years
	13	1	-	-	Between 3 and 5 years
CA III	12	1	-	-	-
	11	1	-	-	Between 6 and 10 years
	10	4	1	3	Between 5 and 7 years
	9	1	1	3	Between 4 and 6 years
	8	0	-	-	Between 3 and 5 years
CA II	6	-	-	-	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
CA I	3	1	-	-	n/a
	2	-	-	-	Between 6 and 10 years
	1	-	-	-	Between 3 and 5 years

C. Gender representation

Table 1: Data on 31.12.2022 statutory staff (only temporary agents and contract agents on 31.12.2022

		OFFICIAL		TEMPORARY		CONTRACT AGENTS		GRAND TOTAL	
		Staff	**%**	**Staff**	**%**	**Staff**	**%**	**Staff**	**%**
Female	Administrator level	-	-	21	29%	11	41%	32	32%
	Assistant level (AST & AST/SC)	-	-	12	16%	4	15%	16	16%
	Total	-	-	33	45%	15	56%	48	48%
Male	Administrator level	-	-	34	47%	8	29%	42	42%
	Assistant level (AST & AST/SC)	-	-	6	8%	4	15%	10	10%
	Total	-	-	40	55%	12	44%	52	52%
Grand Total		-	-	73	**100%**	27	**100%**	100	**100%**

TABLE 2: **DATA REGARDING GENDER EVOLUTION OVER 5 YEARS OF THE MIDDLE AND SENIOR MANAGEMENT (31.12.2022)**	**2018**		**31.12.2022**	
	Number	**%**	**Number**	**%**
Female Managers	2	22%	2[80]	29%
Male Managers	7	78%	5[81]	71%

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

D. Geographical Balance

Table 1: Data on 31.12.2022 - statutory staff only

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

NATIONALITY	AD + CA FG IV		AST/SC- AST + CA FGI/CA FGII/CA FGIII		TOTAL	
	Number	% of total staff members in AD and FG IV categories	Number	% of total staff members in AST SC/AST and FG I, II and III categories	Number	% of total staff
BE	5	7%	1	4%	6	6%
BG	2	3%	0	0%	2	2%
CY	2	3%	2	8%	4	4%
CZ	1	1%	0	0%	1	1%
DE	2	3%	0	0%	2	2%
Double *82	4	5%	3	12%	7	7%
EE	1	1%	0	0%	1	1%
ES	4	5%	0	0%	4	4%
FR	4	5%	1	4%	5	5%
EL	27	36%	14	54%	41	41%
IT	6	8%	0	0%	6	6%
LT	0	0%	1	4%	1	1%
LV	2	3%	0	0%	2	2%
NL	2	3%	0	0%	2	2%
PL	3	4%	1	4%	4	4%
PT	2	3%	1	4%	3	3%
RO	6	8%	1	4%	7	7%
SE	1	1%	0	0%	1	1%
SK	0	0%	1	4%	1	1%
TOTAL	74	100%	26	100%	100	100%

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

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

MOST REPRESENTED NATIONALITY	2017		31.12.2022	
	Number	%	Number	%
Greek	27 (out of 71)	38	41 (out of 100)	41,0

E. Schooling

Agreement in place with the European School of Heraklion	
Contribution agreements signed with the EC on type I European schools	**No**
Contribution agreements signed with the EC on type II European schools	**Yes**

VI. ENVIRONMENT MANAGEMENT

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

In 2021 the Management Board of ENISA established – within the Agency's SPD for 2022-2025 – a goal for the Agency to achieve climate neutrality (defined as zero CO2, CH4 and N2O emissions) across all its operations by 2030. As a first step, in 2022 the Agency undertook an exercise to map its current climate footprint. Based on an audit of past ENISA emissions for which 2019 and 2021 were used as reference years, it was established that ENISA creates 584 485 GHG emissions (tnCO2eq) annually, with indirect emissions from purchased electricity (50.33%) and air travel (36.80%) being the main sources of impact on the climate.

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

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

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

- Acquire an EMAS certificate by Q4 2023.
- 50% of participants in ENISA's organised events and meetings to participate online by 2025, rising to 75% by 2030.
- 50% of ENISA events and meetings to be organised as hybrid or online by 2025, rising to 75% by 2030.
- Initiate and by end 2024 agree a tripartite MoU with the Hellenic Authorities and the landlord of ENISA HQ building to reduce the climate impact of the HQ building at least 40% by 2029,
- Offset all residual emissions generated through ENISA operations by 2030 at the latest.
- Recycle all ENISA residual waste created in its HQ and local offices by 2025.
- Implement ecological sustainability and climate neutrality criteria for procuring event management and support and for facilities management and support services from external contractors by 2025.
- Implement ecological sustainability and climate neutrality criteria for all ENISA tenders for corporate service contractors by 2027 and by 2029 for operational activities.

VII. BUILDING POLICY

Current buildings:

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

Brussels office

The Brussels Office was completed in April 2022 and the office has been operational since then. The office is being used on a daily basis by Brussels based staff, which is a significant benefit for the Operational Cooperation Unit as they are able to communicate easily with the CERT EU Team situated on the same floor. The objective of the second implementation phase, which is currently ongoing, is to obtain accreditation for the secure room, which will enable the agency to handle EU Classified Information (EUCI) in its Brussels premises. The second phase of implementation is likely to continue into Q4 2023. Indicative resources foreseen:

Resources (indicative)	2023	2024	2025	2026
Head count (FTEs)	**12-13**	**12-13**	**12-13**	**13-14**
Budget (one-off & maintenance costs)	**130.000**	**130.000**	**130.000**	**130.000**

VIII. PRIVILEGES AND IMMUNITIES

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

IX. EVALUATIONS

In 2023, the agency conducted stakeholder satisfaction survey to gather feedback on the outcomes/results of ENISA work over the past two reporting periods (2021 and 2022). The survey sought to assess the satisfaction levels of stakeholders in relation to the way the agency implements its projects, specifically how work is organised and managed and how the feedback from external stakeholders is taken into account. The results of the stakeholder satisfaction survey sheds much important light on how stakeholders perceive the added value of ENISA's work. On aggregate the results demonstrate high added value of ENISA's deliverables with 93 % of stakeholders finding significant added value in the outcome / results of ENISA's work. Only 7 % find limited added value and no stakeholder finds no added value. In terms of take up, 85 % of stakeholders also rate the likelihood of taking up the results of ENISA work in support of their tasks in the immediate to medium term, of which the operational cooperation activities 4 and 5 scored the highest in terms of immediate take up (50 %), which, given the nature of these activities, is a good result.

The mandate of the agency requires that the agency carry out its tasks while avoiding the duplication of Member State activities, therefore the result that 83,7 % of stakeholders find that ENISA deliverables do not duplicate or only somewhat duplicate Member State activities is tantamount to ENISA's effort to involve stakeholders in all stages of its work and ensure that the outcomes / results are fit for purpose. However duplication in some areas is unavoidable due to the nature of the work and the need for MS to have their own capacities, as such ENISA will take action to increase efforts to focus its work even more on high added-value / low duplication areas and specifically introduced targets in the work programme to reduce duplication of MS activities.

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

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

As adopted by the Management Board[83], 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.

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

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

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

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

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

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

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

Moreover, since 2021 ENISA has been implementing its anti-fraud strategy[84], which was adopted in line with the recommendations of the European Anti-Fraud Office (OLAF).

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

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

		General information					
		Date of signature	Total amount	Duration	Counterpart	Short description	FTEs
Service level agreements							
1	SLA with ECCC	20/12/22	54.604	1 year	ECCC	The scope of this Service Level Agreement covers support services offered by ENISA to ECCC: data protection officer, accounting officer	0,4 FTEs
2	SLA with eu-LISA M-CBU-23-C35	13/7/23	120.000	31/12/23	eu-LISA	The scope of this Service Level Agreement covers support services offered by ENISA to eu-LISA on the planning, execution and evaluation of upcoming annual exercises	2 FTEs
Contribution agreements							
1	Support Action fund	draft	est. 20 mio	up to 31/12/25	DG CNECT	The purpose of this Agreement is to provide a financial contribution toimplement the action "Incident Response Support and Preparedness for Key Sectors" which is composed of three activities: 1) EU-level cyber reserve with services from trusted private providers for incident response; 2) penetration tests in key sectors and 3) the Party's contribution to the Cyber Analysis and Situation Centre.	est. 13,5 FTEs

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

The international strategy confirms the Agency's mandate in terms of its and focus on the EU and EU actors, while also allowing increased flexibility to engage with international partners in line with the strategic objectives outlined in the ENISA Strategy for a Trusted and Cyber Secure Europe of July 2020 and in support of the EU's international priorities. The Agency's international strategy 85 was adopted by the MB during the November 2021 meeting.

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

Article 42 "Cooperation with third countries and international organisations" states the following

1. To the extent necessary in order to achieve the objectives set out in this Regulation, ENISA may cooperate with the competent authorities of third countries or with international organisations or both. To that end, ENISA may establish working arrangements with the authorities of third countries and international organisations, subject to the prior approval of the Commission. Those working arrangements shall not create legal obligations incumbent on the Union and its Member States.

2. ENISA shall be open to the participation of third countries that have concluded agreements with the Union to that effect. Under the relevant provisions of such agreements, working arrangements shall be established specifying in particular the nature, extent and manner in which those third countries are to participate in ENISA's work, and shall include provisions relating to participation in the initiatives undertaken by ENISA, to financial contributions and to staff. As regards staff matters, those working arrangements shall comply with the Staff Regulations of Officials and Conditions of Employment of Other Servants in any event.

3. The Management Board shall adopt a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent. The Commission shall ensure that ENISA operates within its mandate and the existing institutional framework by concluding appropriate working arrangements with the Executive Director.

XIII. ANNUAL COOPERATION PLAN 2024

The 2024 Annual Cooperation Plan between ENISA, the EU Agency for Cybersecurity, and CERT-EU, the CERT of the EU institutions, bodies and agencies will be annexed to the Single Programming Document 2024-2026 as a separate document.

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

XX-00-00-000-XX-X

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

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

DRAFT Statement of Estimates 2024 (Budget 2024)

European Union Agency for Cybersecurity

CONTENTS

1. GENERAL INTRODUCTION

Explanatory statement

Legal Basis:

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

Reference acts

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

2. JUSTIFICATION OF MAIN HEADINGS

2.1 Revenue in 2024

The 2024 total revenue amounts to € 25836475 and consists of a subsidy of € 24953071 from the General Budget of the European Union and EFTA countries' contributions € 883404
Subsidy from the Greek Government for the rent of the offices of ENISA in Greece is no longer available as rent is directly covered by Greece

2.2 Expenditure in 2024

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

Title 1 - Staff

The estimate of Title 1 costs is based on the Establishment Plan for 2024, which contains 82 Temporary Agent posts.

Total expenditure under Title 1 amounts to	€	12.719.412,14

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to	€	3.519.470,00

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of Work Programme 2024 and amounts to	€	8.944.613,00

3. STATEMENT OF REVENUE 2024

Title	Heading		Voted Appropriations 2022 €	Voted Appropriations 2023 €	DRAFT Appropriations 2024 €	Remarks - budget 2024
1	EUROPEAN COMMUNITIES SUBSIDY		23.633.000	24.475.757	24.953.071	Total subsidy of the European Communities
2	THIRD COUNTRIES CONTRIBUTION		574.625	707.738	883.404	Contributions from Third Countries.
3	OTHER CONTRIBUTIONS		0	0	0	Subsidy from the Government of Greece
4	ADMINISTRATIVE OPERATIONS		0	0	0	Other expected income.
		GRAND TOTAL	**24.207.625**	**25.183.495**	**25.836.475**	

Article Item	Heading		Voted Appropriations 2022 €	Voted Appropriations 2023 €	DRAFT Appropriations 2024 €	Remarks - budget 2024
1	EUROPEAN COMMUNITIES SUBSIDY					
10	EUROPEAN COMMUNITIES SUBSIDY					
100	*European Communities subsidy*		23.633.000	24.475.757	24.953.071	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security.
		CHAPTER 10	23.633.000	24.475.757	24.953.071	
		TITLE 1	**23.633.000**	**24.475.757**	**24.953.071**	
2	THIRD COUNTRIES CONTRIBUTION					
20	THIRD COUNTRIES CONTRIBUTION					
200	*Third Countries contribution*		574.625	707.738	883.404	Contributions from Associated Countries.
		CHAPTER 2 0	574.625	707.738	883.404	
		TITLE 2	**574.625**	**707.738**	**883.404**	
3	OTHER CONTRIBUTIONS					
30	OTHER CONTRIBUTIONS					
300	*Subsidy from the Ministry of Transports of Greece*		0	0	0	Subsidy from the Government of Greece.
		CHAPTER 30	0	0	0	
		TITLE 3	**0**	**0**	**0**	
4	ADMINISTRATIVE OPERATIONS					
40	ADMINISTRATIVE OPERATIONS					
400	*Administrative Operations*		0	0	p.m.	Revenue from administrative operations.
		CHAPTER 40	0	0	0	
		TITLE 4	**0**	**0**	**0**	
		GRAND TOTAL	**24.207.625**	**25.183.495**	**25.836.475**	

4. STATEMENT OF EXPENDITURE 2024

Title	Heading		Voted Appropriations 2022 €	Voted Appropriations 2023 €	DRAFT Appropriations 2024 €	Remarks - budget 2024
1	STAFF		12.494.335	12.719.412	14.739.106	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE		2.824.300	3.519.470	3.666.898	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE		8.888.990	8.944.613	7.430.471	Total funding for operational expenditures.
		GRAND TOTAL	**24.207.625**	**25.183.495**	**25.836.475**	
1	STAFF					
11	STAFF IN ACTIVE EMPLOYMENT					
110	*Staff holding a post provided for in the establishment plan*					
1100	Basic salaries		8.361.489	8.551.219	9.877.711	Staff Regulations applicable to officials of the European Communities and in particular Articles 62 and 66 thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of permanent officials and Temporary Agents (TA).
		Article 1 1 0	8.361.489	8.551.219	9.877.711	

111	***Other staff***					
1110	Contract Agents		1.819.391	1.967.658	2.507.984	Conditions of employment of other servants of the European Communities and in particular Article 3 and Title III thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of Contract Agents (CA).
1113	Seconded National Experts (SNEs)		657.000	501.116	672.621	This appropriation is intended to cover basic salaries and all benefits of SNEs.
		Article 1 1 1	2.476.391	2.468.774	3.180.605	
		CHAPTER 11	**10.837.880**	**11.019.993**	**13.058.316**	
12	**RECRUITMENT/DEPARTURE EXPENDITURE**					
120	***Expenditure related to recruitment***					
1200	Expenditure related to recruitment		10.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201*
1201	Recruitment and Departure expenditure		n/a	404.684	517.889	This appropriation is intended to cover the travel expenses of staff (including members of their families), the installation allowances for staff obliged to change residence after taking up their duty, the removal costs of staff obliged to change residence after taking up duty, the costs of daily subsistance allowances as per Staff Regulations applicable to officials of the European Communities (SR) and in particular Articles 20 and 71 thereof and Articles 5, 6, 7, 9, 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants. This appropriation is intended to cover expenditure related to recruitment, e.g. incurred for interviewing candidates, external selection committee members, screening applications and other related costs.
		Article 1 2 0	10.000	404.684	517.889	
121	***Expenditure on entering/leaving and transfer***					
1210	Expenses on Taking Up Duty and on End of Contract		17.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201*
1211	Installation, Resettlement and Transfer Allowance		204.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201*
1212	Removal Expenses		89.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201*
1213	Daily Subsistence Allowance		92.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1201*
		Article 1 2 1	402.000	0	0	
		CHAPTER 1 2	**412.000**	**404.684**	**517.889**	

13	**SOCIO-MEDICAL SERVICES AND TRAINING**					
131	***Medical Service***					
1310	Medical Service		63.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1332*
		Aticle 1 3 1	63.000	0	0	
132	***Staff Development***					
1320	Staff Development		220.000	232.215	447.501	This appropriation is intended to cover the costs of language and other training needs as well as teambuilding and other staff development activities.
		Article 1 3 2	220.000	232.215	447.501	
133	***Staff Welfare***					
1330	Other welfare expenditure		40.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1332*
1331	Schooling & Education expenditure		530.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 1332*
1332	Staff Welfare		n/a	691.520	307.000	This appropriation is intended to cover staff welfare measures such as the subsidy for the functioning of the School of European Education of Heraklion and other expenditure relevant to schooling & education of children of the Agency staff, health related activities to promote well-being of staff, other activities related to internal events, other welfare measures. This appropriation is also intended to cover the costs of annual medical visits and inspections, occupational doctor services as well as pre-recruitment medical costs and other costs related to medical services.
		Article 1 3 3	570.000	691.520	307.000	
		CHAPTER 1 3	**853.000**	**923.735**	**754.501**	
14	**TEMPORARY ASSISTANCE**					
140	***European Commission Management Costs***					
1400	EC Management Costs		70.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2220*
		Article 1 4 0	70.000	0	0	
142	***Temporary Assistance***					
1420	External Temporary Staffing		321.455	371.000	408.400	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
		Article 1 4 2	321.455	371.000	408.400	
		CHAPTER 1 4	**391.455**	**371.000**	**408.400**	
		Total Title 1	**12.494.335**	**12.719.412**	**14.739.106**	
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**					
20	**BUILDINGS AND ASSOCIATED COSTS**					
200	**Buildings and associated costs**					
2000	Rent of buildings		78.151	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001*
2001	Building costs		n/a	1.357.750	1.000.719	This appropriation is intended to cover various building related costs including the payment of rent for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces, utilities and insurance of the premises of the Agency, cleaning and maintenance of the premises used by the Agency, fitting-out of the premises and repairs in the buildings, costs of building surveillance as well as purchases and maintenance cost of equipment related to security and safety of the building and the staff, expenditure of acquiring technical equipment, as well as maintenance and services related to it, and other costs such as for example market survey costs for rent of buildings, costs of moving to and/or establishing new premises of the Agency and other handling costs.

2003	Water, gas, electricity, heating and insurance		145.317	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001*
2004	Cleaning and maintenance		250.083	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001*
2005	Fixtures and Fittings		40.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001*
2007	Security Services and Equipment		157.590	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001*
2008	Other expenditure on buildings		243.409	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001*
		Article 2 0 0	914.550	1.357.750	1.000.719	
		CHAPTER 2 0	**914.550**	**1.357.750**	**1.000.719**	
21	**MOVABLE PROPERTY AND ASSOCIATED COSTS**					
210	***Technical Equipment and installations***					
2100	Technical Equipment and services		10.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2001*
		Article 2 1 0	10.000	0	0	
211	***Furniture***					
2110	Furniture		125.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230*
		Article 2 1 1	125.000	0	0	
212	***Transport Equipment***					
2121	Maintenance and Repairs of transport equipment		10.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230*
		Article 2 1 2	10.000	0	0	
213	***Library and Press***					
2130	Books, Newspapers and Periodicals		15.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230*
		Article 2 1 3	15.000	0	0	
		CHAPTER 2 1	**160.000**	**0**	**0**	
22	**CURRENT CORPORATE AND ADMINISTRATIVE EXPENDITURE**					
220	***Stationery, postal and telecomunications***					
2200	Stationery and other office supplies		27.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230*
2201	Postage and delivery charges		22.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230*
		Article 2 2 0	49.000	0	0	
221	***Financial charges***					
2210	Bank charges and interest paid		1.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2230*
		Article 2 2 1	1.000	0	0	

222	***Consultancy and other outsourced services***					
2220	Consultancy and other outsourced services (incl. legal services)		270.000	379.650	438.125	This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. in HR area, financial, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy and/or other administrative support services provided by third parties including EC management costs.
		Article 2 2 2	270.000	379.650	438.125	
223	***Corporate and Administrative Expenditures***					
2230	Corporate and Administrative Expenditures		n/a	93.000	78.000	This appropriation is intended to cover corporate and administrative expenditure such as the costs of purchasing, leasing, and repairs of furniture, the costs of maintenance and repairs of transport equipment as well as insurance and fuel, the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions, the costs of office stationery and the purchase of office kitchen consumables, post office and special courrier costs, bank charges, interest paid and other financial and banking costs and other costs of corporate administrative nature.
		Article 2 2 3	0	93.000	78.000	
		CHAPTER 2 2	**320.000**	**472.650**	**516.125**	
23	**ICT**					
231	***Core and Corporate ICT expenditure***					
2310	Corporate ICT recurrent costs		1.065.000	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2312*
2311	Corporate ICT new investments and one-off projects		364.750	n/a	n/a	*As from 2023, whereas the budget structure has been streamlined, this budget line has been moved to budget line 2312*
2312	Core and corporate ICT costs		n/a	1.689.070	2.150.054	This appropriation is intended to cover core and corporate ICT costs including recurrent corporate ICT costs (including support and consulting services) as well as new investments and one-off projects for hardware, software, services and maintenance as well as ENISA website and portals support.
		Article 2 3 1	1.429.750	1.689.070	2.150.054	
		CHAPTER 2 3	**1.429.750**	**1.689.070**	**2.150.054**	
		Total Title 2	**2.824.300**	**3.519.470**	**3.666.898**	
3	**OPERATIONAL EXPENDITURE**					
30	**ACTIVITIES RELATED TO OUTREACH AND MEETINGS**					
300	***Outreach, meetings and representation expenses***					
3001	Outreach, meetings, translations and representation expenses		387.000	438.600	387.000	This appropriation is intended to cover costs of outreach activities (communications, stakeholders' management, publication and translations), meetings (including meetings of ENISA's statutory bodies i.e. MB, AG, NLOs, and meetings with other stakeholders) and other representation costs. It also covers mission costs related to the implementation of Activities 11-13 as defined in the SPD 2024-2026 mainly covering horizontal tasks and other administrative services.
		Article 3 0 0	387.000	438.600	387.000	
		CHAPTER 3 0	**387.000**	**438.600**	**387.000**	

37	**CORE OPERATIONAL ACTIVITIES**				
371	***Activity 1 - Providing assistance on policy development***				
3710	Activity 1 - Providing assistance on policy development	363.000	330.262	357.135	This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT and mission costs).
	Article 3 7 1	363.000	330.262	357.135	
372	***Activity 2 - Supporting implementation of Union policy and law***				
3720	Activity 2 - Supporting implementation of Union policy and law	798.475	773.404	720.268	This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT and mission costs).
	Article 3 7 2	798.475	773.404	720.268	
373	***Activity 3 - Capacity building***				
3730	Activity 3 - Capacity building	1.921.265	1.709.239	1.236.591	This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs).
	Article 3 7 3	1.921.265	1.709.239	1.236.591	
374	***Activity 4 - Enabling operational cooperation***				
3740	Activity 4 - Enabling operational cooperation	1.703.350	2.122.530	1.776.494	This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT and mission costs).
	Article 3 7 4	1.703.350	2.122.530	1.776.494	
375	***Activity 5 - Contribute to cooperative response at Union and Member States level***				
3750	Activity 5 - Contribute to cooperative response at Union and Member States level	824.500	913.512	867.459	This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT and mission costs).
	Article 3 7 5	824.500	913.512	867.459	
376	***Activity 6 - Development and maintenance of EU cybersecurity certification framework***				
3760	Activity 6 - Development and maintenance of EU cybersecurity certification framework	1.025.750	804.578	571.896	This appropriation is intended to cover direct operational costs relevant to the Activity 6 (including operational ICT and mission costs).
	Article 3 7 6	1.025.750	804.578	571.896	
377	***Activity 7 - Supporting European cybersecurity market and industry***				
3770	Activity 7 - Supporting European cybersecurity market and industry	373.800	356.027	266.666	This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT and mission costs).
	Article 3 7 7	373.800	356.027	266.666	
378	***Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities***				
3780	Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities	1.051.950	811.881	711.646	This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT and mission costs).
	Article 3 7 8	1.051.950	811.881	711.646	
379	***Activity 9 - Outreach and education***				
3790	Activity 9 - Outreach and education	439.900	489.209	409.315	This appropriation is intended to cover direct operational costs relevant to the Activity 9 (including operational ICT and mission costs).
	Article 3 7 9	439.900	489.209	409.315	
370	***Activity 10 - Advise on Research and Innovation Needs and priorities***				
3700	Activity 10 - Advise on Research and Innovation Needs and priorities	n/a	195.371	126.000	This appropriation is intended to cover direct operational costs relevant to the Activity 10 (including operational ICT and mission costs).
	Article 3 7 0	n/a	195.371	126.000	
	CHAPTER 3 7	**8.501.990**	**8.506.013**	**7.043.471**	
	TITLE 3	**8.888.990**	**8.944.613**	**7.430.471**	
	GRAND TOTAL	**24.207.625**	**25.183.495**	**25.836.475**	

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

Draft Establishment plan 2024

Category and grade	Establishment plan in voted EU Budget 2023		Establishment plan 2024	
	Off.	TA	Off.	TA
AD 16				
AD 15		1		1
AD 14				
AD 13		2		2
AD 12		4		4
AD 11		2		3
AD 10		4		4
AD 9		11		14
AD 8		25		15
AD 7		10		13
AD 6		4		7
AD 5				
Total AD		**63**		**63**
AST 11				
AST 10				
AST 9				
AST 8		2		3
AST 7		4		2
AST 6		7		7
AST 5		5		4
AST 4		1		2
AST 3				1
AST 2				
AST 1				
Total AST		**19**		**19**
AST/SC1				
AST/SC2				
AST/SC3				
AST/SC4				
AST/SC5				
AST/SC6				
Total AST/SC				
TOTAL		**82**		**82**