European Union Agency for Cybersecurity

DECISION No MB/2023/1
# of the Management Board
# of the European Union Agency for Cybersecurity
(ENISA)
endorsing the draft Programming Document 2024-2026, the draft Statement of estimates 2024 and the draft Establishment plan 2024

THE MANAGEMENT BOARD OF ENISA,

Having regard to the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[1], in particular Article 15.1.(c), Article 24.3., Article 24.4., and Article 29.7;

Having regard to the Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council, in particular Article 32;

Having regard to Commission Communication C(2020) 2297 final of 20 April 2020 on the guidelines for single programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies.

Whereas:

(1) The Management Board should produce, on the basis of the draft drawn by the Executive Director, a statement of estimates of revenue and expenditure for the following year which will be forwarded by the Management Board to the Commission by 31 January 2023;

(2) The Management Board should endorse the draft programming document by 31 January 2023;

(3) The Executive Board has endorsed the draft single programming document 2024-2026 at its meeting held on 19 January 2023.

(4) The Agency should send the draft programming document to the Commission, the European Parliament and the Council no later than 31 January 2023;

[1] *OJ L 151, 7.6.2019, p. 15–69*

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Programming Document 2024-2026 is endorsed as set-out in the Annex 1 of this decision.

Article 2

The Statement of estimates of revenue and expenditure for the financial year 2024 and the Establishment plan 2024 are endorsed as set-out in Annex 2 and Annex 3 of this decision.

Article 3

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

Done by written procedure on 31 January 2023

On behalf of the Management Board,

[signed]

Jean-Baptiste Demaison

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.1

DOCUMENT HISTORY

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

Date	Version	Modification	Author
December 2022	V.01	MB for consultation	ENISA
January 2023	V.1	Updated after MB consultation	ENISA

TABLE OF CONTENTS

LIST OF ACRONYMS

ABAC	Accruals-based accounting
ACER	Agency for the Cooperation of Energy Regulators
AD	Administrator
AST	Assistant
BEREC	Body of European Regulators for Electronic Communications
CA	Contract agenda
CAB	Conformity Assessment Body
Cedefop	European Centre for the Development of Vocational Training
CEF	Connecting Europe Facility
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CERT-EU	Computer Emergency Response Team for EU institutions, bodies and agencies
COVID-19	Coronavirus disease 2019
CSA	Cybersecurity Act
CSIRT	Computer Security Incidence Response Team
CTI	Cyber threat intelligence
CSPO	Cybersecurity Policy Observatory
CyCLONe	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
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
OOTS	The Once Only Technical System
SC	Secretary
SCCG	Stakeholder Cybersecurity Certification Group
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises
SNE	Seconded national expert
SOCs	Security Operation Centres
SOP	Standard Operating Procedure

SPD	Single Programming Document
TA	Temporary agent

INTRODUCTION

FOREWORD

Foreword to be developed during the course of 2023.

MISSION STATEMENT

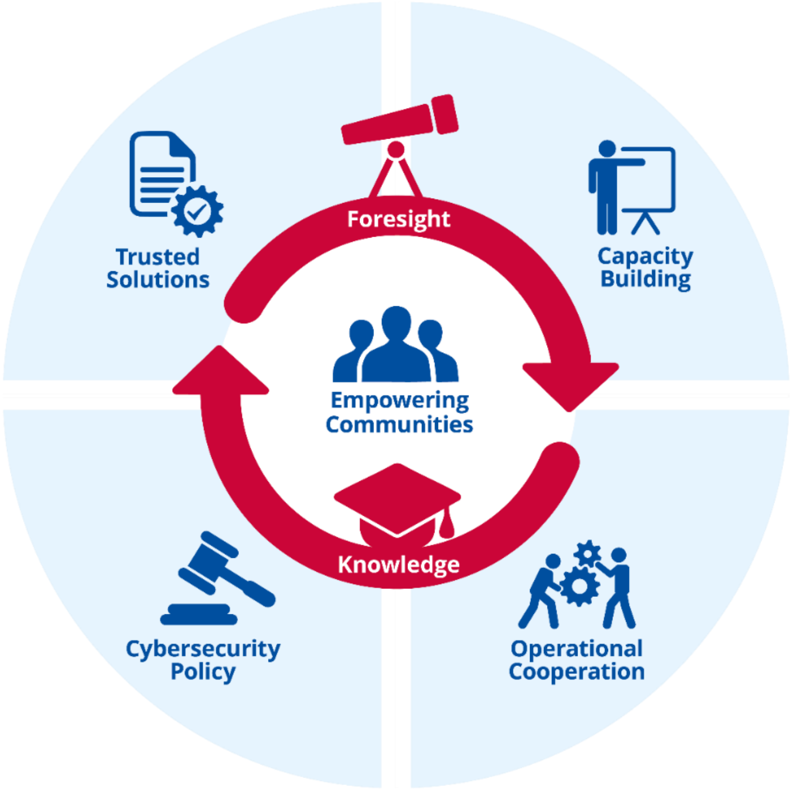
The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical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

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

STRATEGY

EMPOWERING COMMUNITIES

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



CYBERSECURITY POLICY

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

OPERATIONAL COOPERATION

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

CAPACITY BUILDING

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

TRUSTED SOLUTIONS

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

FORESIGHT

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

KNOWLEDGE

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

SECTION I. GENERAL CONTEXT

The present document provides a preliminary multiannual planning and a preliminary draft work programme for 2024, which will be updated accordingly over the course of 2023 until its final adoption by 30 November 2023.

Results from the 2022 threat landscape report highlights a change in trends due to volatile geopolitical situation particularly due to the Russian invasion of Ukraine having acted as a game changer over the reporting period for the global cyber domain. 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.

In terms of the legislative measures designed to strengthen and respond to the threat landscape the European Union (EU) Parliament and the Council approved the NIS 2 directive raising the level of ambition through a wider scope, clearer rules and stronger supervision tools.

ENISA cybersecurity support action

While the implementation of a new "Emergency Response Fund for Cybersecurity" as called by the Council, is under assessment and may require further deliberations, DG CONNECT allocated EUR 15 million to ENISA in 2022 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. The EU needs to respond to these threats and be prepared to respond to cyberattacks.

This short-term support 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 providing ENISA with additional means to support preparedness (ex-ante), and response (ex-post) to large-scale cybersecurity incidents.

Service catalogue

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

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

1. NIS directive (NIS)
2. Training and exercises (TREX)
3. Situational Awareness (SITAW)
4. Certification (CERTI)
5. Cybersecurity index (INDEX)

The multi-annual work programme in section 2 outlines in greater detail the activities that lead and contribute to the service catalogue including the required resources both in terms of budget and human resources.

ENISA's annual Threat Landscape (ETL)[1] for 2022 marks the 10th iteration of this flagship report and was published in October 2022. ETL 2022 looked at threats across EU and the world in the period starting July 2021 and finishing in July 2022. The major highlights include an increase in threats against availability and the persistence of ransomware as one of the prime threats, despite ongoing efforts to tackle it. Threats against availability increased significantly, targeting provisioning of services (telecommunications and energy in particular), and the major motivation behind relevant incidents involved disruption of service. When it comes to ransomware, a dedicated threat landscape was published in July 2022 noting the importance of this threat. Approximately 10 terabytes of data were stolen each month by ransomware threat actors and 58.2% of the data stolen included employees' personal data. While at least 47 distinct threat actors concerning ransomware were identified, for 94.2% of incidents, we do not know whether the company paid the ransom or not. It is estimated however that 62,12% of companies either came to an agreement with the attackers or found another solution. In most cases the affected organisations are unaware of how threat actors managed to get initial access. The latter two findings highlight the issues in incident reporting, whereby just the tip of the iceberg when it comes to ransomware incidents is only reported.

In 2022, a notable increase in the activities of state-sponsored and proxy threat actors was observed, attributed to the volatile geopolitical environment and the war in Ukraine in particular. It is important to highlight the inclusion of vulnerability landscape analysis and impact and motivation per sector that were part of the ETL for the first time in 2022.

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 NIS 2 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 2022

The 3rd ENISA NIS Investments study[2] published in November 2022 offers additional insights into the cybersecurity budgets of Operators of Essential Services (OES) and Digital Service Providers (DSP) and how the NIS Directive has influenced this budget. The annual stock-taking of this data now allows for historical traceability and identification of trends. A typical OES/DSP in the EU earmarks 6.7% of its IT investments for information security, while the average value is 7.2%. When analysing this normalised dataset with historically available data, a decrease of one percentage point is observed in comparison to the median IS vs. IT spending in 2020. However, the historical analysis has to be done while keeping in mind the slight differences in the sample between the years of study and the differences in macro environment, such as the impact of the COVID-19 pandemic in the cost-optimisation practices of OES/DSP. The survey data also indicates that a typical OES/DSP in the EU spends EUR 50 000 on Cyber Threat Intelligence, while the average spending amounts to EUR 399.000. The disparity between the median and average values indicates that most organisations do not earmark vast budgets for CTI, while some (larger) organisations — specifically within the banking and energy sectors — do invest significantly in CTI. Cybersecurity

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

investment strategies of 69% of the OES/DSP in the EU was mostly influenced by the threat landscape, closely followed (66%) by the obligations under the NIS Directive.

A significant change in future iterations of the NIS Investments study was introduced with the substantial expansion of scope introduced by NIS 2 both in terms of the number of sectors, as well as in terms of number of operators. ENISA's work on the topic will adapt to ensure that all new sectors are covered and that the sample of surveyed operators is representative of the new operator size distribution for entities in scope of NIS 2. Changes are expected to be implemented over the next several years as the impact of NIS 2 on the new sectors and entities in scope will likely not be immediate as of 2023.

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. Within this picture, ENISA will determine and adapt its support in particular in the following areas:

NIS 2 Directive

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.

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 - 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[3] 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.

Cyber resilience act (CRA)

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 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 foresees a role for ENISA in the implementation of the Regulation. ENISA's 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.

[3] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_6642/IP_22_6642_EN.pdf

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.

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 and maintaining the candidate schemes. 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 customer trust of digital solutions in the Union. Currently, ENISA has prepared a candidate scheme on EU Common Criteria European candidate cybersecurity certification scheme (EUCC) which is currently being transposed in an EU Implementing Act by the Commission for its final adoption. In 2023 the candidate scheme on Cloud Services (EUCS) will be submitted to the ECCG for its opinion. Furthermore, an ad hoc working group started working to prepare a candidate certification scheme for 5G networks (EU5G), with a first phase to characterise the possibility to reuse existing schemes, and to identify related gaps to be covered by a relevant EU scheme.

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 government services, business and citizens during the time period starting 2024.

In relation to digital identity framework ENISA will support and continue 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 compulsory compliance assessment and voluntary certification within the European cybersecurity certification framework, as established by the Cybersecurity Act. This strategy shall make best reuse of existing relevant cybersecurity certification schemes under development and shall as well identify potential new certification means of schemes that would contribute to the certification of the European Digital Identity wallet.

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 the Regulation provides 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.

Where applicable, certification means CRA related products, such as Protection Profiles or Extension Profiles, of any additional certification tool or scheme. Such certification elements supporting the CRA, as well as other certification elements supporting other legislations should be consolidated into the first public version of the Union Rolling Work Programme which has been pending publication by the Commission. ENISA stands by to support the Commission with the current as well as future editions of the URWP. The adopted schemes will provide the means for the conformity assessment of digital products, services and processes in the Digital Single Market, which would be compliant with the CRA requirements and therefore contribute to increase the level of customer trust of digital solutions in the Union. It further forms the potential basis for other EU regulation relying on cybersecurity making use of synergy effects of using one framework. The above, requires a suitable request of the Commission to ENISA to produce a CRA-related cybersecurity scheme.

Research & Innovation

The EU is expanding its support and investment in of cybersecurity research, technological and industrial development expertise and experience that exists in the EU by prioritizing its efforts to support research and innovation, in particular through a common agenda implemented by the European Cybersecurity Competence Centre (ECCC) and the Network of National Coordination Centres (NCC).

Therefore, a new activity was included in the 2023 work programme dedicated to research and innovation under Article 11 of the CSA. This new activity will consolidate ENISA's processes for identifying cybersecurity research needs and funding priorities and ensure that resources are managed efficiently for delivering stakeholder expectations in this area.

ENISA, with the support from the community, will continue mapping activities in the area of cybersecurity R&I to identify and prioritize areas where more research, development and implementation is needed to improve Europe's knowledge, resilience and response to current and emerging cyber threats. The research and innovation needs and funding priorities identified during the mapping of activities will constitute the basis for ENISA's advice and contribution to the EU's strategic research and innovation agenda.

The European Digital Identity Framework

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.

Artificial Intelligence (AI)

With the EU's AI agenda advancing rapidly following the European Commission proposal on AI[4] and Coordinated Plan on Artificial Intelligence 2021[5], 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

[4] 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

[5] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

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. .

Digital Operational Resilience Act (DORA)

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.

Network Code for cybersecurity aspects of cross-border electricity flows (Network Code on Cybersecurity)

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.

Once-only technical system (OOTS)

Pursuant to Regulation (EU) 2018/1724 [6], the Commission adopted the implementing Regulation C(2022)5628 which sets out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the "once-only" principle. ENISA supports the efforts of the Commission and Member States on cybersecurity aspects of the deployment of the system, including risk management and identification of appropriate technical and organisational measures to mitigate identified threats

Chips Act

[6] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 http://data.europa.eu/eli/reg/2018/1724/oj http://data.europa.eu/eli/reg/2018/1724/oj

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 cybersecurity is an important cross cutting issue for stakeholders.

Cybersecurity and information security for EU institutions, bodies and agencies

In March 2022, the European Commission proposed a new regulation[8] 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[9] 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.

Further developments

Memorandum of Understanding with the European Data Protection Supervisor (EDPS)

ENISA has a long working relationship with the EDPS in the areas of privacy and data protection. Over the years, the two entities have been collaborating on promoting practical recommendations on technical cybersecurity aspects in the implementation of the GDPR and engage relevant communities through the co-location of the Annual Privacy Forum (APF) and the Internet Privacy Engineering Network (IPEN) workshops. In order to strengthen further this collaboration, the two entities signed a Memorandum of Understanding (MOU) on establishing a strategic cooperation in areas of common interest. As part of the strategic plan, EDPS and ENISA will be , developing and delivering capacity building and awareness raising activities to areas such as cybersecurity aspects of personal data protection.

[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

[8] Cybersecurity – uniform rules for EU institutions, bodies and agencies (europa.eu)

[9] 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)

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]. Number of relevant EU 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 & 5	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 availability (disruptions) and utilisation 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	Level of situational awareness and overall level of resilience to tackle massive cyber incidence across the Union
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]
		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

[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

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.

The corporate objective of **sound resource and risk management** is derived from requirements 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”. In addition, the inspiration for this corporate objective stems from the values of **Excellence** and **Transparency** derived from the ENISA strategy and the principle of **Efficiency** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to uphold the highest quality of standards, strive for continuous improvement and enhance the organisation’s performance.

The corporate objective of **building an agile organisation focused on people** is derived from requirements in Art 3(4) of the CSA 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”. In addition, the inspiration for this corporate objective stems from the values of **Responsibility** and **Respect** derived from the ENISA strategy and the principle of **Competences** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to respect fundamental European rights and values in its working environment, assume responsibility for social and environmental dimensions of its procedures and to develop its staff competences, expertise and talent.

CORPORATE OBJECTIVE	ACTIVITY TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	INDICATOR
Sound resource and risk management	Activity 11	Art 4(1)	Maximize quality and value provided to stakeholders and citizens Building lasting credibility and trust	To be determined after the development and adoption of the corporate strategy in 2023

Build an agile organisation focused on people	Activity 12	Art 3(4)	ENISA as an employer of choice and enabling growth and excellence in a secure environment	To be determined after the development and adoption of the corporate strategy in 2023

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 the Agency, rapidly increasing its ability to deliver its mandate 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:

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, 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 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 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 functional capacity in sustaining security (including IT and physical), legal, financial, 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

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.

[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 2023 work programme. During the development of the 2023 work programme the Agency identified a resource shortfall amounting to 734k and 2 FTEs in operations and 2.5m in corporate services. In order to address the resource shortfall each activity manager assessed what could be delivered with the available resources and what couldn't be delivered, and what the impact of the shortfall is on the activity by describing reduced scope, postponed projects and suppressed outputs. This shortfall is documented as an annex to this SPD24-26.

Shared services and partnerships with other institutions and agencies. Structured cooperation with CERT-EU has been formalised with the drafting of an annual cooperation plan to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation. The Agency is imminently expected to finalise agreement to create synergies with the European Cybersecurity Competence Centre and Network 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), a cooperation plan with European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA) 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.

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 lack of proper resourcing.

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

In terms of budgetary resourcing, the Agency was 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 euro. The reduction across activities was outlined in the final draft of SPD 2023 presented to the Management Board, the details of which are annexed in XIV below.

The Agency has 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

[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

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. For example, for ex-ante support services, the Member States requested more than several hundred penetration tests for critical entities, though ENISA could not commit to more than one third of requested pen-tests. Also, the Agency had to mobilise resources beyond the responsible unit, to be able to scale up it's services. Though understandable in the short term, this is not sustainable in the long term.

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, but did not receive any significant additional posts to its Establishment Plan. Thus with the long term outlook of the Union threat landscape remaining gloomy, the Agency cannot, under its current normal budgetary and human resource limits, maintain even this minimum level of support it has been able to muster in 2022, 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 about 4,5 FTEs for ENISA to fulfil the new tasks and suggested they be reallocated from existing resources.. In parallel, 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 - eg human capital - to fulfil these expectations, putting a further strain on the Agency's limited resources.

Acknowledging ENISA's exceptional operational mandate, the Commission and the budgetary authority have continued to support ENISA's annual budget to strengthen operational cooperation domain and through a one-off transfer of up to 15 MEUR in 2022 for supporting the Agency's ability to provide the Member States ex-ante and ex-post services in response to the heightened threat level caused by the Russian war in Ukraine. While ENISA in the short term demonstrated the required agility and flexibility to perform, such new tasks, if they become permanent, ENISA should be entrusted with additional resources.

[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)

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, ENISA would need to prioritise and limit the scope of it services within the existing tasks as well as within new tasks in order to fulfil 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 million euros. As noted above, this level is not sufficient for the Agency to fulfil its mandate, 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 2023 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 5.9 million EUR, and this is without the operational budgetary resources which would be necessary to maintain or expand ENISA 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.

In developing the first budgetary estimates of the first draft 2024 work programme, the Agency has taken into account its imperative needs and priorities (please see under part 2.4. 'efficiency gains') as well as other factors. Namely the inflationary environment, which has had an additional detrimental effect on budgeting, and which is expected to continue into and well beyond 2023. Also, costs for obtaining the goals of climate neutrality of the Agency by 2030 (including by ensuring the energy efficiency of its buildings) as well as staff salaries and staff development costs are expected to increase dramatically over the coming years.

These factors mean, that if current budgetary ceiling is not raised, the Agency's operational budget (Title III) would need to be scaled down significantly [-10% of 2023 level]. Therefore, ENISA has identified the impact of insufficient budgetary resources on the operational activities and has detailed the outputs, which – subject to the review of its Management Board - would be supressed, reduced in-scope and/or postponed, should the budgetary authority be unable to increase the budgetary allocations for the Agency. The identified impact if no new additional resources are forthcoming are detailed under each activity in the draft SPD.

2.3.2 Human Resources

The current establishment plan foresees no change in the number of posts allocated to ENISA (82 posts). The Agency has undertaken a thorough assessment of its internal human resourcing needs for the programming period of 2023-2025, 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 initial assessment must be further

[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) Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

validated and this could lead to some reductions, the current needs assessment points to an overall gap of the equivalent of 44.5 FTEs, out of which additional needs for the equivalent of 21 FTEs are deemed as highly critical or critical to be able to fulfil tasks which are in 2023-2025 designated to be of a high or medium-high priority (please see table below and overall summary of the assessment in the annex).

Table: Evaluation of ENISA's additional FTE needs 2023-2025 in terms of their priority and criticality

PRIORITY[25]	CRITICALITY[26]			TOTAL
	Highly critical	Critical	Not Critical	
High	6	7.5	2	15.5
Medium-high	3.5	4	1	8.5
Medium-low	1.5	5.5	13.5	20.5
TOTAL	11	17	16.5	44.5

The Agency does not have sufficient internal capacity in 2023 to address fully even the highly critical or critical human resource needs, which are necessary to fulfil its tasks and activities. This is despite of the fact that the Agency has taken persistent steps to increase its operational capacity through reallocating posts from administrative and support functions to operational functions (please see above). Thus there is almost no room left to use internal reallocation of posts to increase the Agency's operational human capacity, without seriously undermining its ability to perform. Furthermore, due to already existing shortfall, there are 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 shall develop a cost model under which operational budget lines contribute into outsourcing some technical tasks now performed by operational staff (project administration and support), liberating additional FTE's.

Though the Agency has actively pursued and will continue to pursue number of avenues to build and exploit efficiency gains by developing joint operational and administrative services with other EUIBAs (CERT-EU, ECCC, EU-LISA, CEDEFOP and EUAN), however the efficiencies actually gained from these joint approaches will, and also in the future, cover only a fraction of the assessed shortfalls.

Its Establishment Plan implementation rate is foreseen to reach close to 100% by end of 2023, any unexploited resource means are not nearly sufficient for the Agency to meet its current foreseen workforce needs. The Agency's means will

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.

[25] [**high priority**]: the objective that the resource request is intended to support is clearly referred as a priority in the SPD 2023-2025; [**medium-high priority**]: the objective is acknowledged as important by the Management Board (MB decisions or meeting conclusions), on top of a clear alignment of the resource request with the objectives of the activities in the SPD 2023-2025; [**medium-low priority**]: though the two previous criterions are not met, there exist a clear alignment with objectives of the activities as outlined in the SPD 2023-2025; [**not a priority**]: none of the criterions above are met.

[26] [**highly critical**]: (1) the scope of the tasks and functions of the unit or team is set to be expanded by adopted Union legislation; (2) implementation with only existing resources would critically undermine the attainment of the objective (as measured by defined KPIs); (3) the tasks/functions which the additional resource should support has a clear and legally binding deadline which is not beyond SPD time-frame and (4) the deadline cannot be adjusted by the Management Board; [**critical**]: (1) the scope of the new tasks/functions of the unit/team will expand by MB decision; (2) implementing them with existing resources would undermine the attainment of the objective (as measured by defined KPIs within SPD); (3) the tasks/functions which the additional resource should support has a clear and binding deadline which is not beyond SPD time-frame; [**not critical**]: only 2 or less of the criterions above are met or can be assessed.

become even more inadequate as new legislative proposals get adopted – e.g. the criticality and priority of related workforce needs increases - during in the future programming period of 2024-2026.

Thus, by the end of 2023, ENISA's budgetary and human resource means shall be drawn to their absolute limits. Unless those resource shortfalls are addressed, the Agency will needs to radically limit or scale down its operational activities for the programming period of 2024-2026, which will in turn limit its ability to deliver its mandate, whilst at the same time the already announced legislative and political expectations towards the Agency are ever increasing.

In developing the first draft of the 2024 work programme, the Agency has identified the impact of insufficient workforce on the operational activities and has detailed the outputs, which – subject to the review of its Management Board – shall be suppressed, reduced in scope and/or postponed. The total amount of human resources that the Agency foresees that it requires to fulfil its mandate and by extension the demands of stakeholders in 2024 amount to a total of 145.5 FTEs or additional 17.5 FTEs which is 14% above the current staffing levels (the identified impact if no new additional human resources are forthcoming are detailed under each activity in the SPD).

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. To ensure proper coordination and alignment across tasks of its structural entities on specific cross-cutting topics like: (a) vulnerabilities (CVD policies, European vulnerability database etc), (b) taxonomies and (c) cryptography, ENISA shall set up temporary teams, including relevant experts across different operational units and permanent teams.

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, including 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: MoU with the **European Railway Agency** (ERA) and **European Banking Authority** (EBA) to align ENISA's support for MS under the critical sectors of NIS2 with the activities of the Union bodies in these sectors, utilising the MoU with **EDPS** **,** exchanging of good practices with OECD nations on NISD 2 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**

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 Centre** to utilise synergies in order to serve ENISA mandate and develop further ENISA services under Articles 6 and 7 to align them with the objectives of the forthcoming proposal to respond to the Council call for the **Solidarity mechanism (Emergency Response Fund for cybersecurity.**.

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

Activity 8: utilise the new cooperation arrangements with **CISA**, **NATO** and **Ukraine** to enrich EU cybersecurity knowledge and information.

Activity 9: [developing joint objectives (with relevant programming KPIs) with **ECCC** and **European Institute for Technology (EIT)** to help to tackle skills gap in cybersecurity by supporting the training of 200 000 skilled cybersecurity specialists under European Cybersecurity Skills Framework by 2025]

Activity 10: formalising the structured cooperation with **ECCC** (with whom a Service Level Agreement to share some administrative services was signed end 2022) and setting up cooperation with **Joint Research Centre** (JRC) including in support of the **European vulnerability database** and CVD policies

2.4.2. Strategy to achieve corporate and administrative efficiency gains

ENISAs strategy for achieving efficiency gains shall be formalised within its Corporate Strategy, which shall encompass its human resources strategy, greening and digital strategy and service modelling, and is foreseen to be discussed in the MB in March 2023.

The corporate strategy (including HR strategy) which is expected to present a vision for a modern, flexible and values-driven planning of all its resources in service of an organisation that ensures its staff deliver outstanding results for all stakeholders across the EU. The strategy aims to put ‘people’ and ‘services’ at its heart and steer all of ENISA actions so as to create the right conditions in order to deliver on key priorities while attracting, developing and retaining high calibre talents. While modernising and uplifting our employer branding, ENISA processes, policies and tools will be reviewed with the perspective and vision to give to our staff more flexibility when and how they work, building an even more inclusive workplace, and providing sustainable work environment and solutions. The cornerstone of this transformation, in line with the CSA article 3(4) provisions, is its human capabilities, thus ENISA shall re-adjust its HR processes, including within the Strategic Workforce Planning framework, to be more competency driven.

Pending endorsement of the MB, it shall set the following benchmarks which shall effect the Agency’s budgetary and human resource planning in 2024-2026 by setting:

-the **level and pace of investments** (as % from staff salaries) **into staff development**: should the constraints on the Agency’s Establishment Plan remain as limited as they currently are, and even if they are lifted higher, the only foreseeable way in which the Agency can address its the needs for new skills and competencies which stem for the new tasks and challenges it faces, is to increase rapidly its own talent development. This is also in line with its mandate under Article 3(4) of CSA for the Agency to develop its human resources;

-the **maximum level** (as % from staff salaries) **which the Agency can budget into staff welfare**:

-the **level and pace of investments** (as % from total IT budget) **into the Agency’s own corporate cybersecurity**;

-the **level and pace of investments into achieving carbon neutrality by 2030.**

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. As part of the upcoming corporate strategy, the Agency aims at further improving ENISA’s organisational efficiency and flexibility to meet operational needs. To this end, as part of its HR strategy, the Agency aims to address and include an efficiency strategy component, with specific initiatives and a cross-unit perspective. 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 would aim 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 will be 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 will be 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.

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 upcoming 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 are met.

Digitalisation of services, self-service functionalities and service optimisation will be also at the core of the future way of working and ENISAs 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;

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 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;
- 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, DIGIT and Frontex in the area of HR and financial management;

ENISA has already started its efficiency gains journey and intends in the forthcoming period to connect the separate actions under a corporate plan in order to meet the challenges of the future.

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, peer-review the scope and direction of actions undertaken to implement outputs, as well as 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 as per legal framework in the area of certification.

Since 2021, the framework for structured cooperation with CERT-EU has been formalised with the drafting of an annual cooperation plan to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation (Art 7 of the CSA). The Agency's local office in Brussels established in 2021 will further enable the Agency to further create synergies with other EU Institutions, agencies and bodies within and beyond these activities. The Agency is also pursuing cooperation with relevant Union bodies and will embark to create synergies with the European Cybersecurity Competence Centre and Network to pursue synergies in fulfilling its tasks in the field of research and innovation (Article 11 of the CSA) as well as in administration, namely, accounting, data protection and information security.

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. The Agency is continuing and further expanding the sharing of services among other EU agencies. A number of collaborations and agreements are currently in place European Union Intellectual Property Office (EUIPO) and in 2021 the Agency signed a cooperation plan with European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA). In addition ENISA and European Centre for the Development of Vocational Training (CEDEFOP) are strengthening their cooperation to streamline procurement, share financial services, increase efficiency gains in human resources, explore IT solutions together and to support each other in the area of data protection. The aim is to share knowledge and utilise human resources in the most efficient manner between the two agencies that results in better value for EU citizens.

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 2022 preparatory work to migrate to Advanced Record System (ARES) was initiated and ENISA is engaged in preparatory work to utilise both Missions Integrated Processing System (MIPS) and procurement management processes (PPMT) in the course of 2023.

In 2022 the Agency has embarked on 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. The concept shall be developed in co-operation with CERT-EU and with due consideration of the ongoing legislative process for the new regulation

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 ten operational activities and two 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 the activity objectives to measure the achievements of these 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. The indicators proposed in the SPD will be further elaborated during the course of 2023.

3.1 OPERATIONAL ACTIVITIES

Activity 1 Providing assistance on policy development

OVERVIEW OF ACTIVITY

The activity delivers assistance and advice to the EU and Member States in developing cybersecurity policy and sector-specific policy and law initiatives where matters related to cybersecurity and on the basis of the 2020 EU Cybersecurity Strategy. Aspects such as privacy and personal data protection are also taken into consideration.

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 scouting to support them in identifying potential areas for policy development based on technological, societal and economic trends 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.

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 NIS sectors (Activity 2).

The added value of this activity is to support the decision makers in a timely manner on developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework (see also Activity 8). 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
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. Number 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)	To be determined after assessment of the work programme 2022 implementation

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
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	1	Evidence to assess if current policies are meeting their objectives	DG CONNECT NIS CG NLOs

[27] Policy initiatives such as the forthcoming Cyber Resilience Act and initiatives on Artificial Intelligence (AI), 5G, quantum computing, blockchain, 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]

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	1	Good practices, guidance and recommendations based on evidence	DG CONNECT and other DGs or EUIBAs depending on policy file owner.
1.3 Scout 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	1	Catalogue of EU cybersecurity policies and analysis of gaps, overlaps and inconsistencies	NLOs

Output metrics	**Outputs**	**Type of metric**	**Unit (of measurement)**	**Frequency**	**Data source**	**Results 2022**[29]	**Target 2024**[30]
Stakeholder satisfaction	All outputs	Quantitative	Number	Biennial	Survey		
Number of EU policies supported by ENISA	1.2	Quantitative	Number	Annual	Manual, collected from staff members		
Number of contributions to policy development activities (reports, papers, opinions, participation in workshops etc.)	1.1, 1.2	Quantitative	Number	Annual	Manual, collected from staff members		

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	1,45	215.985	0,00	11.387	0,10	0	1,55	227.372
Output 1.2	NIS, CERTI	1,00	28.086	0,90	27.150	0,10	0	2,00	55.237
Output 1.3	NIS, CERTI	0,95	9.404	0,25	7.523	0,00	0	1,20	16.926
Activity total	FTE: 4.75 Budget: 299.535								

[29] Results to be updated after the annual activity report 2022
[30] Targets to be established based on results of annual activity report 2022

NEGATIVE PRIORITIES - Identified implications if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 1.1	INDEX, SITAW, NIS, CERTI		180,727	Reduced scope of NIS Investments study to cover 15 of the 27 Member states and 8 out of the 18 NIS2 sectors. This will also result in a lack of data for the Index for all indicators supported by this output.
Output 1.2	NIS, CERTI	0,50		Reduced involvement in the CRA and AI Act.
Total		0,50	180,727	

Activity 2 Supporting implementation of Union policy and law

OVERVIEW OF ACTIVITY

The activity provides support to Member States and EU Institutions in the implementation of European cybersecurity policy and legal framework and technical advice on specific cybersecurity aspects of the implementation of the NIS2[31] and other legislations. The activity seeks to avoid fragmentation and supports a coherent implementation of the Digital Single Market across Member States, following a consistent approach between cybersecurity, privacy and data protection.

Under this activity ENISA provides support to the NIS Cooperation Group, its work streams, and the implementation of its biannual Work Program including, for example, the implementation of the 5G toolbox, but also new tasks under the NIS2 like the EU registry for entities that typically provide cross-border of digital infrastructure services or supply chain security.

It further includes horizontal outputs, which address sector-agnostic cross-cutting issues[32], and sectorial outputs, which are sector-specific, and addressed via targeted service packages for the critical (NIS) sectors. In addition, this work contributes with relevant sectorial intelligence to other SPD activities such as exercises and trainings (Activity 3), situational awareness (Activity 5), knowledge and information (Activity 8), and awareness raising (Activity 9).

Furthermore, Activity 2 provides support to MS on cybersecurity aspects of policy implementation in the areas of digital identity (eID) and European Digital Identity Wallets (EUDIW), once-only technical solution (OOTS), technical aspects of privacy and data protection and to the Union's policy initiatives on the security and resilience of the public core of the open internet (e.g. DNS4EU). Overall support is provided to the implementation of the 2020 EU Cybersecurity strategy.

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

Link to strategic objectives (ENISA STRATEGY)	Indicator
SO2. Cybersecurity as an integral part of EU policies	Level of maturity of cybersecurity capabilities and resources across the Union at sector level[33]

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 Register for EU digital entities, NIS CG guidance on CVD policies, supply chain risk assessments	95% of MS have implemented NIS 2 by end of 2024 To be adopted and implemented 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.	To be determined after the first 360 assessment has been concluded
2.C Improve alignment between horizontal, sectorial and transversal EU policies	CSA Article 5	2026	Level of alignment between main NIS2 provisions (incident reporting and security measures)	To be determined after assessment of the work

[31] The NIS2 covers a) critical operators such as telecoms and trust service providers, which were not covered by the NIS1 but by other legislation (EECC and eIDAS), b) sectors which were already covered by the NIS1 such as energy, finance, health and c) new sectors, such as space and public administration.

[32] such cross-cutting issues include namely security measures, technical aspect of cybersecurity, supply chain risk management, and vulnerability disclosure policies.

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

			and sectorial/transversal EU policies	programme 2022 implementation

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
2.1 Support Member States and the EC in the implementation of the NIS CG work program and the NIS directive	NIS CG members will use ENISA advise to implement the NIS Directive.	1, 3	Good practices and recommendations for the implementation of NIS2 Register for EU digital entities, NIS CG guidance on CVD policies, supply chain risk assessments NIS CG work program delivery	DG CNECT, NIS CG
2.2 Support Member States and EC in improving security and resilience of the NIS sectors	Stakeholders use the NIS service package to improve security and resilience of the sectors	2	Delivery of targeted ENISA NIS service packages, according to the maturity of the sector	DG CNECT, NIS CG, sectorial DGs, sectorial EU agencies
2.3 Provide advice on the implementation of cybersecurity provisions in transversal and sectorial EU policies[34].	Stakeholder use ENISA good practices for the implementation of transversal and sectorial EU policies	3	Take up of ENISA good practices and recommendations on the implementation of transversal EU cybersecurity policies.	DG CNECT, NIS CG, sectorial DGs, sectorial EU agencies

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[35]	Target 2024[36]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc) Effectiveness of ENISA guidance to help MS implement their tasks and deliver the NIS CG work program	All outputs	Qualitative		Biennial	Survey		>75 aggregate satisfaction
EU register for digital entities is used by MS	2.1	Quantitative	Number	Biennial	Survey		Used by all MS
CVD guidance is implemented by MS	2.1	Quantitative	Number	Biennial	Survey		Used by all MS
Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)	2.2	Quantitative	Number	Annual	Internal analysis (NIS sector 360)		Increase the level of maturity of sectors compared to 2023
Number and frequency of services delivered to NIS sectors according to the maturity of the sector	2.2	Quantitative	Number	Annual			Number and frequency is consistent with the targets set by the service package.
Number of MS following ENISA guidance for implementing the European Digital Identity wallet	2.3	Quantitative	Number	Annual	Survey		All MS

[34] Including DORA, Electricity Code, privacy and eIDAS
[35] Results to be updated after the annual activity report 2022
[36] Targets to be established based on results of annual activity report 2022

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	SITAW, NIS, TREX	5,7	231846	0	-	0,25	-	5,95	231846
Output 2.2	SITAW, NIS, CERTI, TREX	3,45	312402	0,5	-	0,3	-	4,25	312402
Output 2.3	SITAW, NIS, CERTI		-	2,5	157199	0,3		2,8	157199
Activity total	FTE: 13 Budget: 701.447								

NEGATIVE PRIORITIES - Identified consequences if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
2.1	SITAW, NIS, TREX	0.5 FTE	60000	Postpone NIS2 Digital register going to production after pilot in 2023 (therefore no penetration testing, fixing bugs and finalising.
2.1	SITAW, NIS, TREX		45000	Reduced scope of risk evaluations that will require follow-up recommendations such as 5G toolbox) therefore will not be able to address gaps and to analyse issues in depth.
2.2	SITAW, NIS, CERTI, TREX		60000	Reduced scope of services to NIS packages to the 6 NIS1 priority sectors decided by the MB. One sector: Core internet - will not receive sufficient support – only basic work stream secretariat.
2.2	SITAW, NIS, CERTI, TREX	0.5 FTE	50000	Reduced scope of services to additional NIS2 sectors (public admins, gas). The basic sustain package will have to be reduced, such as support to WG meetings and deep dives or trainings for MS.
2.3	SITAW, NIS, CERTI	0.5 FTE	50000	Reduced scope of services such as new transversal policies (Network code Gas) and many other cyber initiatives up coming
Total		1.5 FTE	271956	

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[37]

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.

Link to strategic objectives (ENISA STRATEGY)	Indicator
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[38]. 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[39]

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
Objective 3.A.1 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 it.
Objective 3.B Prepare and test capabilities to respond to cybersecurity incidents	Art.6 CSA	Annual	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 participants in 2024 increases compared to 2023) 90% participants see positive added value

[37] CSIRT trainings and Capture the Flag (CTF) and Attach Defence (AD) competitions.
[38] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)b
[39] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(1)e

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	Year on year increase in average level of competence of participants Year on year increase in aggregate number of participants across national competitions MS national competence frameworks are aligned with European Cybersecurity Skills framework

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
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	1.1, 1.2, 1.3	Improved national cybersecurity strategies	NLO subgroup on National Cybersecurity Strategies
3.2 Organise large scale biennial exercises and sectorial exercises	Increase the level of preparedness and cooperation Prepare and test capabilities to respond to cybersecurity incidents Increase skill sets Align cybersecurity competencies	1.1, 1.2, 1.3	Stakeholder test and improve capabilities and increase capacity	NLO Network (as necessary) CSIRTs Network (as applicable) CyCLONe members (as applicable) NIS Cooperation Group (as applicable) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as applicable)
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), 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	1.1, 1.2, 1.3	Stakeholders improve capabilities and skill set	NLO Network (as necessary) CSIRTs Network (as applicable) CyCLONe members (as applicable)

	Increase skill sets			NIS Cooperation Group (as necessary) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as necessary)
~~3.4 Develop coordinated and interoperable risk management frameworks~~[40]	~~Increase the level of preparedness~~	~~1.1~~	~~Stakeholders aligned on risk management practices~~	~~Ad-hoc WG on RM~~
3.5 Support the reinforcement of Security Operational Centres (SOCs) as well as their collaboration, assisting the Commission and Member States initiatives in this area in line with the objectives of the EU Cybersecurity Strategy in the building and improving of SOCs	Increase the level of preparedness and cooperation	1.1, 1.2, 1.3	Prepare and test capabilities to detect cybersecurity threats	Ad-hoc WG on SOCs
3.6 Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)	Align cybersecurity competencies Increase skill sets	1.3	Increase skill sets	ECSC Steering Committee (NLO Subgroup)

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[41]	Target 2024[42]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc)	All outputs	Qualitative		Biennial	Survey		
Maturity of national cybersecurity strategies, ISACs, SOCs etc	3.1 & 3.5	Qualitative		Annual	Survey		
Evaluation of capacity building actions by participants in exercises and trainings	3.2	Qualitative		Annual	Survey		
Number of participants in trainings and challenges organized by ENISA	3.2 & 3.5	Quantitative		Annual	Survey		

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, 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***

[40] Suppressed output
[41] Results to be updated after the annual activity report 2022
[42] Targets to be established based on results of annual activity report 2022

		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 3.1	TREX, INDEX	2,00	108.919	0,00	0	0,00	0	2,00	108.919
Output 3.2	TREX, NIS	4,00	584.153	0,00	0	0,00	0	3,75	584.153
Output 3.3	TREX	4,80	635.580	0,00	0	0,00	0	4,80	635.580
~~Output 3.4~~	~~TREX~~	~~0,55~~	~~64.000~~	~~0,00~~	~~0~~	~~0,00~~	~~0~~	~~0,55~~	~~64.000~~
Output 3.5	TREX	0,50	28.544	0,00	0	0,00	0	0,50	28.544
Output 3.6	TREX	3,00	193.043	0,00	0	0,00	0	3,00	193.043
Activity total	FTE: 13,75 - Budget: €1.550.213								

NEGATIVE PRIORITIES - Identified implications if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 3.4	TREX	0,55	64.000	Output suppressed
Output 3.6	TREX	0	159.000	Reduce scope by not preparing a Team Europe and not participating at the International Cyber Security Challenge final
Total		0,55	223.000	

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[43] and the EU Vulnerability Database. . As such, this activity could also frame 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[44].

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
SO3: Effective cooperation amongst operational actors within the Union in case of massive cyber incidents	Level of availability (disruptions) and utilisation of Union level networks, tools and databases

GENERAL ACTIVITY OBJECTIVE	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
4.A. Ensure effective functioning of vulnerability database and relevant vulnerability disclosure mechanisms at the Union level	Article 7 & NIS2	2024	EU vulnerability database usage and added-value	EU vulnerability database fully functional and aligned with national mechanisms
4.B. Tools and platforms which ensure operational cooperation at Union level are in place and used	Article 7	2024	Continuous operations and use of secure communication tools for CyCLONE and CSIRTN	No disruption in the working of operational tools and platforms recorded All beneficiaries use the tools

[43] This is especially relevant for the year 2023 and onwards because the support contract procured by the Commission finishes by the end of 2022.
[44] the Agency will prepare where possible for the future Emergency Response Fund for Cybersecurity, providing that ENISA will be asked to support it and without pre-empting the outcome of the legislative process.

4.C. Improve the added value of ENISA support as well as maturity and capabilities of operational communities (CSIRTs Network, CyCLONe)	Article 7	2024	High satisfaction with ENISA support Maturity of operational communities	80% of satisfaction of stakeholders Average overall level of maturity increases year by year

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
4.1. Support the functioning and operations of the operational networks and communities and cooperation with relevant stakeholders including blueprint actors	TBD	1,2 and 3	TBD	NLO Network (as necessary) Blueprint actors
4.2. Support coordinated vulnerability disclosure efforts by designing and deploying the EU Vulnerability Database.[45]	TBD	1	TBD	CSIRTs Network and CyCLONe
4.3. Deploy , maintain and promote operational cooperation platforms and tools	TBD	2	TBD	Blueprint actors

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[46]	Target 2024[47]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc)	1, 2 & 3	Qualitative		Biennial	Survey		
Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA	3	Quantitative	Number	Annual	Report		
Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	1 & 2	Qualitative		Annual			

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

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

[45] Resources for output 4.2 will be assessed during the course of 2023 for the next iteration of the SPD24-26
[46] Results to be updated after the annual activity report 2022
[47] Targets to be established based on results of annual activity report 2022

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	5,7	144567	3,7	398.138	0,35	0	9,75	542.705
Output 4.2[48]	NIS, SITAW	-							
Output 4.3	SITAW, NIS	3,5	786908	3,25	595.440	0	0	6,75	1.382.348
Activity total	FTE: 16,5 - Budget: 1.925.053								

NEGATIVE PRIORITIES - Identified implications if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 4.1	NIS, SITAW		14757	Cut mission, this will reduce the support for CNW and CyCLONe (mandatory tasks)
Output 4.3	NIS, SITAW		290.000	Postpone development of platforms and tools (ISAC platform)
Total		1,5	304757	

[48] The resource requirements for output 4.2 will be reinstated during the next iteration of the SPD24-26 during the course of 2023

Activity 5 Contribute to cooperative response at Union and Member States level

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. ENISA is delivering this activity by aggregating and analyzing reports to establish a common situational awareness, ensuring information flow between the CSIRTs Network, EU-CyCLONe , the 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 and EC3 and 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)..

In addition, the activity foresees, at the request of Member states, the support for techinical handling of incidents or crises (including analysis and exchange of technical information). 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 supports operational cooperation, including assistance ,situational awareness and a EU crisis management framework (Blueprint / potential JCU). In addition, this activity implements the ENISA Cybersecurity Support Action and services[49].

Moreover the activity implements structured cooperation with CERT-EU (please see Annex XIII Annual Cooperation Plan 2024).

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
SO3: Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents	Level of situational awareness and overall level of resilience to tackle massive cyber incidence across the Union

ACTIVITY OBJECTIVES	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
5.A Enhanced preparedness and effective incident response	Article 7	2024	Level of follow up of the EU cybersecurity technical report findings (JCAR) have been followed up by relevant action plans and taken up by MS and relevant Union actors[50] Take-up and added-value of ENISA support services	All JCAR findings are covered by relevant action plans All MS have taken-up the recommendations in JCAR All MS participate in ENISA support services 80% satisfaction rate of received services
5.B Improved common situational awareness before and during cyber incidents and crisis across the Union	Article 7	2024	Usefulness and timeliness of situational reports Stakeholders ability to make informed decisions based on ENISA situational reports	Quarterly JCAR reports have been issued Action plans have been agreed with communities to address critical JCAR observations

[49] the Agency will prepare where possible for the future Emergency Response Fund for cybersecurity, providing that ENISA will be asked to support it and without pre-empting the outcome of the legislative process.
[50] As part of the report of the state of cybersecurity in the Union in NIS2 Article 18(2)

				Weekly union reports are issued At least 80% of users find the reports useful
5.C Information exchange and cooperation between public and private stakeholders	Article 7	2024	Number of entities signed up for ENISA trusted partners program	More than 10 entities have been signed up

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
5.1 Generate 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[51]	Briefings, reports, summaries of situational awareness	SO3	Take up of recommendations	Blueprint actors
~~5.2 Support technical (including through MeliCERTes) and operational cooperation, incident response coordination and EU wide crisis communication during large-scale cross border incidents or crises~~[52]		~~SO3~~		~~Blueprint actors~~
5.3 Maintain, develop and promote ENISA trusted partnership program for vendors/suppliers for information exchange and situational awareness		SO3	List of trusted vendors / suppliers for stakeholders	Blueprint actors
5.4 Provision of ENISA cybersecurity support services to raise resilience or assist in response of critical threats or massive incidence[53]	ENISA ex ante and ex post services	SO3	Increase of resilience in response to threats and incidents	Blueprint actors

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[54]	Target 2024[55]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc)	All outputs	Qualitative		Biennial	Survey		
Number of relevant incident responses ENISA contributed to as per CSA Art.7	5.1 and 5.2	Quantitative	Number	Annual	Report		
Meeting expectation on (timeliness and frequency of delivering services to stakeholders)	5.1	Quantitative	Number	Annual			

[51] Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1
[52] Output suppressed in 2024
[53] Output resources to be determined during the course of 2023 during the next iteration of the SPD24-26
[54] Results to be updated after the annual activity report 2022
[55] Targets to be established based on results of annual activity report 2022

Number of engagements/request through support program	5.1 & 5.2	Quantitative	Number	Annual			
Number of new and total partners in the ENISA partnership program	5.1 & 5.2	Quantitative	Number	Annual			
Number of RFI answered by members of partnership program	5.1 & 5.2	Quantitative	Number	Annual			
Number of trusted vendors	5.3	Quantitative	Number	Annual			

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: EU Member States (incl. CSIRTs Network members and 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 5.1	SITAW, INDEX	8,6	764.432	0	0	0	0	8,6	764.432
~~Output 5.2~~	~~SITAW~~								
Output 5.3	SITAW	0,45	37.000	0,95	0	0	0	1,4	37.000
Activity total	FTE: 10 - Budget: 828.519								

NEGATIVE PRIORITIES - Identified implications if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 5.1	SITAW, INDEX, NIS		300.000	Reduction in situational awareness of OpenCSAM and OpenCTI and thus reduction in ability to provide effective and credible situational awareness Cease subscription to SHODAN therefore impacting situational awareness, also used in INDEX
Output 5.2	SITAW	1.5	197.701	Output suppressed, unable to support technical (MeliCERTes) and operational cooperation and incident response coordination
Output 5.3	SITAW		64379	Reduced scope of the development and promotion of trusted network of vendors/suppliers for information exchange
Total		1.5 FTE	562.080	

Activity 6 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

This activity emcompasses 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 in providing secretariat of 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. Furthermore, ENISA contributes in relation to cybersecurity certification aspects along the lines of legal instruments such as, CRA, EUDI Wallet, AI, Chips Act etc.

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

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

Link to strategic objectives (ENISA STRATEGY)	Indicator
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 security posture management of certified products, services and processes	Article 8 and Title III	2025	Monitor ENISA take up of technical standards and technical specifications in support of EU legislation (document monitoring)	All relevant standards have been taken up by ENISA
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	High level of readiness by CABs to respond to request on EU schemas (80% via survey) [X] number of requests received by conformity assessment bodies for EU schemas
6.C Increase use and uptake of European cybersecurity certification	Article 8 and Title III	2024	Number of schemes adopted Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework Number of existing certification schemes Number of certified products.	Private entities representing [at least 20%] of the EU market relevant to the schema have taken up certification in [12 months] after the adoption of the implementing act, growing to [40%] after [24 months] and [60%] after [36

			number of stakeholders adopting EU schemes	months] of the adoption.
6.D Increase trust in ICT products, services and processes	Article 8 and Title III	2025	Number of certificates issued and number of labelled products under an EU certification scheme Rate of acceptance of an EU cybersecurity designation e.g. label by all stakeholders including consumers organizations	To be determined after assessment of the work programme 2022 implementation

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
6.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes	Scheme purports to stakeholder requirements	2	Take up of schemes by stakeholders	Ad hoc working groups on certification ECCG European Commission
6.2 Implementing and maintaining of the established schemes including evaluation of adopted schemes, participation in peer reviews etc.	Review of schemes to improve efficiency and effectiveness	1	Take up of schemes by stakeholders	Ad hoc working groups on certification ECCG European Commission
6.3 Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks		2		ECCG European Commission SCCG
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 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	3, 4	Promotion of certificates	ECCG European Commission SCCG

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[56]	Target 2024[57]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc)	6.1	Qualitative		Biennial	Survey		

[56] Results to be updated after the annual activity report 2022
[57] Targets to be established based on results of annual activity report 2022

Number of opinions of stakeholders managed	6.1	Quantitative	Number	Annual	Report		
Number of people/organizations engaged in the preparation of certification schemes	6.1	Quantitative	Number	Annual	Report		
Timeliness and coherence of evaluation of adopted schemes	6.2	Qualitative		Annual	Survey		
Satisfaction of ENISAs role in NCCA peer reviews	6.2	Qualitative		Annual	Survey		
Feedback from statutory bodies on ENISAs role	6.3	Qualitative		Annual	Survey		
Satisfaction of users of the certification website services	6.4	Qualitative		Annual	Survey		
Usage of certification website	6.4	Quantitative	Number	Annual	Report		

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	5,15	503.799	0,7	945	0	0	5,85	504.744
Output 6.2	CERTI	1,1	78.000	0	-	0	0	1,1	78.000
Output 6.3	CERTI	0,8		0		0	0	0,8	-
Output 6.4	CERTI	1,1	75.859	0,15	71.118	0	0	1,25	146.977
Activity total	FTE: 9 Budget: 729.721								

NEGATIVE PRIORITIES - Identified implications if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments

Output 6.1	CERTI, NIS	0,50	162.137	Reduced ability to process concurrently multiple cybersecurity certification scheme requests; reduced scope of feasibility studies
Output 6.2	CERTI	0,25	72.720	Reduced scope of tasks carried out for EUCC and EUCS and longer application periods for monitoring schemes adopted or in the phase of adoption
Output 6.3	CERTI	0,25		Reduced scope of support services to statutory bodies
Total		1	234.857	

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 could also in the future frame parts of ENISA's potential tasks outlined in the Commission's legislative proposal on CRA. 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 internal digital market.

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.

This activity contributes to the CERTI and NIS service packages.

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
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 and take-up of ENISA analysis and recommendations by means of a survey State of the EU cybersecurity industry and market for products and services (index) Industry perception of the internal market (survey)	To be determined after assessment of the work programme 2022 implementation
7.B Improve the conditions for the functioning of the internal market	CSA Article 8 and Title III CRA proposal	2025	Level of incidents affecting products with digital elements [58] (statistics and qualitative analysis) Records (based on the European vulnerability database) of known vulnerabilities and analyses of how	To be determined after first analysis.

[58] Referred as a potential indicator in the Commission's proposal on CRA

			these are/were managed[59]	

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
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	TBD	1 & 2	TBD	Ad hoc working groups cybersecurity market analysis ECCG Advisory Group NLO (as necessary)
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	TBD	2	TBD	SCCG NLO (as necessary)
7.3. Guidelines and good practices on cybersecurity for ICT products, services and processes and recommendations to the EC and the ECCC	TBD	1 & 2	TBD	SCCG NLO (as necessary) ECCG AHWG Market
7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services	TBD	1 & 2	TBD	ECCG NLO (as necessary)

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[60]	Target 2024[61]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc)	7.1, 7.2, 7.3, 7.4	Qualitative		Biennial	Survey		
Analysis on vulnerabilities and dependencies in ICT products and services on the basis of EU	7.1, 7.2, 7.3, 7.4	Quantitative and qualitative		Annual	Report	-	TBD after NIS2 implementation

[59] Referred as a potential indicator in the Commission's proposal on CRA
[60] Results to be updated after the annual activity report 2022
[61] Targets to be established based on results of annual activity report 2022

vulnerability database and incident reports							end 2024

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	3,05	150161	0,1	0	0	0	4,25	124.161
Output 7.2	CERTI, NIS	1,75	150132	0,1	0	0	0	2,3	123.009
Output 7.3	CERTI	0,5	73.017	0	0	0	0	0,5	35.017
Output 7.4	CERTI	0,50	54.716	0,00	0	0,00	0	0,50	40.716
Activity total	FTE: 7,55 - Budget: 322,903								

NEGATIVE PRIORITIES - Identified implications if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED

Output	Service package	FTEs required	Budget required	Comments
7.1	CERTI, INDEX, CERTI	1,1	26.000	Reduced scope of market analysis on main trends
7.2	CERTI, NIS	0,45	27.123	Reduced scope of analysis in the area of standardisation
7.3	CERTI		38.000	Guidelines and good practices on cybersecurity for ICT products, services and processes limited in quantity and scope
7.4	CERTI		14.000	Reduced scope of monitoring and documenting the dependencies and vulnerabilities of ICT products and services
Total		1,55	105.123	

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.

Moreover, under this activity the Agency will map threat landscapes and provides topic-specific as well as general assessments on the expected societal, legal, economic, technological and regulatory impact, with targeted recommendations to Member States and Union institutions, bodies, offices and agencies. In doing so, the Agency will take into account incident reports submitted to it under Article 23 of NIS2 and other relevant EU legislations..

In terms of knowledge management, ENISA will work towards consolidating data, information and knowledge concerning the status of cybersecurity across MS and the EU and continue its effforts in developing and maintaining the EU cybersecurity index and developing the biennial on the state of cybersecurity in the Union. The Agency will also continue its efforts to organise and make available to the public information on cybersecurity by means of a dedicated infohub that will cater for different stakeholders’ needs.

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.

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) ..

Link to strategic objectives (ENISA STRATEGY)	Indicator
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 the mapped emerging technology threats in national risk
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 80% of MS are using the index in some form as benchmarks in their national cybersecurity strategies

8.C Deliver relevant and timely information	Art.9 CSA and European Cybersecurity Atlas	2024	Usage of knowledge management portals, i.e. index tool, CIRAS, infohub, etc. Value and usability of knowledge management portals	80% of targeted stakeholders use the portals regularly 80% of Stakeholders are satisfied with the portals

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
8.1 Develop and maintain EU cybersecurity index	Measuring maturity	1.1 and 1.2	Stakeholders can better prepare for future challenges based on indication of maturity	NISD CG
8.2 Collect and analyse information to report on the cyber threat landscapes	Mapping threats	1.2	Generate recommendations for stakeholders to take up	NLO, AG and Cybersecurity Threat Landscape AhWG CSIRTs Network
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	1.2	Generate recommendations for stakeholders to take up	WS3 of the NISD CG, ECASEC and eIDAS Art.19 groups
8.4 Develop and maintain a portal (information hub), respectively identify appropriate tools for a one stop shop to organise and make available to the public information on cybersecurity, and establishment of procedural framework to support knowledge management activities maximising synergies with the European Cybersecurity Atlas	Maintaining information portal	1.3	Stakeholders have relevant information delivered timely	NLO and AG
8.5 Foresight on emerging and future cybersecurity challenges and recommendations.	Identifying future challenges and opportunities	1.1	Generate recommendations for stakeholders to take up	Foresight AhWG, NLO and AG

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[62]	Target 2024[63]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc)	All outputs	Qualitative		Biennial	Survey		
No of downloads	8.1, 8.2, 8.3, and 8.5	Quantitative	Number	Annual	Website		
Recurring visitors	8.4	Quantitative	Number	Annual	Portal		

[62] Results to be updated after the annual activity report 2022
[63] Targets to be established based on results of annual activity report 2022

Unique visitors	8.4	Quantitative	Number	Annual	Portal		
Average time spent	8.4	Quantitative	Number	Annual	Portal		
Number of recommendations, analyses and challenges identified and analysed (reports)	8.2, 8.3 and 8.5	Quantitative	Number	Annual	ENISA reports		
The influence of foresight on the development of ENISA work programme	8.5	Quantitative	SPD	Biannual	ENISA SPD		
Uptake of reports generated in activity 8	8.2, 8.3, 8.5	Quantitative	Number of references to ENISA work	Annual	Media monitoring report		
Uptake of the cybersecurity index	8.1	Quantitative	Recurring visitors Unique Visitors Average time spent	Biannual	Index platform		

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	2,5	181.982	0	0	0	0	2,5	181.982
Output 8.2	INDEX, SITAW, NIS	2	121.079	0,35	0	0,25	15.000	2,6	136.079
Output 8.3	INDEX, SITAW, NIS	1	58.791	0,2	0	0	0	1,2	58.791
Output 8.4	INDEX, TREX	1	152.235	0	0	0	0	1	152.235
Output 8.5	INDEX	1,1	207.257	0	0	0,1	0	1,2	207.257
Activity total	FTE: 8,50 - Budget: 736.344								

NEGATIVE PRIORITIES - Identified consequences if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 8.2	INDEX, SITAW, NIS	0	35.537	Reduced scope of threat landscape reporting
Output 8.3	INDEX, SITAW, NIS	1	120.000	Postpone advanced incident reporting needs for DORA, CRA, and further developments of CIRAS platform for consolidated reporting and integration/interfacing with OpenCTI (OCU/OSA) and NIS strategy
Output 8.5	INDEX	0	40.000	Postpone Threathunt
Total		1	195.537	

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.

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"	[X% level][64] 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 [X level] 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	2025	Increase in cybersecurity indicator "CYBERSECURITY GRADUATES IN HIGHER EDUCATION"	"CYBERSECURITY GRADUATES IN HIGHER EDUCATION"

[64] To be determined after the results of the pilot index project have been discussed in the MB meeting in March 2023

			Number of professionals trained under ECSF	At least 200 000 professionals trained by 2025
9.C Foster EU cybersecurity values and priorities	Article 42 of the CSA	2024	General level of cybersecurity awareness and hygiene among citizens[65]	Year by year increase

OUTPUS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
9.1 Develop activities to enhance behavioural change by essential entities[66]	Targeted awareness campaigns to improve behaviour	1	Take up of best practices by stakeholders	AR AHWG, NISD WS
9.2 Promote cybersecurity topics and good practices[67]	Recognise threats and risks and how to act cyber secure	1	Better informed stakeholder	AR AHWG
9.3 Implement ENISA international strategy and outreach		3	EU values recognised by international stakeholders	MT and (MB as required)
9.4 Organise European cybersecurity month (ECSM) and related activities	Recognise threats and risks and how to act cyber secure	1	Better informed stakeholders	ECSM coordinators group
9.5 Support the implementation and uptake of EU cybersecurity skills framework	Promoting cybersecurity skills courses	2	Greater number of participants in cybersecurity courses	AHWG on Cybersecurity Skills, ECCC WG on Skills (if created)
9.6 Implement the Cybersecurity in Education roadmap68	Influence education to include cybersecurity	2	Greater awareness and interest in cybersecurity as a career path	AR AHWG

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[69]	Target 2024[70]
Stakeholder satisfaction (Results / outcome taken up, added value, duplication of existing work etc)	All outputs	Qualitative		Biennial	Survey		
Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics	9.1 9.2 and 9.4	Quantitative		Annual	ENISA calendar and registry of activities		
Number of download of materials	9.1, 9.2 & 9.4	Quantitative		Annual	ENISA website		

[65] Article 18(1)c of NIS2
[66] Defined by NIS 2
[67] Including based on stakeholder strategy
[68] Roadmap developed by ENISA during the course of 2022
[69] Results to be updated after the annual activity report 2022
[70] Targets to be established based on results of annual activity report 2022

Number of cybersecurity programmes (courses) and participation rates	9.5	Quantitative		Annual	CyberHEAD		
Number of entities included in ECSF registry	9.5	Quantitative		Annual	CyberHEAD		
Staff satisfaction with international coordination	9.3	Qualitative		Annual	Survey		
Number of international engagements	9.3	Quantitative		Annual	Report		
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 **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 (CISA, NIST etc)							

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[71]	NIS	1	50.000	0,5	30.000	0	0	1,5	80.000
Output 9.2	INDEX, CERTI	0,5	50.000	0,5	30.000	0	0	1	80.000
Output 9.3	SITAW, TREX	0,75	-	0,75	23.544	0	0	1,5	23.544
Output 9.4	TREX	0,1	-	0,9	80.000	0	0	1	80.000
Output 9.5*	INDEX, TREX	1	60.000	0,5	30.000	0	0	1,5	90.000
Output 9.6	INDEX	0,5	60.000	0,5	30.000	0	0	1	90.000
Activity total	FTE: 7,50 - Budget: €443.693								

NEGATIVE PRIORITIES - Identified consequences if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 9.1	NIS	0,5	40.000	Reduced scope of campaign and coverage of less sectors, and cease physical meetings of the awareness raising ad hoc working group

Output 9.2	INDEX, CERTI	0,5	20.000	Physical meetings ceased for the enterprise security ad hoc working group
Output 9.3	SITAW, TREX		2.851	Reduced missions budget and scope
Output 9.4	TREX		20.000	Reduced scope and campaign coverage and cease physical meetings of the ECSM Coordinators Group
Output 9.5	INDEX, TREX		30.000	Reduced scope of MoUs Physical meetings ceased of the ad hoc working group on skills
Output 9.6	INDEX	0,5	30.000	Physical meetings ceased of the ad hoc working group on education
Total		1,5	143.851	

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 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	To be determined after assessment of the work programme 2022 implementation
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.	To be determined after assessment of the work programme 2022 implementation
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	To be determined after assessment of the work programme 2022 implementation

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
10.1 Consolidated cybersecurity research and innovation roadmap across the EU.	Mapping emerging trends	O.10.1	Generate relevant and substantiated advice	Academia, Industry and National R&I Entities (NCCs)
10.2 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	O.10.1	Generate relevant and substantiated advice	Academia, Industry and National R&I Entities (including NCCs) and EUIBAs

10.3 Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment.	Advising EU Funding programmes including the ECCC	O.10.2	Stakeholders have relevant information to decide on funding priorities	EC including CNECT and JRC, ECCC and NCCs

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[72]	Target 2024[73]
Stakeholder satisfaction	All outputs	Qualitative		Biennial	Survey		
Number of contributions to EU funding programmes	10.3	Quantitative	Number	Annual	AWP		
Evaluation of the trends, wild cards and week signals on emerging cybersecurity challenges leading to R&I needs and priorities	10.3	Quantitative	Number	Annual	Reports		

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				1	41.428	0,00	0	1	41.428
Output 10.2	NIS	0.6	0	0.4	105.276	0,00	0	1	105.276
Output 10.3				1.8	35.490	0,20	5.000	2	40.490
Activity total	FTE: 4 Budget: 177.194								

NEGATIVE PRIORITIES - Identified consequences if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 10.2	NIS	1	38177	Reduced scope of research and innovation actions
Total				

[72] Results to be updated after the annual activity report 2022
[73] Targets to be established based on results of annual activity report 2022

1.2 CORPORATE ACTIVITIES

Activities 11 to 12 encompass enabling actions that support the operational activities of the agency.

Activity 11: Performance and risk management

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 an efficient performance and risk management framework, and the development of single administrative practices. It also 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 confinue to enhance key objectives of the renewed organisation, as described in the MB decision No MB/2020/5., including the need to adress the gaps in the Agency's quality assessment framework, enhance proper and functioning internal controls and compliance checks. In terms of resource management the budget management committee ensures 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 Art 32 of the CSA, the latter of which strongly focuses on the sound financial management principle with a view to maximise value to stakeholders.

Link to corporate objective	Indicator
CO1: Sound resource and risk management	To be determined by the development and adoption of the corporate strategy in 2023

ACTIVITY OBJECTIVES[74]	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
11.A Increased effectiveness and efficiency in achieving Agency objectives, including via contribution to efficiency gains within the EU Agencies Network	Art 4(1) and Art 32	2024	Proportion of SPD indicators reaching targets Value of ENISA budget savings (EUR)[75]	To be set after the MB endorsement of new ENISA corporate strategy in March 2023
11.B Compliant with legal and financial frameworks in the performance of the Agency	Art 4(1) and Art 32 Financial regaulations	2024	Assessment of the Internal control framework "Critical" exceptions as registered in the Agency register of exceptions Observations from external audit bodies (e.g. European Court of Auditors ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and Percentage of observations	To be set after the MB endorsement of new ENISA corporate strategy in March 2023

[74] The objectives and KPIs of Activity 11 will be reviewed and set after the MB endorsement of new ENISA corporate strategy in March 2023

[75] To be reviewed after the MB endorsement of new ENISA corporate strategy in March 2023

			successfully completed and closed	
11.C Protect the Agency's assets and reputation, while managing risks	Art 4(1) and Art 32	2025	Level of trust in ENISA	To be set after the MB endorsement of new ENISA corporate strategy in March
11.4 Full climate neutrality of all operations	Art 4(1) and Art 32	2030	% of CO2 reductions at ENISA % of recommendations that include CO2 reductions in operations	To be set after the MB endorsement of new ENISA corporate strategy in March 2023

OUTPUTS	How output expected to contribute to activity objective for the year	Link to activity objective	Expected results of output	Validation
11.1 Maintain performance management framework, implement Agency wide IT and budget management[76] processes including through results of risk assessment with a focus on streamlining procedures / policies including climate neutrality.	Unified day to day practices across the agency upon implementing SPD Alignment between performance and risks Legal and regulatory compliance of the agency; identifying issues and areas of improvement Ensuring environmental efficiency/performance	1,2,3,4	Processes and policies are developed and known within ENISA Results of the yearly risk assessment and internal controls assessment (including security risk assessment) EU Eco-Management and Audit Scheme (EMAS) certificate established and maintained at yearly basis	MT and relevant committees External and internal audits
11.2 Develop and implement annual communications strategy	Increase transparency and outreach Support effectiveness of implementation of work programme (validation of operational outputs)	3	Engaged communities	MT
11.3 Manage and provide secretariat for statutory bodies, as well as single administration practices across the Agency	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 Timely response to enquiries	1, 2 and 3	Hosting and planning meetings, liaising with decision making stakeholders of the Agency Engaged community Management board decisions and recommendations from NLO & AG Streamlined document management across the Agency	Statutory bodies MT, Committees

[76] IT management, intellectual property and budget management committee's

11.4 Provide support services in the EU Agencies network and in key areas of the Agency's expertise	CISO advisory services in implementation of the cybersecurity regulation of EUIBAs and in co-operation with CERT-EU Shared services in the area of data protection and accounting	1	Efficiency gains to Agencies receiving ENISA's services	MT, BMC EUAN (Agencies receiving ENISA's support)

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[77]	Target 2024[78]
Individual staff contribution to agency objectives via indicators	11.1	Quantitative	Percentage	Annual	HR report		
Staff feedback on alignment of objectives with indicators	11.1	Qualitative	Percentage	Annual	Survey		
Staff satisfaction with project management procedures and tools	11.1	Qualitative	Percentage	Annual	Survey		
Number of high risks identified in annual risk assessment	11.1	Quantitative	Number	Annual	Risk assess ment report		
Number of exceptions in the risk register (financial/other)	11.1	Quantitative	Number	Annual	Internal control report		
Number of complaints filed against ENISA, including number of inquiries/complaints submitted to the European Ombudsman	11.1	Quantitative	Number	Annual	Report		
Percentage of complaints addressed timely and according to relevant procedures	11.1	Quantitative	Percentage	Annual	Internal control files		
Percentage of implementation of risk treatment plans	11.1	Quantitative	Percentage	Annual	Report		
Number of critical risks identified in annual risk assessment exercise	11.1	Quantitative	Number	Annual	Report		
Number & types of activities at each engagement level (stakeholder strategy implementation)	11.1	Quantitative	Number	Annual	AAR		
Stakeholder satisfaction with ENISA outreach	11.2	Qualitative	Percentage	Biennial	Survey		
Number of social media / ENISA website engagements	11.2	Quantitative	Number	Annual	Reports		
Staff satisfaction with ENISA internal communications	11.2	Qualitative	Percentage	Annual	Survey		
Number of feedback received per NLO / AG consultation	11.3	Quantitative	Number	Annual	Report		

[77] Results to be updated after the annual activity report 2022
[78] Targets to be established based on results of annual activity report 2022

Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA	11.3	Qualitative	Percentage	Annual	Survey		
Staff satisfaction with single administrative practices at ENISA	11.3	Qualitative	Percentage	Biennial	Survey		
Satisfaction within the EU Agency network with ENISA support services	11.4	Qualitative	Percentage	Annual	Survey		
STAKEHOLDERS AND ENGAGEMENT LEVELS							
Partners: Members of statutory bodies such as Management Board, Advisory Group and National Liaison Officers, EU Agencies Network **Involve / Engage:** All ENISA stakeholders							

Resource forecasts							
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 11.1	All service packages	2		8.5	356.000		
Output 11.2	All service packages	2		2.5	340.000		
Output 11.3	All service packages	1		1	74.010		
Output 11.4				1	0		
Total	FTEs 18 Budget 770.010						

NEGATIVE PRIORITIES - Identified consequences if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
All outputs	All service packages		22.990	Reduced missions across the unit
Output 11.1	All service packages	0.25	31.000	Postpone MS project to enhance implementation of SPD
Output 11.1	All service packages		7.000	Reduce scope of annual risk assessment
Output 11.1			20.000	Reduced legal consultancy services
Output 11.2	All service packages	0.25	300.000	ENISA website migration to DIGIT
Output 11.2	All service packages	0.25	50.000	Reduced communications support to operations
Output 11.3	All service packages	0.25	40.000	Reduced events to statutory bodies
Total		1	470.990	

Activity 12 Staff development and working environment

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.

Link to corporate objective	Indicator
CO2: Build an agile organisation focused on people	To be determined after the development and adoption of the corporate strategy in 2023

ACTIVITY OBJECTIVES[79]	CSA article and other EU policy priorities	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
1.12.A Engaged, committed and motivated staff	Art 3(4) Staff regulations	2024	Staff satisfaction / morale (staff survey) Staff turnover rate Rate of absence	To be set after the MB endorsement of new ENISA corporate strategy in March 2023
12.B Enhanced competencies, skills and knowledge of staff	Art 4 (1) and Art 3(4)	2024	Staff satisfaction with training & development (staff survey) Number of training and development undertaken according to strategic workforce planning Number of competency driven initiatives implemented Average training hours per staff member	To be set after the MB endorsement of new ENISA corporate strategy in March 2023

[79] The objectives and KPIs of Activity 12 will be reviewed and set after the MB endorsement of new ENISA corporate strategy in March 2023

12.C Matching Agency needs with available resources, and obtaining internal and external efficiency gains	Art 3(4)	2024	Staff satisfaction with resource planning by managers (staff survey) Average value of efficiency gains	To be set after the MB endorsement of new ENISA corporate strategy in March 2023
12.D Enhanced and digitally enabled, safe and secure working environment		2024	Staff satisfaction with working environment (staff survey) Number of safety and security incidents reported at workplace in any of the 3 ENISA offices	To be set after the MB endorsement of new ENISA corporate strategy in March 2023

Outputs	**How output expected to contribute to activity objective for the year**	**Link to activity objectiv e**	**Expected results of output**	**Validation**
12.1 Manage and provide horizontal, recurrent, quality support services in the area of resources and infrastructure[80] for ENISA staff, partners and visitors	Ensure business continuity in horizontal services in HR, Budget and Finance, Procurement, IT, Facility and Security for a modern, collaborative and welcoming place to work	1,2,3,4	- Services offered are qualitative and timely - Provide a secure, safe, modern and welcoming place to work (and telework) - Maturity level is increasing year to year and staff awareness of products and services is raised; - Set up service provision standards and establish SLAs that are fit for purpose and in accordance with recognised standards; - Ensure compliance with and raise awareness of the regulatory framework (SR, FR,GIP) etc - Ensure and execute physical security corporately and enable operations at highest level of security; - Maximise business impact through customer centric, can do and agile attitude teams;	• Management Team • IT Management Committee • Budget Management Committee • Staff Committee
12.2 Develop and implement Agency's corporate strategy (including HR strategy) with emphasis on talent development, growth and welfare, innovation and inclusiveness, digitalisation and sustainability while aiming for organisational efficiency.	ENISA corporate strategy sets main strategic direction for provision of horizontal services and enhancement of organisational efficiency and service provision standards	1,2	- ENISA corporate strategy prepared and implemented - Implement Strategic Workforce Planning to ensure optimal allocation to activities; - Implement new competency management framework and revised role descriptions; - Further explore shared services with other EU agencies and EUIBAs - Increased staff engagement and staff welfare; - Optimise budget planning, forecasting and execution; - Improve agency's ABB/ABC/ABM methodology and processes; - Modernisation mindset and a culture of continuous improvement and development;	• Management Board • Management Team • Staff Committee • EUAN • BMC • ITMC
12.3 Enhance operational excellence and digitalisation through modern, safe and secure and streamlined ways of working	Increased efficiency in administrative services, due to	1,2	- Tools and technologies used are modern, collaborative and provide advanced analytic capabilities;	• Management Team • IT Management Committee

[80] Including full accreditation of the Agency to handle and manage EUCI by end of 2023 confirmed by DG Human Resources and Security

and introducing self-service functionalities.	new/improved ICT solutions and/or reengineered business processes that modernise the work environment		- Transform legacy to secure and cost-efficient cloud infrastructure in line with the IT strategy and risk based approaches; - Introduce and support roll out of a wide range of digital systems and applications (cloud based/DIGIT); - Review and redesigning key business processes, standardise processes across locations and raise awareness; - Implementation of Zero Trust Architecture programs; - Raise awareness	

Output metrics	Outputs	Type of metric	Unit (of measurement)	Frequency	Data source	Results 2022[81]	Target 2024[82]
Percentage of staff satisfaction survey	1,2,3	Qualitative	%	Annual	Staff satisfaction survey		
Percentage of actions planned to follow up on staff satisfaction survey results and implemented on time	1,2,3	Qualitative	%	Annual	Staff satisfaction survey		
Turnover rates	1, 2	Quantitative	%	Annual	CSS files		
Establishment plan posts filled	1	Quantitative	%	Annual	CSS files		
Time spent from vacancy announcement to candidate selection	1,2,3,	Qualitative	Number	Annual	CSS files		
Percentage of the implementation of approved Recruitment plan	1,2,3	Qualitative	Number	Annual	CSS files		
Number of competency driven initiatives implemented	1,2,3	Qualitative	Number	Annual	CSS files		
Number implemented competency driven training and development activities	1,2,3	Qualitative	Number	Annual	CSS files		
Number of multisource feedback evaluations implemented and followed up	1,2	Qualitative	Number	Annual	CSS files		
Number of policies/IR revised or adopted	1, 2, 3	Qualitative	%	Annual	CSS files and document registry		
Number of processes reviewed/redesigned	1,2,3	Qualitative	Number	Annual	CSS files		
Percentage of customer service	1,2,3	Qualitative	%	Annual	Staff satisfaction survey		
Number of projects initiated based on a business case or cost-benefit analysis	1,2,3	Quantitative		Annual	CSS files		
Resilience and quality of ENISA IT systems and services	3	Quantitative	%	Annual	CSS files Staff satisfaction survey		
Safety and security incidents reported at workplace in any of the 3 ENISA offices	1,2,3	Qualitative	Number	Annual	CSS files		

[81] Results to be updated after the annual activity report 2022
[82] Targets to be established based on results of annual activity report 2022

Workplace flex ratio	1,2,3	Quantitative	%	Annual	CSS files		
Occupant Satisfaction Rates	1,2,3	Quantitative	%	Annual	CSS files		
HVAC and energy costs	1,2,3	Quantitative	%	Annual	CSS files		
Percentage of the implementation of approved Procurement Plan	1,2,3	Quantitative	%	Annual	CSS files		
Percentage of procurement procedures launched via e-tool (PPMT)	1,2,3	Quantitative	%	Annual	CSS files		
Percentage of budget implementation	1,2,3	Quantitative	%	Annual	CSS files		
Average time for initiating a transaction (FIA role)	1	Quantitative	Number	Annual	ABAC		
Average time for verifying a transaction (FVA role)	1	Quantitative	Number	Annual	ABAC		
Number of local line transfers	1	Quantitative	Number	Annual	ABAC		
Percentage of payments made within 30 days	1	Quantitative	%	Annual	ABAC		
Late payments	1	Quantitative	%	Annual	ABAC		

STAKEHOLDERS AND ENGAGEMENT LEVELS

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

Involve / Engage: Private Sector and International Organisations

Resource forecasts

Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)	
		FTE	EUR	FTE	EUR	FTE	EUR
Output 12.1				11	2.488.473		
Output 12.2				3	433.000		
Output 12.3				3	1.826.000		
Total	FTE 17 Budget 4.747.473[83]						

NEGATIVE PRIORITIES - Identified consequences if no new resources are allocated to the Agency (OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED

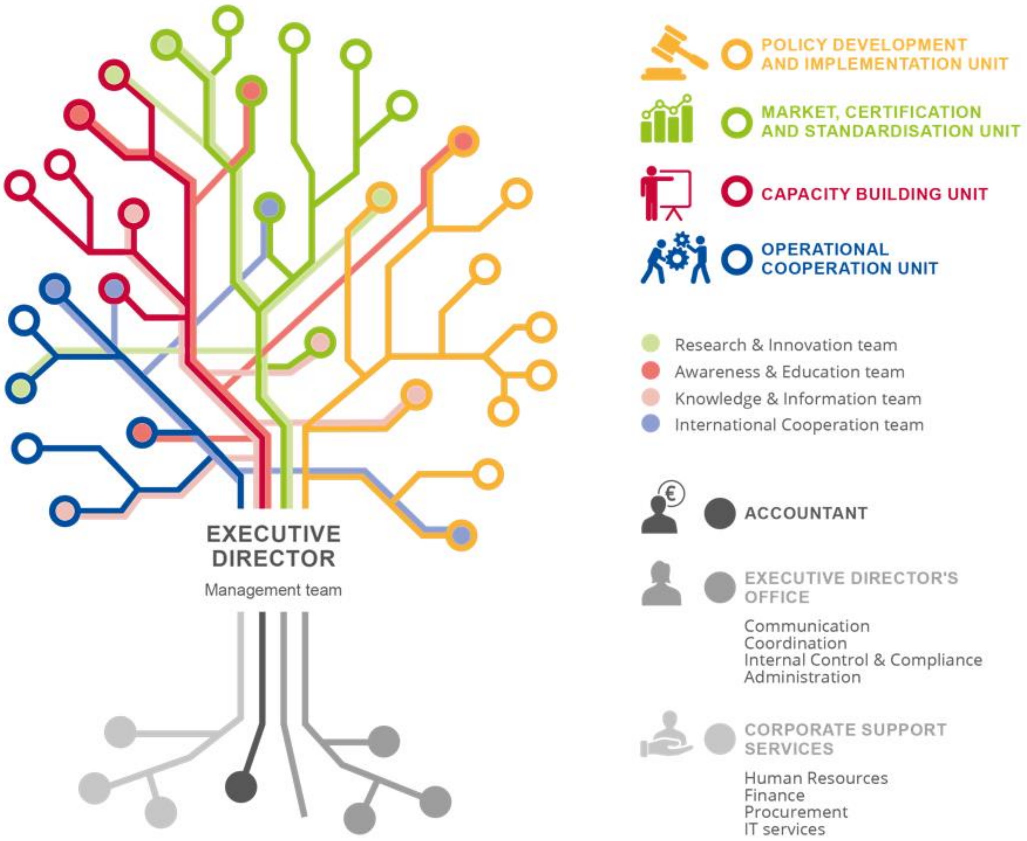
Output	Service package	FTEs required	Budget required	Comments

[83] Indicated budget excludes staff (TA, CA, SNE) salaries and allowances + 5.5% inflationary increase in fixed recurring costs in facilities management and IT

Output 12.1		2	100.000	Reduce consultancy services in areas of SR legal advice, FR consultancy, staff survey as well as intra muros external service provisions
			50.000	Postpone facilities and space improvement /optimisation
			40.000	Reduce missions that ensure business continuity among all geographical locations
Output 12.2		1	100.000	Reduce staff development activities
Output 12.3		2	200.000	Postpone Zero Trust Architecture projects
			100.000	Postpone further Implementation/ Optimisation of ServiceNow Platform for increasing internal capabilities
			50.000	Reduce DG services SLA
			50.000	Reduce DG HRIS and Financial Information Systems implementation (estimation pending information from DG HR/Digit)
			662.000	Postpone SAN solution – data storage upgrade
			60.000	Postpone DR Implementation
			150.000	Postpone Mobile devices EOL with insurance
			300.000	Postpone End User devices EOL
			104.210	Postpone Networking Equipment (FW and Switches) EOL
Total		5	2.055.790	

ANNEX

I. ORGANISATION CHART AS OF 01.12.2022



EXECUTIVE DIRECTOR
Management team

POLICY DEVELOPMENT AND IMPLEMENTATION UNIT

MARKET, CERTIFICATION AND STANDARDISATION UNIT

CAPACITY BUILDING UNIT

OPERATIONAL COOPERATION UNIT

- Research & Innovation team
- Awareness & Education team
- Knowledge & Information team
- International Cooperation team

ACCOUNTANT

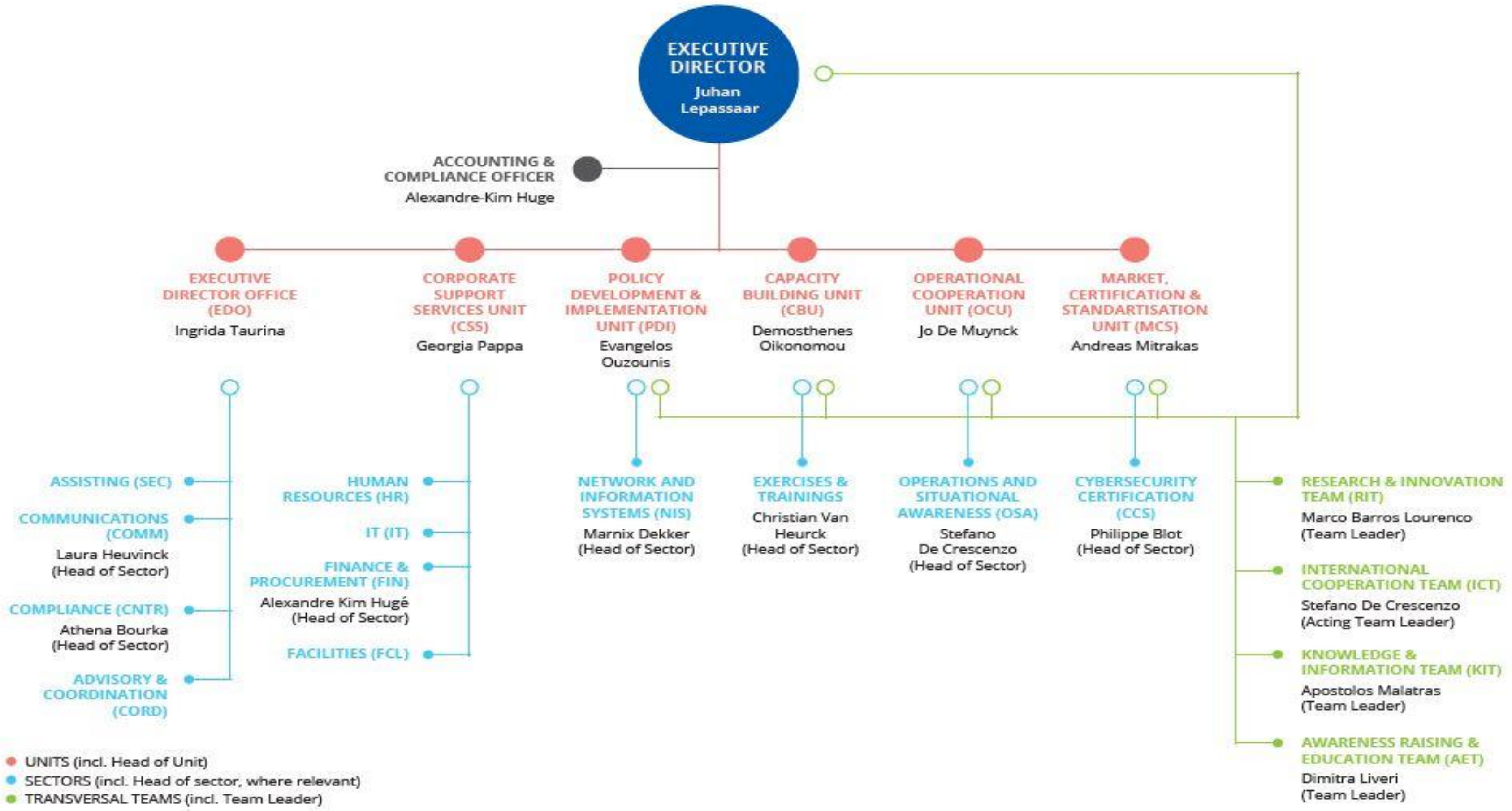
EXECUTIVE DIRECTOR'S OFFICE

Communication
Coordination
Internal Control & Compliance
Administration

CORPORATE SUPPORT SERVICES

Human Resources
Finance
Procurement
IT services

Administrative Organigramme



EXECUTIVE DIRECTOR
Juhan Lepassaar

ACCOUNTING & COMPLIANCE OFFICER
Alexandre-Kim Huge

EXECUTIVE DIRECTOR OFFICE (EDO)
Ingrida Taurina

- ASSISTING (SEC)
- COMMUNICATIONS (COMM)
  Laura Heuvinck
  (Head of Sector)
- COMPLIANCE (CNTR)
  Athena Bourka
  (Head of Sector)
- ADVISORY & COORDINATION (CORD)

CORPORATE SUPPORT SERVICES UNIT (CSS)
Georgia Pappa

- HUMAN RESOURCES (HR)
- IT (IT)
- FINANCE & PROCUREMENT (FIN)
  Alexandre Kim Hugé
  (Head of Sector)
- FACILITIES (FCL)

POLICY DEVELOPMENT & IMPLEMENTATION UNIT (PDI)
Evangelos Ouzounis

- NETWORK AND INFORMATION SYSTEMS (NIS)
  Marnix Dekker
  (Head of Sector)

CAPACITY BUILDING UNIT (CBU)
Demosthenes Oikonomou

- EXERCISES & TRAININGS
  Christian Van Heurck
  (Head of Sector)

OPERATIONAL COOPERATION UNIT (OCU)
Jo De Muynck

- OPERATIONS AND SITUATIONAL AWARENESS (OSA)
  Stefano De Crescenzo
  (Head of Sector)

MARKET, CERTIFICATION & STANDARTISATION UNIT (MCS)
Andreas Mitrakas

- CYBERSECURITY CERTIFICATION (CCS)
  Philippe Blot
  (Head of Sector)

RESEARCH & INNOVATION TEAM (RIT)
Marco Barros Lourenco
(Team Leader)

INTERNATIONAL COOPERATION TEAM (ICT)
Stefano De Crescenzo
(Acting Team Leader)

KNOWLEDGE & INFORMATION TEAM (KIT)
Apostolos Malatras
(Team Leader)

AWARENESS RAISING & EDUCATION TEAM (AET)
Dimitra Liveri
(Team Leader)

🟥 UNITS (incl. Head of Unit)
🟦 SECTORS (incl. Head of sector, where relevant)
🟩 TRANSVERSAL TEAMS (incl. Team Leader)

Status in-house staff (AD;AST;CA;SNEs) on 31.12.2022

ED*		EDO		CSS		PDI		CBU		OCU		MCS		SUMMARY	
AD	2	AD	7	AD	2	AD	15	AD	8	AD	10	AD	14	**AD**	**55**
Total	**2**	AST	7	AST	6	AST	0	AST	2	AST	1	AST	2	**AST**	**18**
		CA	2	CA	7	CA	5	CA	7	CA	3	CA	3	**CA**	**27**
		SNE	1	SNE	0	SNE	0	SNE	1	SNE	6	SNE	2	**SNE**	**10**
		Total	**17**	**Total**	**15**	**Total**	**17**	**Total**	**18**	**Total**	**20**	**Total**	**21**	**Total**	**110**

* ED and accountant

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 (Act 11-12) 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	€757.564	4,75
Supporting implementation of Union policy and law	Activity 2	€1.955.001	13
Building capacity	Activity 3	€2.876.088	13,75
Enabling operational cooperation	Activity 4	€3.516.103	16,5
Contribute to cooperative response at Union and Member States level	Activity 5	€1.792.792	10
Development and maintenance of EU cybersecurity certification framework	Activity 6	€1.597.567	9
Supporting European cybersecurity market and industry	Activity 7	€901.466	6
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	€1.555.976	8,5
Outreach and education	Activity 9	€1.166.897	7,5
Research and innovation	Activity 10	€562.903	4
Performance and risk management	Activity 11	€2.682.263	18
Staff development and working environment	Activity 12	€6.310.176	17
TOTAL		**€25.674.796**	**128,00**

III. FINANCIAL RESOURCES 2024 - 2026

Table 1: Revenue

revenues	2023	2024
EU contribution	24.475.757	24.953.072
Other revenue (EFTA)	707.738	721.724
Total	25.183.495	25.674.796

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%	24.953.072	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	1,98%	721.724	723.392	727.009
- of which EEA/EFTA (excl. Switzerland)	*707.738*	*1,98%*	*721.724*	*723.392*	*727.009*
- of which Candidate Countries					0
4 OTHER CONTRIBUTIONS	*	N/A	*	*	
5 ADMINISTRATIVE OPERATIONS					0
- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)					0
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT					0
7 CORRECTION OF BUDGETARY IMBALANCES					0
TOTAL REVENUES	**25.183.495**	**1,95%**	**25.674.796**	**26.163.325**	**26.294.142**

* - 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 2024-2025 same surplus as indicated under 2023 is included with 2,93% EFTA proportionality factor

Additional EU funding: grant, contribution and service-level agreements not applicable to ENISA

Table 2: Expenditure

EXPENDITURE	2023		2024		2024
	Commitment appropriations	**Payment appropriations**	**Commitment appropriations**	**Payment appropriations**	**Required budget**
Title 1	12.719.412	12.719.412	13.634.668	13.634.668	13.961.668
Title 2	3.519.470	3.519.470	3.969.506	3.969.506	6.313.040
Title 3	8.944.613	8.944.613	8.070.622	8.070.622	11.275.347
Total expenditure	**25.183.495**	**25.183.495**	**25.674.796**	**25.674.796**	**31.550.055**

EXPENDITURE (in EUR)	Commitment and Payment appropriations						
	Amended budget 2022 (*)	Adopted Budget 2023 Agency	Draft estimated budget 2024	VAR 2024 / 2023	Required budget 2024	Envisaged in 2025	Envisaged in 2026
Title 1. Staff Expenditure	**11.917.868**	**12.719.412**	**13.634.668**	**7%**	**13.961.668**	**13.894.103**	**13.963.574**
11 Staff in active employment *	9.862.695	11.019.993	12.342.690	12%	12.342.690	12.577.542	12.640.430
12 Recruitment expenditure	405.780	404.684	100.000	-75%	100.000	101.903	102.412
13 Socio-medical services and training	1.101.619	923.735	850.423	-8%	1.148.423	866.604	870.937
14 Temporary assistance	547.774	371.000	341.555	-8%	370.555	348.054	349.795
Title 2. Building, equipment and miscellaneous expenditure	**3.236.767**	**3.519.470**	**3.969.506**	**13%**	**6.313.040**	**4.045.036**	**4.065.261**
20 Building and associated costs	1.065.153	1.357.750	1.382.841	2%	1.482.841	1.409.153	1.416.199
21 Movable property and associated costs (**)	64.285	0	0	n.a.	0	0	0
22 Current corporate expenditure	480.593	472.650	978.262	107%	1.081.796	996.876	1.001.861
23 Corporate ICT	1.626.737	1.689.070	1.608.402	-5%	3.748.402	1.639.006	1.647.201
Title 3. Operational expenditure	**9.052.990**	**8.944.613**	**8.070.622**	**-10%**	**11.275.347**	**8.224.186**	**8.265.307**
30 Activities related to meetings and missions	551.000	438.600	356.000	-19%	936.000	362.774	364.588
37 Core operational activities	8.501.990	8.506.013	7.714.622	-9%	10.339.347	7.861.412	7.900.720
TOTAL EXPENDITURE	**24.207.625**	**25.183.495**	**25.674.796**	**0**	**31.550.055**	**26.163.325**	**26.294.142**
(*) 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							

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**

III.a Cancellation of appropriations to be updated after closure of the year

To be updated during next iteration for work programme 2022.

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	2024	2025	2026
ESTABLISHMENT PLAN POSTS	Authorised **Budget**	**Actually filled as of 31/12/2022**	**Occupancy rate %**	Adopted	Envisaged staff	Required staff to fullfil mandate	Envisaged staff	Envisaged staff
Administrators (AD)	63	55	87%	63	63	75	63	63
Assistants (AST)	19	18	94%	19	19	22	19	19
Assistants/Secretaries (AST/SC)								
TOTAL ESTABLISHMENT PLAN POSTS	82	73	90%	82	82	97	82	82
EXTERNAL STAFF	**FTE corresponding to the authorised budget 2022**	**Executed FTE as of 31/12/2022**	**Execution Rate %**	**Adopted FTE**	**Envisaged FTE**	Required staff	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	32	27	84%	32	32	32	32	32
Seconded National Experts (SNE)	12	10	83%	14	14	16	14	14
TOTAL External Staff	**44**	37	**84%**	**46**	46	48	46	46
TOTAL STAFF[84]	**126**	**110**	**87%**	**128**	**128**	**145**	**128**	**128**

[84] 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
	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	n/a	n/a	n/a	n/a	n/a
Seconded National Experts (SNE)	n/a	n/a	n/a	n/a	n/a
TOTAL	n/a	n/a	n/a	n/a	n/a

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[85]

Function group and grade	2022				2023		2024		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		23		24		24
AD 7		8		11		10		9		8		8
AD 6		9		15		4		3		2		2
AD 5												
AD TOTAL		63		55		63		63		63		63
AST 11												
AST 10												
AST 9												
AST 8		2		2		2		3		4		4
AST 7		3		1		4		4		4		4
AST 6		8		5		7		7		7		7
AST 5		5		4		5		5		4		4
AST 4		1		4		1		0		0		0
AST 3				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												

[85] 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.

Function group and grade	2022				2023		2024		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 Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication *		CA Recruitment Function Group (I, II, III and IV)
	Due to foreseen retirement/ mobility	New post requested due to additional tasks	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		3 TAs	n/a	n/a	n/a

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)**	**2017**		**31.12.2022**	
	Number	**%**	**Number**	**%**
Female Managers	2	0	3[86]	27%
Male Managers	8	100	8[87]	73%

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

[86] This category comprises Heads of Unit and Team Leaders
[87] This category comprises Heads of Unit and Team Leaders

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 *[88]	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%
GR	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%

[88] 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

Looking back to 2021, it has been noted that the positive mesures to improve the diversity of nationalities which had taken place in 2020 and 2021, have borne fruit. This can be attributed to the broad outreach campaigns on popular media across the European Union, closer consideration on the nationality spread in relation to competencies requested, and specific provisions on the vacancy notices have been continued[89].

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**
Number of service contracts in place with international schools:	**Same as the previous school year, for school year 2022-2023, the process for the financial support for the staff of ENISA in relation to the cost of schooling has been updated via EDD 2021-41, leading to the abolishment of SLAs and remains unchanged.**

VI. ENVIRONMENT MANAGEMENT

ENISA investigating opportunities to strengthen its environmental management during the course of 2022 with the introduction of a dedicated output in activity 11 to carry out an overarching audit on the CO2 impact of all operations of the Agency. The results and accompanying action plan have been produced and will be rolled out over the coming years. In addition a new tender was launched in 2022 for building management that includes an emphasis on energy efficiency.

VII. BUILDING POLICY

Current buildings

Building Name and type	Location	Location SURFACE AREA(in m²)	RENTAL CONTRACT	Host country	Building present value(€)

[89] The seeming imbalance related to the most represented nationality at ENISA is related to several factors, such as, for example, the level of posts and related salaries which may be perceived as less appealing for job seekers in relatively more advanced member state economies; the fact that ENISA has a better position as employer compared to average conditions offered in the Greek job market; the small job market in Greece for cybersecurity professionals; historic decisions taken by previous AIPNs. Another reason that may be cited is the need for stability during the start up phase of the Agency, as staff from the hosting member state (Greece) is less prone to resign (resulting in lesser turnover), which in combination with the relatively young age of the Agency compared to others, still has its original impact; the relatively better academic profile of Greek candidates that bears for lower level posts; the relatively smaller payroll cost for staff that is relatively better qualified than average while costing less if expatriation allowance is considered, as well as the general predisposition to retain a lower level position in the home country.

								(grant or support)	
		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					

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 the course of 2022 a satisfaction survey was developed to gather feedback from stakeholders on the added value and take up of ENISA work programmes over the past two years. The survey will be launched in Q1 2023 to provide lessons learned for ex-ante evaluation.

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

As adopted by the Management Board[90], the Agency's strategy for effective internal controls is based on international practices (COSO Framework's international Standards), as well the relevant internal control framework of the European Commission.

The Control Environment is the set of standards 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.

The Common Approach on EU Decentralised Agencies foresees that EU agencies should be more active concerning fraud prevention issues and that the related communication forms an essential part of its success. In 2021 ENISA adopted an anti-fraud strategy[91] as recommended by the European Anti-Fraud Office (OLAF).

The Anti-Fraud Strategy and action plan describes the objectives, actions and roles of responsibilities in order to address identified risks.

The following five objectives are outlined in strategy:

Objective 1: Integrity and compliance through efficient and targeted communication on ethics and fraud awareness.
Objective 2: Compliance and transparency measures in Procurement.
Objective 3: Compliance and transparency measures in Recruitment.
Objective 4: Compliance and transparency measures in Assets management/inventory.
Objective 5: Establish a system for internal reporting of suspected fraud or irregularities.

An action plan has been drawn up and is described in the strategy to meet the objectives mentioned above. This action plan is intended to implement the ENISA Anti-fraud strategy and ensure the sound management of public procurement, recruitment and the other risk areas identified.

[90] 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)
[91] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-5-on-anti-fraud-strategy

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 aimed to consolidate input from different sources and integrate the results of various risk assessments within a single internal control assessment process. The revised ENISA's internal control framework will will be used for the assessment of internal controls within 2023, together with a comprehensive methodology for enterprise risk assessment across the Agency.

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

ENISA does not receive any form of grant, contributions or service level agreements leading to additional revenue.

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

The international strategy foresees a continuation of the strong 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. The Agency's international strategy [92] was adopted by the MB during the November 2021 meeting and the actions for international strategy is addressed under output 9.3 in activity 9.

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 of the CSA requires the Management Board of ENISA to adopt 'a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent' (1). The CSA also refers to specific international organisations (e.g. Organisation for Economic Co-operation and Development (OECD), Organization for Security and Co-operation in Europe (OSCE) and North Atlantic Treaty Organisation (NATO)) that ENISA is called to develop relations with (see recital 43).

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.

XIV. SUPPRESSED OUTPUTS, POSTPONED PROJECTS, REDUCED SCOPE FROM 2023

The following tables detail the impact of insufficient resources on the Agency's operations and corporate services in 2023. ENISA conducted a prioritisation exercise to select the most impactful outputs and suppress or reduce the scope of certain projects to meet resources constraints if no additional resources are allocated to ENISA in the short and/or medium term. The total shortfall that the Agency identified amounts to 2.5m in corporate services and 734k and 2 FTEs in operations.

Activity 3

OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED

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

Output	Service package	FTEs required	Budget required	Comments
Output 3.2	TREX, NIS		100.000	Scope reduction: Two less exercises than planned
Output 3.4	TREX	0,55	64.000	Output proposed to be suppressed during 2023 work programme. The RM Framework developed in 2022 can be reviewed and optimised as from 2024.
Output 3.5	TREX		30.000	Reduced scope of project, remaining amount adequate in order to maintain the operations of the respective adhoc working group.
Total		0,55	194.000	

Activity 4

OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 4.1	NIS, SITAW	0,30	30.000	Reduced scope of CSIRT/LEA cooperation activities
Output 4.3	SITAW, NIS		50.000	Reduced maintenance for some (internal and external) situational awareness systems
Total		0,30	80.000	

Activity 5

OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 5.1	SITAW, INDEX		100.000	Postponement of new features for OpenCSAM
Output 5.2	SITAW	0,20	100.000	Reduced engagements under the Cyber Assistance Mechanism
Total		0,20	200.000	

Activity 8

OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments

Output 8.6	INDEX, SITAW	1,00	110.000	Propose to suppress this output in 2023 and revisit the ransomware threat landscape in 2024. In the context of the 2023 ETL, ransomware will also be covered to some degree.
Total		1,00	110.000	

Activity 9

OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 9.1	NIS		20,000	Reduce material for the OES campaigns
Output 9.2	INDEX, CERTI		35,000	Reduce activities on #CyberAll such as diversity in cybersecurity
			15,000	Cancel activities supporting EUROPOL nomoreransom campaign
Output 9.4	TREX		40,000	Cancel planned ECSM related physical events
Output 9.5	INDEX, TREX		20,000	Reduce scope of the European Cybersecurity Skills Framework review
Output 9.6	INDEX		20,000	Reduce scope of Cybersecurity Educational Roadmap
Total			150,000	

Activity 11

OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 11.1	All service packages		136.000	Postponement of project for the web development to 2024
Output 11.2	All service packages		50,000	Postponement of ENISA website migration and development to 2024
Output 11.5	All service packages		110,000	Postponement of IntraMuros support services

Total			296,000	

Activity 12

OUTPUTS SUPRESSED / SCOPE REDUCED / PROJECTS POSTPONED				
Output	Service package	FTEs required	Budget required	Comments
Output 12.1	All service packages		29000	Reduced volume of interim services
			15000	*Reduce Webex large meetings*
			14000	*Postpone Microsoft licences renewal*
			20000	*Postpone other smaller ICT recurrent projects*
Output 12.2			95000	Reduced consultancy services in areas of SR legal advice, FR consultancy, staff survey
			35000	Reduced staff development activities
Output 12.3			*700000*	*Postpone Alternative Back Up solution (vs IDPA)*
			200000	*Postpone Zero Trust Architecture Projects*[93]
			80000	*Postpone eRecruitment and CEI tool*[94]
			50000	*Postpone Ticketing and IT Asset Management Tool*
			70000	*Postpone Mobiles Devices with Insurance*
			20000	*Postpone datacenter hardware renewals*

			5000	*Postpone other smaller ICT one off projects*
			260000	*Reduced providers of ICT services and helpdesk*
			100000	*Postponed Data recovery site update*
			100000	*Reduced Videoconferencing and services (Boardroom)*
			50000	*Reduced Webex advanced support*
Output 12.4			218000	Reduced staff welfare package
Output 12.5			210000	Reduced intra-muros services and missions (EUR 5 K)
Total			2 271 000	

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 € 25674796 and consists of a subsidy of € 24953072 from the General Budget of the European Union and EFTA countries' contributions € 721724

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 € 13.634.668,18

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to € 3.969.505,92

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of
Work Programme 2024 and amounts to € 8.070.621,91

3. STATEMENT OF REVENUE 2024

Title	Heading	Voted Appropriations 2022 €	Voted Appropriations 2023 €	Proposed Draft Appropriations 2024 €	Remarks - budget 2024
1	**EUROPEAN COMMUNITIES SUBSIDY**	**23.633.000**	**24.475.757**	**24.953.072**	Total subsidy of the European Communities
2	**THIRD COUNTRIES CONTRIBUTION**	**574.625**	**707.738**	**721.724**	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**	**25.674.796**	

Article Item	Heading	Voted Appropriations 2022 €	Voted Appropriations 2023 €	Proposed Draft Appropriations 2024 €	Remarks - budget 2024
1	**EUROPEAN COMMUNITIES SUBSIDY**				
10	**EUROPEAN COMMUNITIES SUBSIDY**				
100	***European Communities subsidy***	**23.633.000**	**24.475.757**	**24.953.072**	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security. *Includes a reserve of EUR 610 00 under NIS2 directive*
	CHAPTER 10	**23.633.000**	**24.475.757**	**24.953.072**	
	TITLE 1	**23.633.000**	**24.475.757**	**24.953.072**	
2	**THIRD COUNTRIES CONTRIBUTION**				
20	**THIRD COUNTRIES CONTRIBUTION**				
200	***Third Countries contribution***	**574.625**	**707.738**	**721.724**	Contributions from Associated Countries.
	CHAPTER 2 0	**574.625**	**707.738**	**721.724**	
	TITLE 2	**574.625**	**707.738**	**721.724**	
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	0	Revenue from administrative operations.
	CHAPTER 40	**0**	**0**	**0**	
	TITLE 4	**0**	**0**	**0**	
	GRAND TOTAL	**24.207.625**	**25.183.495**	**25.674.796**	

4. STATEMENT OF EXPENDITURE 2024

Title	Heading	Voted Appropriations 2022 €	Voted Appropriations 2023 €	Proposed Draft Appropriations 2024 €	Remarks - budget 2024
1	**STAFF**	**12.494.335**	**12.719.412**	**13.634.668**	Total funding for covering personnel costs.
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**	**2.824.300**	**3.519.470**	**3.969.506**	Total funding for covering general administrative costs.
3	**OPERATIONAL EXPENDITURE**	**8.888.990**	**8.944.613**	**8.070.622**	Total funding for operational expenditures.
	GRAND TOTAL	**24.207.625**	**25.183.495**	**25.674.796**	
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	9.374.377	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). *Includes a reserve of EUR 450 000 under NIS2 directive*
		Article 1 1 0	8.361.489	8.551.219	9.374.377	
111	***Other staff***					
1110	Contract Agents		1.819.391	1.967.658	2.146.417	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). *Includes a reserve of EUR 160 000 under NIS2 directive*
1113	Seconded National Experts (SNEs)		657.000	501.116	821.896	This appropriation is intended to cover basic salaries and all benefits of SNEs.
		Article 1 1 1	2.476.391	2.468.774	2.968.313	
		CHAPTER 11	**10.837.880**	**11.019.993**	**12.342.690**	
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	100.000	This appropriation is intended to cover the travel expenses of staff (including members of their families), the installation allowances for staff obliged to change residence after taking up their duty, the removal costs of staff obliged to change residence after taking up duty, the costs of daily subsistance allowances as per Staff Regulations applicable to officials of the European Communities (SR) and in particular Articles 20 and 71 thereof and Articles 5, 6, 7, 9, 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants. This appropriation is intended to cover expenditure related to recruitment, e.g. incurred for interviewing candidates, external selection committee members, screening applications and other related costs.
		Article 1 2 0	10.000	404.684	100.000	
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**	**100.000**	

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	213.785	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	213.785	
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	636.637	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	636.637	
		CHAPTER 1 3	**853.000**	**923.735**	**850.423**	
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	341.555	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
		Article 1 4 2	321.455	371.000	341.555	
		CHAPTER 1 4	**391.455**	**371.000**	**341.555**	
		Total Title 1	**12.494.335**	**12.719.412**	**13.634.668**	
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	1.382.841	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	1.382.841	
	CHAPTER 2 0	**914.550**	**1.357.750**	**1.382.841**	
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	892.643	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	892.643	
223	***Corporate and Administrative Expenditures***				
2230	Corporate and Administrative Expenditures	n/a	93.000	85.619	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	85.619	
	CHAPTER 2 2	**320.000**	**472.650**	**978.262**	
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 corpororate ICT costs	n/a	1.689.070	1.608.402	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	1.608.402	
	CHAPTER 2 3	**1.429.750**	**1.689.070**	**1.608.402**	
	Total Title 2	**2.824.300**	**3.519.470**	**3.969.506**	
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	356.000	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 11-12 as defined in the SPD 2024-2026 mainly covering horizontal tasks and other administrative services.
	Article 3 0 0	387.000	438.600	356.000	
	CHAPTER 3 0	**387.000**	**438.600**	**356.000**	

37	**CORE OPERATIONAL ACTIVITIES**				
371	***Activity 1 - Providing assistance on policy development***				
3710	Activity 1 - Providing assistance on policy development	363.000	330.262	299.535	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	299.535	
372	***Activity 2 - Supporting implementation of Union policy and law***				
3720	Activity 2 - Supporting implementation of Union policy and law	798.475	773.404	701.447	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	701.447	
373	***Activity 3 - Capacity building***				
3730	Activity 3 - Capacity building	1.921.265	1.709.239	1.550.213	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	1.550.213	
374	***Activity 4 - Enabling operational cooperation***				
3740	Activity 4 - Enabling operational cooperation	1.703.350	2.122.530	1.925.053	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	1.925.053	
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	828.519	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	828.519	
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	729.721	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	729.721	
377	***Activity 7 - Supporting European cybersecurity market and industry***				
3770	Activity 7 - Supporting European cybersecurity market and industry	373.800	356.027	322.903	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	322.903	
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	736.344	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	736.344	
379	***Activity 9 - Outreach and education***				
3790	Activity 9 - Outreach and education	439.900	489.209	443.693	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	443.693	
370	***Activity 10 - Advise on Research and Innovation Needs and priorities***				
3700	Activity 10 - Advise on Research and Innovation Needs and priorities	439.900	195.371	177.194	This appropriation is intended to cover direct operational costs relevant to the Activity 10 (including operational ICT and mission costs).
	Article 3 7 0	439.900	195.371	177.194	
	CHAPTER 3 7	**8.501.990**	**8.506.013**	**7.714.622**	
	TITLE 3	**8.888.990**	**8.944.613**	**8.070.622**	
	GRAND TOTAL	**24.207.625**	**25.183.495**	**25.674.796**	

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

Draft Establishment plan 2024[1]

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		23
AD 7		10		9
AD 6		4		3
AD 5				
Total AD		**63**		**63**
AST 11				
AST 10				
AST 9				
AST 8		2		3
AST 7		4		4
AST 6		7		7
AST 5		5		5
AST 4		1		0
AST 3				
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**

[1] The change in the number of establishment plan up to 10% requested for year 2024 is modified as per Art 38 of the ENISA Financial Regulation