MB Decision 2022/14 on the Single Programming Document (SPD) 2023-2025

DECISION No MB/2022/14 of the Management Board of the European Union Agency for Cybersecurity (ENISA) adopting the Single Programming Document (SPD) 2023-2025, the statement of estimates for 2023 and the establishment plan for 2023

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.

Having regard to Commission Opinion C(2022) 6778 on the draft Single Programming Document for 2023 – 2025 of ENISA dated 16.09.2022;

Having regard to Commission Communication C(2014) 9641 final, on the guidelines for programming document for decentralised agencies and the template for the Consolidated Annual Activity Report for decentralised agencies dated 16.12.2014;

Whereas:

(1) The Single Programming Document 2023-2025 should be adopted by the Management Board by 30 November 2022.

(2) The Single Programming Document 2023 -2025 was scrutinised by the Executive Board on 21 October 2022.

[1] *OJ L 151, 7.6.2019, p. 15–69*

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

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2023-2025, including the Annual Cooperation Programme with CERT-EU for 2023 is adopted as set out in the Annex 1 of this decision.

Article 2

The statement of estimates of revenue and expenditure for the financial year 2023 and the establishment plan 2023 is adopted as set-out in Annex 2 and Annex 3 of this decision. They shall become final following the definitive adoption of the general budget of the Union for the financial year 2023.

Article 3

Where necessary, the Management Board shall adjust ENISAs Single Programming Document 2023-2025 and ENISA's budget and the establishment plan in accordance with the general budget of the Union for the financial year 2023.

Article 4

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

Done at Athens on 17 November 2022.

On behalf of the Management Board,

Chair of the Management Board of ENISA

MB Decision 2022/14 on the Single Programming Document (SPD) 2023-2025

ANNEX 1

Adopted Single Programming Document 2023-2025

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ADOPTED_SINGLE PROGRAMMING DOCUMENT _2023-2025

Including Multiannual planning,
Work programme 2023 and
Multiannual staff planning

VERSION: ADOPTED

TABLE OF CONTENTS

LIST OF ACRONYMS

To be updated at a later stage

ABAC	Accrual-based accounting
AD	Administrator
AST	Assistant
BEREC	Body of European Regulators for Electronic Communications
CA	Contract agenda
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 the EU institutions, bodies and agencies
COVID-19	Coronavirus disease 2019
CSA	Cybersecurity Act
CSIRT	Computer Security Incidence Response Team
CyCLONe	Cyber Crisis Liaison Organisation Network
DORA	Digital Operational Resilience Act (DORA)
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
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
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
MoU	Memorandum of understanding
NIS	Networks and Information Systems
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
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

The strong cyber dimension of the Russian war of aggression against Ukraine and its reflections to the cybersecurity threat landscape have once again emphasized the role of ccybersecurity as a cornerstone of a digital and connected Europe. Despite the spill-overs and direct attacks, by-and-large the EU has been able to deal with the cyber threats posed by the Russian aggression through the resilience of the Member States and across Europe, as well as forging support and cooperation with Ukraine and other allies and partners.

Within this context, ENISA's challenge is both to keep pace and set the pace in supporting the Union in achieving a high common level of cybersecurity across Europe. This Single Programming Document (SPD) for the years 2023-2025 represents another step to bring this about:

Firstly, it puts emphasis on strengthening the resilience of Member States and EU Institutions, Bodies and Agencies. In 2023, approximately half of ENISA's operational resources, both budget and human resources, shall be dedicated to enhancing operational cooperation and building capacity. Together with the one-off support of up to 15 MEUR, which the European Commission allocated to ENISA in Autumn 2022, the Agency will be able to massively scale up and expand its ex-ante and ex-post services to the Member States in 2023.

Secondly, building on the outcomes of strategic discussions within its Management Board throughout 2022, the Agency has developed service packages in key areas of its mandate. They 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.

Thirdly, through this work-programme ENISA shall endeavor to help Member States to prepare for the transposition of the reviewed NIS Directive, as well as to prepare the ground for the roll-out and implementation of the EU cybersecurity certification schemes.

Finally, recognizing the growing need to bring together the EU's activities and resources across the cybersecurity communities, this SPD establishes a new activity in the area of research and innovation, to structure the Agency's cooperation and collaboration with the European Cybersecurity Competence Centre (ECCC) and its emerging networks.

All those areas also accentuate the resource constraints under which the Agency now operates. The foreseen budget increase for the 2023 work programme has been fully absorbed by the increase in staff expenditure and inflation. Due to a shortfall of over 3 MEUR, the Agency has had to reduce the scope of some of its operational activities, limiting the number of exercises and training it rolls-out or postponing its actions in countering ransomware.

Such reductions mean drawbacks in certain areas, but might become a real obstacle if new tasks should be added to the Agency without a parallel increase of its resources. Thus, though ENISA welcomes the pioneering set of cybersecurity initiatives being put forward in 2022 and relishes the different and varied roles they imply for the Agency, it needs to have the right level of human and financial resourcing to match those aims and ambitions.

The EU has been mastering cybersecurity initiatives and structures not least through a unique cross-party and cross-Member State general consensus as its prime driving force. This consensus should now also include the resourcing of the Agency. This would give the Union the ability it needs to steer cybersecurity developments in the years to come.

Juhan Lepassaar
Executive Director

MISSION STATEMENT

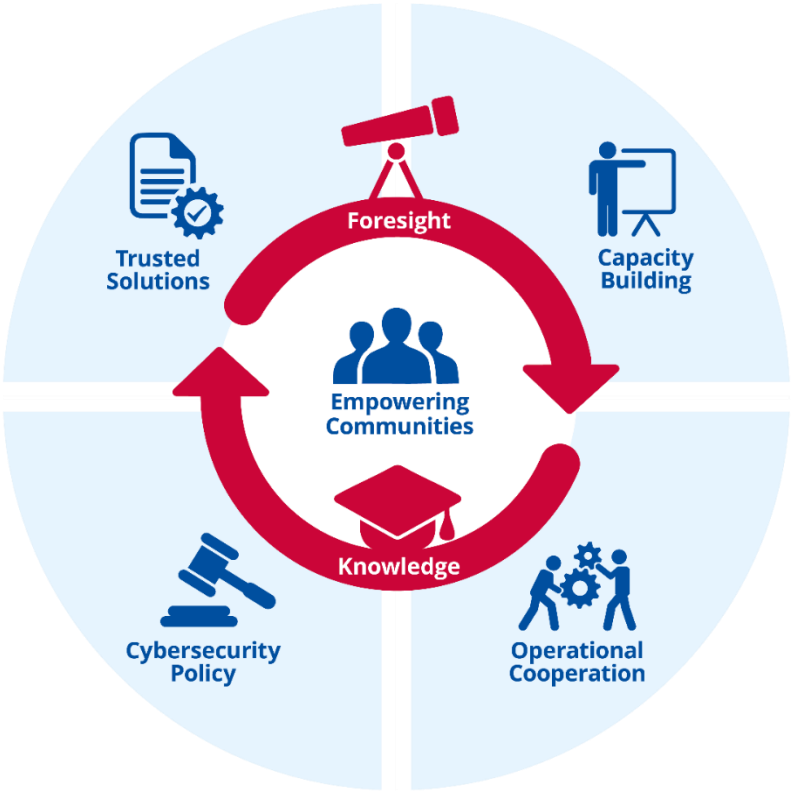
The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical 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 Russian war of aggression against Ukraine dominates today's EU security agenda and threatens global stability and security. ENISA has stepped up its coordination and preparedness and contributed to the EU's shared situational awareness by providing regular situational reports of cyber activity. There has also been intensified coordination and exchange of information with cybersecurity networks, such as the Cyber Crises Liaison Organisation Network (CyCLONe) consisting of national cybersecurity crisis management authorities, and numerous sectorial communities supported by ENISA. In addition constant efforts ensured channels of communication between the political, operational and technical levels, as well enhanced cooperation with the Computer Security Incident Response Teams (CSIRT) Network were realised.

Preparedness in the area of cybersecurity is more essential than ever, given the increased exposure of Europe to an accumulation of threats due to the war. Efforts to step up preparedness included a number of actions such as exercises, guidance, legislative measures, increasing resilience in critical sectors, and work with partners. During the French Presidency of the Council of the European Union, together with the European External Action Service (EEAS) and ENISA organised a scenario-based exercise in early 2022, called EU CyCLES (Cyber Crisis Linking Exercise on Solidarity), with the aim of raising awareness at the political level and strengthening cooperation between the operational and political levels in case of a large-scale cyber-attack.

ENISA cybersecurity support action

While the implementation of a new "Emergency Response Fund for Cybersecurity" is under assessment and may require further deliberations, DG CONNECT allocated EUR 15 million 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. As such the work programmes regular tasks under activities 3, 4 and 5 have been expanded to continue this support well into 2023.

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 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) for 2022 marks the 10th iteration of this flagship report and will be 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 revised Network and Information Security Directive (NIS 2) is expected to change 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 is scheduled for publication in November 2022 and 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 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.

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

In May 2022 political agreement was reached between the European Parliament and EU Member States on the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) proposed by the Commission in December 2020. The NIS2 proposal consolidates, reinforces and extends the existing approach under the NIS1, consolidating cybersecurity provisions from other legislation (EECC/telecoms and eIDAS/trust) under the NIS2, strengthening for example the incident reporting provisions, and extending the scope, including cloud and data centres under the critical services, and adding additional sectors, such as space (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 or shield, protecting less mature and harder to protect sectors such as health care. In addition the NIS2 ambitions need to be supported for instance on better 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, on 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. The transposition of NIS2 into national law and implementation phase lie ahead, as such 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 NIS Directive , with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the outcome of the proposal in the coming years, using existing resources and building on these wherever necessary.

Joint Cyber Unit

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 2020 EU Cybersecurity Strategy outlined the need for a Joint Cyber Unit (JCU), identifying the main problems that it would contribute to solve, its objectives and the steps needed to achieve it and builds on the work started with the Recommendation (4520 (2021) on a coordinated response to incidents and crises - so called Blueprint in 2017.

ENISA will contribute to the next steps following the EC Recommendation (4520 (2021) on 'building the Joint Cyber Unit') and Council Conclusions (20 October 2021 (ST 13048 2021) on ‘exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises’), with a view to contributing to the further development of an EU crisis management framework along the lines and according to the roles defined in the on-going discussions amongst Member States and EU operational actors.

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 (and upcoming NIS2 framework) and the Cybersecurity Act. The Act establishes common European cybersecurity requirements for products with digital elements that are placed on the internal market by introducing essential requirements for products with digital elements as well as obligations for manufacturers, importers and distributors. 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 CRA will apply 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.

ENISA has provided expert opinion and is working towards collecting evidence to support the Impact Assessment through its Cybersecurity Policy Observatory (CSPO) 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.

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 public authorities in the Member States. It is expected that the draft candidate cybersecurity certifications schemes proposed by ENISA will be adopted as 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 transposed in an EU Implementing Act by the Commission for its final adoption. In 2022 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 2023-2025.

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 under a notified eID scheme to 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 schemes under development and shall as well identify potential new certification means of schemes that would contribute to the certification of a wallet.

ENISA will also support the development of certification means that would allow to demonstrate compliance with certain requirements of Article 18 of the NIS 2 directive, as the Regulation provisions 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 for CRA related products, such as Protection 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, that the EC foresees to publish in Q4 2022.

Research & Innovation

The EU is expanding its support and investment in the wealth 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 has been 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 ongoing activities 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. These research and innovation need and funding priorities will constitute 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 (eIDAS) Regulation and identified factors hindering adoption of electronic identification mechanisms. In June 2021 the Commission made a proposal for a revised eIDAS Regulation establishing a European Digital Identity framework and a European Digital 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 2023-2025 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 proposal for a revised eIDAS regulation in addition to promoting the exchange of good practises and capacity building of relevant stakeholders. The revised eIDAS regulation also expands the list of qualified trust services with distributed ledgers and electronic archiving and management of remote devices for the creation of electronic signatures and seals. The NIS2 proposal for a revised NIS Directive foresees that the security 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). When this proposal is adopted, 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[1] and Coordinated Plan on Artificial Intelligence 2021[2], the EU is addressing the major technological, ethical, legal and socio-economic challenges to put AI at the service of European citizens and the economy, for instance by considering linking high-risk AI systems to mandatory trustworthiness requirements. One of these challenges is understanding the interplay between cybersecurity and AI and how this can affect availability, safety or resilience of future AI services and applications.

Building on ENISA's efforts towards securing AI / machine learning the Agency can continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2023-2025. 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 June 2022 the Council presidency and the European Parliament reached a political agreement on the regulation on digital operational resilience for the financial sector. 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 proposed legislation will require firms 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 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 [3], 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

[1] 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
[2] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review
[3] 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 [4] 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[5] with rules to increase cybersecurity in all EU institutions, by making it easier to share information on cyber threats and improving the efficiency of action to prevent and respond to cyber threats. This is expected to reduce the risk of incidents that cause material or reputational damage to EUIBAs. The proposal calls for increased cooperation with relevant bodies and stakeholders in the EU, via CERT-EU and ENISA. In addition it is proposed that ENISA will receive on a monthly basis a summary report from CERT-EU on significant cyber threats, significant vulnerabilities and significant incidents.

A proposed regulation[6] on information security in the institutions, bodies, offices and agencies of the Union was also put forward earlier in 2022 to create a minimum set of information security rules and standards for all EU institutions, bodies, offices and agencies to ensure an enhanced and consistent protection against the evolving threats to their information. These new rules will provide a stable ground for a secure exchange of information across EU institutions, bodies, offices and agencies and with the Member States, based on standardised practices and measures to protect information flows.

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 have initiated the discussion on signing 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 consider designing, developing and delivering capacity building and awareness raising activities to areas such as cybersecurity aspects of personal data protection and contribute jointly to similar activities organised by other EU or national bodies.

Trusted network of vendors and suppliers

[4] 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
[5] Cybersecurity – uniform rules for EU institutions, bodies and agencies (europa.eu)
[6] Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union | European Commission (europa.eu)

ENISA has initiated the development of a trusted network of vendors and suppliers for information exchange and cyber situational awareness with the aim to contribute to a cooperative response at Union and Member States level. The focus will be on building trusted bilateral partnerships about the threat and situational awareness and information sharing on cyber events. Followed by a request for information response (initiated by ENISA or by the other party) and collaboration on cyber information exchange projects.

SECTION II. MULTI-ANNUAL PROGRAMMING 2023 – 2025

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 new 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[7], 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.

[7] 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	KPI	METRICS
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	Community-building across the cybersecurity ecosystem	Number & types of activities at each engagement level Stakeholder satisfaction of ENISA's role as facilitator of community-building and collaboration across the cybersecurity ecosystem (survey)
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	ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante)	1. Number of relevant contributions to EU and national policies and legislative initiatives 2. Number of references to ENISA reports, analysis and/or studies in EU 3. Satisfaction with ENISA added-value of contributions (survey) 4. Number of EU policy files under development and supported by ENISA
			• 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	Contribution to policy implementation and implementation monitoring at EU and national level (ex-post)	1. Number of EU policies and regulations implemented at national level supported by ENISA 2 Number of ENISA reports, analysis and/or studies referred to at the EU and NIS cooperation group documents (survey) 3 Satisfaction with ENISA added-value of support (survey) [8] 4 Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)

[8] Surveys will be designed and developed in order to solicit a measurable response from participants to determine the added value of ENISAs contribution.

SO3 **Effective cooperation amongst operational actors within the Union in case of massive[9] 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	Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation	1. Number of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA 2. Uptake of the platform/ tool/ SOPs during massive cyber incidents 3. Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs including EU vulnerability database
			• 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	ENISA ability and preparedness to support response to massive cyber incidents	1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate 2. Number of relevant incident responses ENISA contributed to as per CSA Art7 3 Take up of ENISA support services 4 Number of trusted vendors 5.Stakeholders' satisfaction of ENISA's ability to provide operational support
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	Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	1. Increase/decrease of maturity indicators 2. Outreach, uptake and application of lessons learnt from capacity-building activities. 3. The number of exercises executed annually. 4. Stakeholder assessment on usefulness, added value and relevance of ENISA; and cooperation amongst communities in capacity building activities 5. ISAC maturity
		Art.10 & Art.12	• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience.	Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU Level of outreach	1. Number of cybersecurity incidents reported having human error as a root cause 2. Number of activities and participation to awareness raising actions organised by ENISA on cybersecurity topics

[9] large scale and cross-border

					3. Number of cybersecurity programmes (courses) and participation rates 4. Geographical and community coverage of outreach in the EU 5. Level of awareness, on cybersecurity across the EU/ general public (e.g. EU barometer)
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 are adopted Smooth transition to the EU cybersecurity certification framework Certified ICT products, services and processes are preferred by consumers and where relevant, Operators of Essential Services or Digital Service Providers	Uptake of the European cybersecurity certification framework and schemes as an enabler for more secure digital solutions Effective preparation of candidate certification schemes prepared by ENISA	1. Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions 2. Stakeholders level of trust in digital solutions of certification schemes (Citizens, public sector, businesses) and number of certificates issued on the basis of EU certification schemes 3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework 4. Number of candidate certification schemes prepared by ENISA 5. Number of people/organizations engaged in the preparation of certification schemes 6. Satisfaction with ENISA's support in the preparation of candidate schemes (survey)
			• Contribution towards understanding market dynamics • A more competitive European cybersecurity industry, SMEs and start-ups	Effectiveness of ENISAs supporting role for participants in the European cybersecurity market	1. Number of market analysis, guidelines and good practices issued by ENISA 2. Uptake of lessons learnt / recommendations from ENISA reports 3. Stakeholder satisfaction with the added value and quality of ENISA's work
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.	Contributing to Europe's Strategic Research and Innovation Agenda in the field of cybersecurity.	1 Number of requests from the EU-IBAs (including the ECCC) and MS to contribute, provide advice or participate in activities. 2 Number of references to ENISA advice and recommendations in the EU Strategic Research and Innovation Agenda including Annual and

					Multiannual Work programmes. 3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's advice on cybersecurity research needs and funding priorities (Survey)
SO7 **Efficient and effective cybersecurity information and knowledge management for Europe**	Activity 8	Art.9	• Decisions about cybersecurity are future proof and to take account the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision making	ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge	1. Number of users and frequency of usage of dedicated portal (observatory) 2 Number of recommendations, analysis, challenges identified and analysed 3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities (including threat landscapes 4 The influence of foresight on the development of ENISA work programme 5 Uptake of reports generated in activity 8 6 Uptake of the cybersecurity index

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	KPI	METRICS
Sound resource and risk management	Activity 11	Art 4(1)	Maximize quality and value provided to stakeholders and citizens Building lasting credibility and trust	1.Organisational performance 2. Trust in ENISA brand	1. Proportion of KPI's reaching targets 2. Individual contribution to achieving the objectives of the agency via clear link to KPI's (CDR report) 3. Exceptions in Risk Register 4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman 5. Number of complaints addressed timely and according to relevant procedures 6. Number of high risks identified in annual risk assessment exercise 7. Implementation of risk treatment plans 8. Number & types of activities at each engagement level 8. Observations from external audit bodies European Court of Auditors (ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed 9. Level of trust in ENISA (survey)

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	Staff commitment, motivation and satisfaction	1. Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools) 2. Quantity and quality of ENISA training and career development activities organised for staff 3. Reasons for staff departure (exit interviews) 4. Turnover rates 5. Establishment plan posts filled 6. Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services & tools) 7. Percentage of procurement procedures launched via e-tool (PPMT) 8. Percentage of payments made within 30 days 9. Late Payments

2. HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2023 – 2025

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

A number of factors, not considered or foreseen in 2021-2022 when the Commission established the MFF 2021-2027 programming, have had a cumulative effect on ENISA's resource requests during this period. Acknowledging ENISA's exceptional operational mandate, the Commission and the budgetary authority have continued to support ENISA's annual budget and post requests, including allocating additional posts to the Agency through the NIS2 directive, transferring additional seconded national expert posts 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.

The Agency has also, under the guidance of its Management Board, elaborated comprehensive service catalogues around its key tasks. Those service catalogues cover the Agency's services in support for the implementation of the revised NIS directive, certification, operational cooperation (in particular creating services to strengthen situational awareness at the Union level), capacity building (trainings and exercises) and knowledge and information management. The service catalogues have enabled the Agency to better match its outputs to the needs and priorities of the beneficiaries, create internal and external synergies thus increasing efficiency but also estimating resource needs necessary to cover the full catalogue of services. Those resource needs have been mapped under each activity within the current SPD, and they outline the fact that current resources represent over EUR 3 million less than ENISA's projected needs.

In terms of its human resources, the number of Establishment Plan posts has grown from 59 to 82 posts during the period 2019-2022, that is by 39 % as a result of the new tasks that were foreseen under the new Cybersecurity Act which came into force in 2019. Additional 5 posts (3 TAs and 2 CAs) have been authorised under 2022 for the new tasks under NIS2 Directive. The number of all authorised posts including TAs, CAs and SNEs grew following a similar trend or by 33 % during the period 2019-2022.

Table 1a Evolution of authorised posts and fulfilment

	2019	2020	2021	2022[10]
Number of posts in the Establishment Plan	59	69	76	82
% of fulfilment of the establishment plan on 31st of December	76%	80%	80%	94%
Total number of authorised posts (TAs, CAs, SNEs)	95	111	118	126
% of fulfilment of the total authorised posts (TAs, CAs, SNEs) on 31st of December	77 %	77 %	90 %	94 %

As an Agency, ENISA has historically struggled to meet its human resources needs and take steps to ensure timely and rapid fulfilment of its Establishment Plan. The gap between the available posts and the fulfilment is evidenced in

[10] 3 TA posts and 2 CA posts subject to approval of NIS2 directive; projection on 31.12.2022 depends on successful conclusions of ongoing selections Q3-Q4 2022.

the table above. Historically, this has hampered the Agency to make use of its potential capabilities in the most efficient manner, resulting in a smaller real capacity of the Agency in terms of its human resources.

In order to change this, the Agency embarked on some human resources management novelties such as a large-scale call for expression of interest for temporary agents (TAs) and contract agents (CAs) in 2020, with the aim of creating a sufficiently diverse and broad reserve shortlists of candidates with more transversal competences and skills that could be used to recruit staff and thus fill the gaps in the current establishment plan, as well as serve as a pool of candidates for the establishment plan on a multiannual basis. In 2021 the Agency also embarked in an extensive reorganisation of its human resources management creating a Strategic Workforce Planning framework[11], which prompts the organisation to analyse its human resources needs ahead, on multiannual basis for the Single Programming Document, and to plan and review the allocation and development of human resources between different activities as well as to prepare new recruitment calls well in advance of the enactment of the applicable annual Establishment Plan[12]. Under this framework, the Agency has reviewed and restructured its human resources both in direct operational areas and administrative and corporate areas.

In the course of the 2021 Strategic Workforce Review, the Agency, along with other measures, reallocated altogether 4 posts from EDO and CSS, to be able to meet the threshold foreseen in Article 3(3) of MB/2020/9. This resulted in a termination of 1 contract and the prolongation of 2 contracts was put under review. The posts were allocated to the operational units of Policy Development & Implementation Unit (PDI), Capacity Building Unit (CBU) and Market, Certification and Standardisation Unit (MCS).

In the course of the 2022 Strategic Workforce Review, the Agency, along with other measures, reallocated altogether 3 posts from EDO and CSS, to be able to meet the threshold foreseen in Article 3(3) of MB/2020/9. This resulted in a termination of 2 contracts and a cancellation of one recruitment procedure. The posts are now allocated to the operational units of Policy Development & Implementation Unit (PDI), Capacity Building Unit (CBU) and Operational Cooperation Unit (OCU), to be fulfilled via ongoing recruitment calls.

The original impact that the conclusions of the 2021 and 2022 Strategic Workforce Review were supposed to bring are summarised in the table below.

Table 1b Monitoring of workforce under operational and support units

	Operational units		**Supporting offices and services**	
	Established staff (TAs & CAs)	***Average***	*Established staff (TAs & CAs)*	***Average***
Allocated posts as of 01.01.2021	48	**12**	38	**19**
Allocation as of (01.10. 2021)	67	**16.75**	40	**20**
Allocated posts as of 01.08.2022	71	**17.75**	35,5	**17.75**

[11] Strategic workforce planning also enables the Agency to take corrective actions if and when necessary, to achieve the aims set out in Article 3(3) of the MB decision MB/2020/9, which foresees that the Executive Director will ensure that: “the average number of staff members assigned to the Executive Directors Office (EDO) and Corporate Support Services (CSS) [offices and services supporting the functioning of the Agency] shall not exceed the average number of staff members assigned to units [executing the objectives and tasks of the Agency].”

Current staff in house at 01.08.2022	60	**15**	32,5	**16.25**

Though these exercises aimed at fulfilling and supporting the resourcing of operational activities, the Agency's tight budgetary resources left limited space for manoeuvring and delivering of existing services in corporate and administrative units as due to budget limitations possibilities of externalising service provision could not have been implemented.

2.2. OUTLOOK FOR THE YEARS 2023 – 2025

ENISA shall commit to develop and adopt its 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.

To do so, ENISA has embarked on a revision of its competency framework by defining competencies, technical and behavioural, as well as those next-generation competencies that would enable ENISA to meet its future challenges. This would enable ENISA to make staff development a key area of professional growth, as well as empowering the Agency to adopt frameworks for enhancing career development opportunities. All HR processes will be reviewed and adjusted to reflect modern, competency driven practices and best practices of the market, with the aim to attract, retain and develop highly skilled staff.

In 2022, ENISA has already 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 strategic workforce review decision, 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. 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.

Besides that, in order to 'build an agile workforce' traditional ways of working will continue to be adjusted and the Agency will continue operating in its matrix format. The working environment will need to be reviewed as well so as to accommodate the flexibility that has arrived as a result of the new way of working following COVID, including by enabling staff to telework outside from place of assignment. Agility and flexibility are at the core of ENISA *modus operandi* the last few years and the Agency shall support dynamic ways of working also within the next programming period.

Currently ENISA is still waiting for the final adoption of NIS2 directive where ENISA is tasked with additional action areas. While these action areas are covered by ENISA's general tasks in accordance with its mandate, they would be supported by five supplementary fulltime equivalents (FTEs) (three TAs and two CAs) with a corresponding budget of around EUR 610 000 per year. This is an integrated part of the NIS2 proposal, which is subject to approval and is

currently managed as reserve that the Agency can draw on following the completion of the adoption process. It is expected that NIS2 directive will be adopted in Q4 2022. The indicated posts have been included in the general workforce planning as part of the approved human resources under the EU general budget 2023.

Besides that, a letter of intent between DG CONNECT and ENISA on the provision of support to Member States to further mitigate the risks of largescale cybersecurity incidents in the short term through a new "Emergency Response Fund for Cybersecurity" has been signed in July 2022. This covers the short term phase of the pilot with an amount of 15 million euros provided by DG CONNECT, Here, DG CONNECT provides ENISA with the necessary financial resources that will allow the Agency to reinforce its catalogue of services and enhance the support provided to Member States, it does not grant any additional posts for the implementation of activities under this one off injection. For this initial phase ENISA has capitalised on its expertise and has implemented an innovative cross-unit approach model in order to fulfil its entrusted funds, which is more than double its budget for 2022, while this comes at the expense and on top of already existing defined priorities by all entities. While ENISA on short scale demonstrated the required agility and flexibility to perform, such new tasks, if they become permanent, ENISA should be entrusted with additional resources.

Altogether, the financial resource requirements based on administrative needs and to face upcoming operational challenges are by far exceeding the allocated EU financial envelope. Given the inflationary context, administrative costs for the buildings as well as staff costs, these expenses are expected to dramatically increase over the coming years. This would unfortunately result in reduced available budget for operations. Therefore, ENISA must prioritise and select the most impactful output and suppress or reduce the scope of certain projects to meet these budgetary constraints if no additional resources are allocated to ENISA in the short and/or medium term. The total shortfall that the Agency has identified amounts to over 3 millions euros.

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, it will continue to closely monitor, assess and optimise its structures, services, processes, activities and resource allocation. ENISA faces a constant increase in its workload and while it will still seek for further efficiency gains across the organisation, these gains will only compensate for minor workload increases and temporary absences of staff. However, the MFF 2021-2027 foresees no increase in the agency's establishment plan and thus imposes further constraints for its human resources. 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 2023 – 2025

2.3.1 Financial Resources

In order for the Agency to manage more efficiently its financial and human resources and in order to be able to manage operations extending over a number of budget years while respecting the budget annuality and reducing the administrative workload, will further examine and apply differentiated appropriations in its overall budget management. As this is a standard operating procedure of the Institutions, the Agency in order to manage its upcoming growth and increase its operational efficiency, will make structural efforts towards this direction.

In 2021 the financial structure of the title 3 budget was revised to match the activities of Single Programming Document, in accordance with the CSA. This budget structure aims to implement activity based budgeting and cost based reporting thus allowing ENISA to make budgetary decisions based on specific activity budgetary drivers and their importance to the Agency's activities.

To strengthen budget management, the Agency established the Budget Management Committee (BMC) in 2021 to ensure the coherent planning, implementation and follow-up of the Agency's budget. The mandate of the BMC encompasses the entire lifecycle of the budget, including assisting in setting the overall framework and guiding the development, roll-out and implementation as well as follow-up and analysis of the budget. The committee gives recommendations to the Executive Director (ED) on the execution of the budget including the steps, which should be

taken in order to ensure proper planning and implementation of the annual budget of the Agency, and give feedback on the utilization and budget implementation of the relevant units and managers.

The introduction of the BMC and activity based budgeting have allowed enhanced monitoring of financial planning, leading to a more efficient execution of the budget. Concretely, higher budgetary execution rate and fewer budgetary transfers were expected as a result of this, as evidenced in 2021. The budgetary execution rate in 2021 increased to 99,51% of the budget vs 97,35% in 2020 and there were five internal transfers by ED decision versus seven in 2020 and ten in 2019.

As such and based on lesson learned from 2021 the Agency has extended this efficiency to title 1 and title 2 by merging budget lines of these titles in the proposed 2023 budget structure. By reducing the number of budget lines from 30 to 11 for title 1 and 2, the Agency will be able to reduce the number of ED decisions required to transfer funds between budget lines thus reducing administrative burden and enhance the quality of the monitoring and reporting of the budget. The budget lines consolidated were those budget lines with less 500 kEUR within the same type / category of expenditure in title 1 and 2. This would allow also the agency to apply a more agile and flexible way of managing its funds and services. The consolidated budget lines are reflected in the statement of estimates submitted and adopted along-side the draft SPD 2023-2025.

In light of the current economical / political environment and due to the increase of cybersecurity requirements, the financial resources allocated to ENISA are insufficient to meet these challenges. An annex will be included in the draft single programming document 2024-2026 detailing the assessed impact due to lack of resources on the Agency's planned activities.

The total EU contribution to ENISA over the period from 2023 to 2025, as well as for the full period of the new multiannual financial framework 2021–2027, is planned to remain stable, with a slight annual increase of circa 2% to reflect inflation (see table 2b below).

Table 2

	2022	2023 (*)	2024 (**)	2025 (**)
Total appropriations for ENISA *(thousand EUR)*	24 208	25 183	25 322	25 733

Source:

(*) Draft Union annual budget for the financial year 2023 COM (2022) 400

(**) Fiche no. 68 – MFF 2021-2027 dated 08/06/2020, % of EFTA funds as per COM (2022) 400 and an additional amount of EUR 610 000 has been added subject to the approval of the NIS2 Directive

In 2023 ENISA's revenue is composed of 97.2 % from the EU contribution and 2.8 % was from the European Economic Area (EEA) country contribution (Table 1 in Annex III). In absolute terms, the EU and EEA contribution for 2023 is estimated respectively to reach EUR 24.5 million and EUR 0.7 million.

The general allocation of funds across titles is expected to remain stable over the period 2023-2025. Expenditure in 2023 is expected to amount to EUR 25.2 million, of which EUR 12.7 million in Title 1 covers all staff-related costs (50%), EUR 3.5 million in Title 2 covers main items such as building related expenditure and ICT expenses (14%) and EUR 9.0 million in Title 3 covers all core operating expenditure (36%). Total expenditure include the reserve budget of EUR 610 thousand expected to be allocated to cover additional staff (3 TAs and 2 CAs) to manage part of the activities linked to the NIS2 directive to be adopted in Q4 2022.

2.3.2 Human Resources

In its budget proposal for the Single Programming Document (SPD) 2023-2025, the Agency asks for an extra four SNE posts (introduced gradually 2+2 over 2 years as of 2024). The four additional SNE posts requested would be justified

both by the Agency's current activity areas, particularly the operational needs stemming from Article 7 of the CSA as well as by those extra activities and requirements, as foreseen especially in the initial phases laid out in the Commission's Recommendation on the Joint Cyber Unit (JCU) of 23 June 2021.

Engaging further with SNEs is a cost-effective solution of mutual benefit that on one hands supports the Agency to fulfil its mandate and on the other hand adds the most value for Member States as it strengthens the trust-bond relationship between Member States and ENISA as well as facilitates a smooth knowledge-sharing and service delivery from ENISA to the Member States.

The collective knowledge acquired from the Member State's perspective through such posts will be crucial for the success of these tasks. In fact, by importing unique expertise and knowledge into the Agency through SNE posts rather than having to outsource certain tasks or create any dependencies on other external staff, ENISA is catering for the increasing activities which require close cooperation with Member States as part of its mandate. Higher SNE turnovers will in turn be of direct benefit for all Member States and offer a rich experience to SNEs following their posting.

In 2021 the Agency's request for two additional SNEs for 2022 did not materialise, the Agency therefore has taken the decision to reallocate two SNE posts internally that were earmarked for other operational units and will transfer them to the Operational Cooperation Unit in 2022 specifically for tasks related to Article 7 of the CSA.

This decision to transfer posts from other operational units will have consequences in terms of those units' capacity to carry out their tasks. Therefore, the Agency will need to seek alternative ways to compensate for this decision in order to fulfil its mandate and tasks. Such measures include the re-allocation of further resources from administrative and corporate areas to the operational units and specifically to the Operational Cooperation Unit, inevitably leading to gaps across corporate and administrative functions of the Agency that will need to be covered by externalising these tasks to external service providers. This affect is further compounded by the lower than required graded posts stemming from the NIS2 proposal (3 AD posts) which was authorised by the draft EU general budget for 2022. While acknowledging the budgetary principles, the geopolitical location of ENISA acts as a negative driver in attract high calibre talents, particularly in such a niche market. This brings the agency in reproducing reserve lists of reduced geographical diversity.

Reallocation of posts within ENISA shall be done following the established strategic workforce planning framework. Annual strategic workforce reviews will be conducted through the period 2023-2025 in order to develop and maintain current staff competencies to fulfil the Agency's operational needs and achieve the balance of internal resource allocation between operational and corporate support units. As indicated in Table 1b under Section 2.1 current allocation of posts between operational and corporate support units is balanced. ENISA will thus continue its best efforts to ensure that current staff in house to be reported on 31.12.2022 will also become balanced keeping the same trend throughout the upcoming period 2023-2025. For this, ENISA aims to put emphasis on development of staff competences, including by gradually rolling out multisource feedback tools, which enable staff members to actively address their development areas, expertise and skills in line with the needs of the Agency.

Summary of expected evolution of human resources is outlined below, while detailed data is available in Annex IV.

	2022[13]	2023[14]	2024[15]	2025[16]
Number of posts in the Establishment Plan	82	82	82	82
% of expected fulfilment of the establishment plan on 31st of December	94 %	95 % or higher	95 % or higher	95 % or higher
Total number of authorised posts (TAs, CAs, SNEs) and expected (2024 & 2025)	126	128	130	132
% of expected fulfilment of the total authorised posts (TAs, CAs, SNEs) on 31st of December	94 %	95 %	95 %	95 %

In order to meet the expected targets ENISA within its HR strategy (as part of its overall corporate strategy) will set targets for reserve list establishment of sufficient scope and length. Optimum retention target of <10 % departures during the year is being considered as KPI for the upcoming period 2023-2025.

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

ENISA remains committed to the continuous improvement of its operational and administrative efficiency. It aims to ensure that it 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 strategic workforce review decision, 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.

This 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

[13] Forecast, data will be finalised in November 2022 and 3 TA posts and 2 CA posts subject to approval of NIS2 directive; projection on 31.12.2022 depends on successful conclusions of ongoing selections Q3-Q4 2022.
[14] 3 TA posts and 2 CA posts subject to approval of NIS2 directive
[15] 3 TA posts and 2 CA posts subject to approval of NIS2 directive
[16] 3 TA posts and 2 CA posts subject to approval of NIS2 directive

competencies that are needed in order to meet operational priorities. 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 In 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 should 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 (virtual CISO. concept)

SECTION III. WORK PROGRAMME 2023

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 2023.

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 activity KPIs and associated metrics are expected to transition in due time with metrics stemming from the development of the cybersecurity index, that is currently being piloted. Initial introduction of the cybersecurity index metrics to the activity KPIs are expected in the 2024 work programme. In addition the Agency will take measures to better explain and align the metrics with EU policies and by extension the strategic objectives, activity objectives and individual output objectives.

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. While aspects such as privacy and personal data protection are taken into consideration (incl encryption).

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[17] 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.

OBJECTIVES

- Foster cybersecurity as an integral part of EU policy (existing and new)
- Ensure that EU policy makers are regularly informed about the effectiveness of the existing frameworks and EU policy makers and stakeholders are provided with timely and tailor-made policy recommendations on future cybersecurity challenges and opportunities

RESULTS	LINK TO STRATEGIC OBJECTIVE (ENISA STRATEGY)
Cybersecurity aspects are considered and embedded across EU and national policies	Cybersecurity as an integral part of EU policies

OUTPUTS	VALIDATION
1.1 Assist and advise the EC and Member States in reviewing the effectiveness of current cybersecurity policy frameworks 1.2 Assist and advise the EC and MS on new policy development, as well as carrying out preparatory work 1.3 Support policy monitoring of existing and emerging policy areas and maintain a catalogue of all relevant cybersecurity legislations and policies at the EU level	• NIS Cooperation Group (NIS CG) and other formally established Groups (outputs 1.1, 1.2 and 1.3) • ENISA ad hoc working groups[18] (outputs 1.1 and,1.2 1.3) • National Liaison Officers Network, ENISA Advisory Group and other formally established expert group (when necessary)

STAKEHOLDERS AND ENGAGEMENT LEVELS[19]

Partners: DG Connect, NIS Cooperation Group, National Competent Authorities, other formally established groups, European Commission Directorate General's and Agencies - depending on policy area (e.g. DG GROW, European Insurance and Occupational Pensions Authority)

Involve / Engage: ENISA National Liaison Officers, operators of essential services, digital service providers and industry associations/representatives.

[17] 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
[18] in accordance with Art 20(4) of CSA
[19] Stakeholders and engagement levels stem from the implementation of the ENISA stakeholder strategy

Key performance indicators: ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (*ex ante*)	**Unit of measure-ment**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
1.1. Number of relevant contributions to EU and national policies and legislative initiatives	Number	Annual	Manual collection from staff members	193	215
1.2. Number of references to ENISA reports, analysis and/or studies in EU policy documents		Biennial	Survey[20]	N/A	Baseline to be established in 2023
1.3. Satisfaction with ENISA's added value of contributions		Biennial	Survey	N/A	Baseline to be established in 2023
1.4. Number of EU policy files under development and supported by ENISA	Number	Annual	Report	N/A	Baseline to be established in 2023

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	246.712	0,00	11.387	0,10	0	1,55	258.099
Output 1.2	NIS, CERTI	1,30	28.086	0,60	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: 330.262								

[20] Biennial surveys for each activity will be conducted in Q1 2023 for reference year 2022. Results will be recorded in annual activity report 2022 and single programming document 2024-2026

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[21] 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 register for operators of digital infrastructure.

It further includes horizontal outputs, which address sector-agnostic cross-cutting issues[22], 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 and wallets (eID), 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.

OBJECTIVES

- Consistent development of sectorial Union policies with horizontal Union policy to avoid implementation inconsistencies
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in Member States
- Effective implementation of cybersecurity policy across the Union and consistency between sectorial and horizontal cybersecurity policies.
- Improved cybersecurity practices taking on board lesson learned from incident reports

RESULTS	Link to strategic objective (ENISA STRATEGY)
• 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	• Cybersecurity as an integral part of EU policies • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	VALIDATION
2.1 Support the activities of the NIS Cooperation Group including its work programme 2.2 Support Member States and the EC in the implementation of horizontal aspects of the NIS directive 2.3 Support Member States and EC with security and resilience of the NIS sectors via targeted service package identified in the ENISA NIS strategy 2.4 Provide advice, Issue technical guidelines and facilitate exchange of good practices to support Member States and EC on the implementation of cybersecurity aspects of transversal EU policies[23]	NIS Cooperation Group and or established work streams (Outputs 2.1, 2.2, 2.3) Telecoms working group (ECASEC) and trust services working group (Outputs 2.3, 2.4) eID Cooperation network, ENISA Ad Hoc Working Group on data protection engineering (Output 2.4) ENISA National Liaison Officers' Network (as necessary)

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: National cybersecurity agencies and national authorities for cybersecurity in the EU Member States (NIS CG plenary and work streams), National Regulatory Authorities (ECASEC), National Supervisory bodies (ECATS), Conformity Assessment Bodies (CABs), and informal groups of authorities (e.g. FESA, informal working group of financial authorities), EC, EU Institutions/ bodies (e.g. Body of European Regulators for Electronic Communications (BEREC), European Data Protection Supervisor (EDPS), European Data Protection Board (EDPB), European Railway Agency

[21] 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.

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

[23] Including DORA, Electricity Code, privacy and eIDAS

(ERA), European Maritime Safety Agency (EMSA), other sectorial EU Agencies (e.g. ACER, EASA, ESA, ECB, EBA) and institutional industry bodies (e.g. ICANN, RIPE-NCC, ENTSO-E, ENTSO-G, EU.DSO entity)

Involve / Engage: ENISA National Liaison Officers, operators of essential services, digital service providers, trust service providers, data protection authorities, Information Sharing and Analysis Centres (ISACs), research and academia, and industry associations/representatives.

Key performance indicators: Contribution to policy implementation and implementation monitoring at EU and national levels (*ex post*)	**Unit of measure-ment**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
2.1. Number of EU policies and regulations implemented at national level supported by ENISA	Number	Annual	Manual collection from staff members	5	5
2.2. Number of ENISA reports, analyses and/or studies referred at EU and NIS CG documents (survey)		Biennial	Survey	N/A	Baseline to be established in 2023
2.3. Satisfaction with ENISA added-value of support (survey)		Biennial	Survey	N/A	Baseline to be established in 2023
2.4. Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)		Annual	Internal analysis (NIS sector 360)	N/A	Baseline to be established in 2023

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	6,2	336.846	0	-	0,25	-	6,45	336.846
Output 2.2	SITAW, NIS, CERTI, TREX	4,45	422402	0		0,3	-	4,75	422.402
Output 2.3	SITAW, NIS, CERTI	-	-	3	214.155	0,3		3,3	214.155
Activity total	FTE: 14.5 Budget: 973.404								

Activity 3 Building capacity

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[24]

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.

OBJECTIVES

- Increase the level of preparedness, capabilities and cooperation within and between Member States and sectors and EU institutions, bodies and agencies
- Prepare and test capabilities to respond to cybersecurity incidents
- Foster interoperable, consistent European risk management, methodologies and risk assessment practices
- Increase skill sets and align cybersecurity competencies
-

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Enhanced capabilities across the community • Increased cooperation between communities	• Cutting-edge competences and capabilities in cybersecurity across the Union • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	VALIDATION
3.1 Assist MS to develop, implement and assess National Cybersecurity Strategies 3.2 Organise large scale biennial exercises and sectorial exercises[25] 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) and work streams, information sharing and analysis centers (ISACs)and other communities 3.4 ~~Develop coordinated and interoperable risk management frameworks~~[26] 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[27] 3.6 Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)[28]	NLO Network (as necessary) CSIRTs Network, (output 3.3.) CyCLONe members (as necessary) NIS Cooperation Group (output 3.2 and 3.3) EU ISACs (output 3.3) Ad-hoc WG on SOCs (output 3.5)

STAKEHOLDERS AND ENGAGEMENT LEVELS

Involve / Engage: Cybersecurity professionals, Private industry sectors (operators of essential services such as health, transport etc.), EU Institutions and bodies, CSIRTs Network and related operational communities, European ISACs, CyCLONe members, NISD Cooperation Group,ISACs Blueprint stakeholders

[24] CSIRT trainings and Capture the Flag (CTF) and Attach Defence (AD) competitions.
[25] (including Cyber Europe, Blueprint operational level exercise (BlueOLEx), Cyber Exercise to test SOPs (CyberSOPEx etc) and through cyber ranges. NIS cooperation group exercise postponed due to resource constraints
[26] Proposed output is supressed in 2023 work programme due to insufficient resources. I
[27] would be priority output for the consideration for consuming any surplus budget in 2023
[28] In the context of this output ENISA is also preparing a few Service Levels Agreements with key EU Agencies with advanced capacity building activities requirements (e.g. eu LISA).

Key performance indicators: Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents	Unit (of measurement)	Frequency	Data source	Results 2021	Target 2023
3.1. Increase/decrease in maturity indicators					
Maturity of national cybersecurity strategies					
Number of Member States that rate the overall maturity of their cybersecurity strategy					
High maturity	Number	Annual	Survey	3	5
Medium maturity	Number	Annual	Survey	4	5
Low maturity	Number	Annual	Survey	3	2
Number of Member States planning to use ENISA framework to measure the maturity of their national cybersecurity capabilities					
Already using	Number	Annual	Survey	1	3
Not using but planning to use	Number	Annual	Survey	5	7
Don't know or will not use in the foreseeable future	Number	Annual	Survey	4	4
Number of Member States that have set KPIs to measure progress and effectiveness of the implementation of their strategic objectives when drafting their NCSSs					
Already using	Number	Annual	Survey	3	5
Not set but planning to use	Number	Annual	Survey	4	5
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	3	3
The frequency with which Member States update their strategies to adapt to technological advancements and new threats					
Every 2–3 years	Number	Annual	Survey	2	3
Every 4–5 years	Number	Annual	Survey	6	8
More than 6 years or don't know	Number	Annual	Survey	2	2
Total maturity of ISACs (self-assessment)	%	Annual	Report	63 %	65%
3.2. Outreach, uptake and application of lessons learned from capability-building activities					
CySOPEx 2021 (number of improvements proposed by participants)	Number	Per exercise	Report	5	3[29]
3.4 The number of exercises executed annually	Number	Annual	Report	5[30]	5

[29] Average number of improvements across all exercises
[30] Relates to 2022 exercises executed as of October 2022

3.5 Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey)					
Usefulness low	%	Average of capacity building activities	Survey	9%	Maximum 5%
Usefulness medium	%	Average of capacity building activities	Survey	71%	25% to 50%
Usefulness high	%	Average of capacity building activities	Survey	20%	Minimum 45%
Relevance low	%	Average of capacity building activities	Survey	4%	Maximum 5%
Relevance medium	%	Average of capacity building activities	Survey	53%	25% to 50%
Relevance high	%	Average of capacity building activities	Survey	43%	Minimum 45%
3.5 ISACs maturity					
Number of Exercises organised by EU ISACs	%[31]	Over 2 years	Report	N/A	Minimum 30%
Number of Trainings organised by EU ISACs	%	Over 2 years	Report	N/A	Minimum 30%

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 3.1	TREX, INDEX	2,00	108.919	0,00	0	0,00	0	2,00	108.919
Output 3.2	TREX, NIS	4,25	584.153	0,00	0	0,00	0	3,75	584.153
Output 3.3	TREX	4,00	635.580	0,00	0	0,00	0	4,00	635.580

[31] the % out of a total of 10 EU ISACs (as per NIS and NIS2)

Output 3.4[32]									-
Output 3.5	TREX	0,50	28.544	0,00	0	0,00	0	0,50	28.544
Output 3.6	TREX	3,00	352.043	0,00	0	0,00	0	3,00	352.043
Activity total	FTE: 13,75 - Budget: 1.709.239								

Activity 4 Enabling operational cooperation

OVERVIEW OF ACTIVITY

[32] Propose output to be suppressed in 2023 given resource constraints

The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities in-particular through its local office in Brussels, Belgium. Actions include establishing 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 with the view to exchange know how, best practices, provide advice and issue guidance.

In addition, inline with NIS2 requirements ENISA will continue to support Member States in the CSIRTs Network in respect to operational cooperation. Moreover with the formal establishement of the EU CyCLONe (Cyber Crisis Liason Organization Network) in NISD2 ENISA will support cyber crisis coordination by advising and assisting both 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[33]. Furthemore, in the view of the implementation of NIS 2 Directive the activity supports Coordinated Vulnerability Disclosure efforts by designated CSIRTs in the CSIRTs Network and the implementation of a European vulnerability database.

In view of the EC Recommendation 4520 (2021) and Council Conclusions of the 20 October 2021 (ST 13048 2021) on 'exploring the potential of the Joint Cyber Unit initiative - complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises', ENISA will engage in exploring the potential of the JCU, along the lines and the roles defined according to on-going discussions amongst MS and relevant EU institutions, bodies and agencies. In addition, this activity implements the ENISA Cybersecurity Support Action[34].

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

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

OBJECTIVES

- Enhance and improve incident response capabilities across the Union
- Enable effective European cybersecurity crisis management by continuously improving the cyber crisis management framework
- Ensure coordination in cybersecurity crisis management among relevant EU institutions, bodies and agencies (e.g. CERT-EU, European External Action Service (EEAS), European Union Agency for Law Enforcement Cooperation (EUROPOL)
- Improve maturity and capacities of operational communities (CSIRTs Network, EU CyCLONe)
- Contribute to preparedness, shared situational awareness and coordinated response and recovery to large scale cyber incidents and crises across different communities (e.g. by providing Ex-ante services).

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• All communities (EU Institutions and MS) use a streamlined and coherent set of SOPs for cyber crises management • Efficient tools (secure & high availability) and methodologies for effective cyber crisis management	• Effective cooperation amongst operational actors within the Union in case of massive cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem
OUTPUTS	**VALIDATION**
4.1. Support the functioning and operations of the operational networks and communities and cooperation with relevant stakeholders including blueprint actors[35]. 4.2. Support coordinated vulnerability disclosure efforts by designing and deploying the EU Vulnerability Database. 4.3. Deploy , maintain and promote operational cooperation platforms and tools including preparations for a secure virtual platform for CyCLONe	4.1. NLO Network (as necessary) 4.2. CSIRTs Network and EU CyCLONe 4.3. Blueprint actors

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: Blueprint actors, EU decision makers, institutions, agencies and bodies, CSIRTs Network Members, EU CyCLONe Members, SOCs.

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

[33] This is especially relevant for the year 2023 and onwards because the support contract procured by the Commission finishes by the end of 2022.
[34] the Agency will prepare where possible for the future Emergency Response Fund, providing that ENISA will be asked to support it and without pre-empting the outcome of the legislative process.
[35] CSIRTs Network, CyCLONe, SOCs network, potentially JCU

Key performance indicators: Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation	Unit (of measurement)	Frequency	Data source	Results 2021	Target 2023
4.1 Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA					
CSIRT Network					
Active users increase from 2020	%	Annual	Platform	115 %	110%
Number of exchanges/interactions increase from 2020	%	Annual	Platform	291 %	100%
EU CyCLONe					
Active users increase from 2020	%	Annual	Platform	143 %	100%
Number of exchanges/interactions increase from 2020	%	Annual	Platform	1 011 %	150%*
4.2 Uptake of platforms/tools/SOPs during massive cyber incidents[36]		Ad hoc		N/A	
4.3 Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs including EU vulnerability database	N/A	Biennial	Survey	N/A	Baseline to be established in 2023

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	4,00	44.567	3,70	412.895	0,35	0	8,35	457.462
Output 4.2	NIS, SITAW	1,00	72.978	1,00	69.743	0,20	0	2,20	142.720
Output 4.3	SITAW, NIS	3,00	636.908	3,00	885.440	0,00	0	6,00	1.522.348
Activity total	FTE: 16,55 - Budget: 2.122.530								

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

OVERVIEW OF ACTIVITY

[36]Massive is defined as large scale cross border incidents and crises that require the highest escalation mode of the EU CSIRTs Network and/or EU CyCLONe.

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, 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 facilitation of 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 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 mutual assistance and the situational awareness in the framework of the proposed potential JCU. In addition, this activity implements the ENISA Cybersecurity Support Action[37].

Moreover the activity persues to further foster and optimise the structured cooperation with CERT-EU (please see Annex XIII Annual Cooperation Plan 2023).

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

OBJECTIVES

- Enhanced preparedness and effective incident response and cooperation amongst Member States and EU institutions, including cooperation of technical, operational and political actors during incidents or crisis
- Common situational awareness before and during cyber incidents and crisis across the Union
- Information exchange and cooperation, cross layer and cross border between Member States and as well as with EU institutions

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Member States and institutions cooperating effectively during large scale cross border incidents or crises • Stakeholders and public aware of current cybersecurity development	• Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	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[38] 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 5.3. Maintain, develop and promote the trusted network of vendors/suppliers for information exchange and situational awareness	• Blueprint actors

TARGET GROUPS AND BENEFICIARIES

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

Key performance indicators: ENISA ability and preparedness to support response to massive cyber incidents	Unit (of measure-ment)	Frequency	Data source	Results 2021	Target 2023

[37] the Agency will prepare where possible for the future Emergency Response Fund, providing that ENISA will be asked to support it and without pre-empting the outcome of the legislative process.
[38] Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1

5.1 Number of relevant incident responses ENISA contributed to as per CSA Art.7	Number	Annual	Report	775[39]	TBD
Number of incidents analysed/curated			OSINT report	775	
Number of high visibility incidents analysed			Flash report	38	
Number of large-scale cross-border incident with high impact analysed			Joint Rapid Report[40]	13	
Number of incident to which ENISA contributed to respond			Cyber Assistance Mechanism	1	
5.2 Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents that ENISA contributes to mitigation efforts	N/A	Biennial	Survey	N/A	Baseline to be established in 2023
5.3 Take up of ENISA support services	Number	Annual	Report	N/A	Baseline to be established in 2023
5.4 Number of trusted vendors	Number	Annual	Report	N/A	Baseline to be established in 2023
5.5 Stakeholder satisfaction with ENISA's ability to provide operational support	N/A	Biennial	Survey	N/A	Baseline to be established in 2023

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 5.1	SITAW, INDEX	7,40	764.432	0,00	0	0,00	0	7,40	764.432
Output 5.2	SITAW			1,4	97.701	0,00	0	1,40	97.701
Output 5.3	SITAW	0,25	51.379	0,95	0	0,00	0	1,20	51.379
Activity total	FTE: 10 - Budget: 913.512								

Activity 6 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

[39] As of October 2022 for year 2022
[40] structured cooperation with CERT-EU.

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.

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.

OBJECTIVES

- Trusted ICT products, services and processes
- Increase use and uptake of European cybersecurity certification
- Efficient and effective implementation of the European cybersecurity certification framework
-
- Improve the security posture management of certified products, services and processes by applying continuous compliance monitoring for assurance level high

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Certified ICT products, services and processes are preferred by consumers and businesses	• High level of trust in secure digital solutions • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	VALIDATION
6.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes 6.2. Implementing and maintaining of the established schemes including evaluation of adopted schemes, participation in peer reviews etc. 6.3. Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks 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.)	• Ad hoc working groups on certification (output 6.1 and 6.2.) • ECCG (6.1.6.2, 6.3 and 6.4) • European Commission (outputs 6.1, 6.2.-6.3, 6.4) • SCCG (output 6.3. and 6.4.)

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

Key performance indicators: 1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions 2. Effective preparation of candidate certification schemes prepared by ENISA	**Unit (of measurement)**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
6.1. Number of stakeholders (public authorities and/or commercial solution providers) in the EU market using the cybersecurity certification framework for their digital solutions (average of responses)	%	Annual	Survey	44 %	50%
6.2 Stakeholders level of trust in digital solutions of certification schemes (citizens, public sector and businesses).		Biennial	Survey	N/A	Baseline to be established in 2023

6.3 Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework		Biennial	Survey	N/A	Baseline to be established in 2023
6.4 Number of candidate certification schemes prepared by ENISA[41]	Number	Annual	Report	N/A	Minimum 75% of schemes formally requested to be under ongoing development
6.5 Number of people/organizations engaged in the preparation of certification schemes[42]	Number	Annual	Report	N/A	Minimum: 10 organisations; 10 individual experts; 50% of EU MS joining an AHWG; 30% of organisations to be an SME; 5% to be from a third country
6.6 Satisfaction with ENISA's support for the preparation of candidate schemes		Biennial	Survey	N/A	Baseline to be established in 2023

Resource forecast									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 6.1	CERTI, NIS	4,65	565.936	0,70	945	0,00	0	5,35	566.881
Output 6.2	CERTI	1,35	90.720	0,00	-	0,00	0	1,35	90.720
Output 6.3	CERTI	1,05		0,00		0,00	0	1,05	-
Output 6.4	CERTI	1,10	75.859	0,15	71.118	0,00	0	1,25	146.977
Activity total	FTE: 9 - Budget: 804.578								

Activity 7 Supporting European cybersecurity market and industry

[41] Number of schemes formally requested by the Commission or given the go ahead on the basis of the Union Rolling Work Program, and the number of cybersecurity certification schemes under development by ENISA
[42] Numerical value from ENISA records; on a per scheme basis to produce number of: organisations, individual experts, EU Member States, percentage of SMEs, percentage of third country organisations involved that support the promulgation of a cybersecurity certification scheme.

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. 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.

OBJECTIVES
• Improve the conditions for the functioning of the internal market • Foster a robust European cybersecurity industry and market

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Contributing towards understanding cybersecurity market dynamics. • A more competitive European cybersecurity industry, SMEs and start-ups	• High level of trust in secure digital solutions • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	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 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 7.3. Guidelines and good practices on cybersecurity for ICT products, services and processes and recommendations to the EC and the ECCC 7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services	• SCCG (outputs 7.2. & 7.3.) • ENISA Advisory Group (output 7.1.) • NLO (as necessary) • ECCG (7.4) • Ad hoc working groups cybersecurity market analysis (O.7.1)

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

Key performance indicators: Effectiveness of ENISAs supporting role for participants in the European cybersecurity market	Unit (of measurement)	Frequency	Data source	Results 2021	Target 2023
7.1. Number of market analyses, guidelines and good practices issued by ENISA					
Cybersecurity market analysis framework	Number	Annual	Reports	2	1
7.2. Uptake of lessons learned / recommendations from ENISA reports (average of responses)	%	Annual	Survey	49%	60%

7.3. Stakeholder satisfaction with the added value and quality of ENISA's work	%	Biennial	Survey	N/A	Baseline to be established in 2023

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	2,90	116.161	0,35	0	0,00	0	3,25	116.161
Output 7.2	CERTI, NIS	1,60	112.132	0,20	0	0,00	0	1,80	112.132
Output 7.3	CERTI	0,50	73.017	0,00	0	0,00	0	0,50	73.017
Output 7.4	CERTI	0,50	54.716	0,00	0	0,00	0	0,50	54.716
Activity total	FTE: 6 - Budget: 356.027								

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 and advice on emerging and future technologies, based on the results of regular cybersecurity foresight exercises. Typical examples may include artificial intelligence, quantum computing, space technology, etc

Moreover, on the basis of risk management principles, and consolidation of information and knowledge the Agency will identify cyber threats, vulnerabilities and risks, and map threat landscapes and provides topic-specific as well as general assessments on the expected societal, legal, economic and regulatory impact, as well as targeted recommendations to Member States and Union institutions, bodies, offices and agencies. In doing so, the Agency will take into account work on incident reporting as per relevant EU legislations. In this respect, the Agency will continue analysing and reporting on incidents as required by Art 5(6) of CSA and will upon request support incident reporting and analysis in other legislative acts such as Art. 10 of eIDAS Regulation, DORA, etc.

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. 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.

OBJECTIVES

- Identify and understand emerging and future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase Member States' and Union's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities
- Greater insight of the current state of cybersecurity across the Union
-

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Decisions about cybersecurity are future proof and take account of the trends, developments and knowledge across the ecosystem • • MS have the tools for assessing and understanding their cybersecurity maturity	• Foresight on emerging and future cybersecurity challenges • Efficient and effective cybersecurity information and knowledge management for Europe • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	VALIDATION
8.1 Develop and maintain EU cybersecurity index 8.2 Collect and analyse information to report on the cyber threat landscapes 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.) 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 8.5 Foresight on emerging and future cybersecurity challenges and recommendations. 8.6 ~~Building and exchanging knowledge on ransomware threat (incl. capacity building and awareness raising and education)~~[43]	• NLO Network (for Output 8.4 and 8.5, as well as necessary for other Outputs) • ENISA Advisory Group (as necessary) • ENISA ad hoc working groups (for Outputs 8.1, 8.2, 8.4 and 8.6 as necessary • CSIRT Network (output 8.1 and 8.2) • Formally established bodies and expert groups as necessary (output 8.3) • NIS Directive Cooperation Group (output 8.1)

STAKEHOLDERS AND ENGAGEMENT LEVELS

[43] It is proposed that this output be supressed during 2023 work programme due to insufficient resources

Partners: EU and national decision making bodies and authorities , ECASEC and Art. 19 Expert Group members

Involve / Engage: Industry, research and academic institutions and bodies

Key performance indicators: ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including foresight on emerging and future challenges	**Unit (of measurement)**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
8.1. Number of users and frequency of use of a dedicated portal (observatory)	N/A[44]				
8.2. Number of recommendations, analyses and challenges identified and analysed (reports)	Number	Annual	ENISA reports and studies	288	300
8.3 Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in threat landscapes		Biennial	Survey	N/A	
8.4 The influence of foresight on the development of ENISA work programme	Number	Annual	SPD	N/A	Applicable as of 2023
8.5 Uptake of reports generated in activity 8	Number	Annual	Media monitoring report	N/A	Applicable as of 2023
8.6 Uptake of the cybersecurity index	Number	Annual	Index platform	N/A	Applicable as of 2023

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	0,00		0,00		2,50	181.982
Output 8.2	INDEX, SITAW, NIS	2,00	156.616	0,35		0,25	15.000	2,60	171.616
Output 8.3	INDEX, SITAW, NIS	1,00	58.791	0,20		0,00	-	1,20	58.791

[44] InfoHub is in the process of being developed

Output 8.4	INDEX, TREX	1,00	152.235	0,00		0,00	-	1,00	152.235
Output 8.5	INDEX	1,10	207.257			0,10	40.000	1,20	247.257
~~Output 8.6~~[45]									
Activity total	FTE: 8,50 - Budget: 811.881								

[45] Proposed that output is suppressed in 2023 due to insufficient resources

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.

OBJECTIVES

- Advance cyber-secure behaviour by essential service providers in critical sectors
- Elevate the understanding of cybersecurity risks and practices across the EU and globally
- Foster EU cybersecurity values and priorities
- Increase the supply of skilled professionals to meet market demand, and promote cybersecurity education

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience	• Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	VALIDATION
9.1 Develop activities to enhance behavioural change by essential service providers in critical sectors (as defined by the NISD) 9.2 Promote cybersecurity topics, education and good practices in the basis of the ENISA stakeholders' strategy 9.3 Implement ENISA international strategy and outreach 9.4 Organise European cybersecurity month (ECSM) and related activities 9.5 Report on cybersecurity skills needs and gaps, and support skills development, maintenance and implementation (incl. Digital Education Action Plan and a report on higher-education programmes) 9.6: Implement the Cybersecurity in Education roadmap[46]	• Management Board (as necessary) • SCCG (for certification related issues under output 9.2) • NLO Network (as necessary) • ENISA Advisory Group (outputs 9.1. and 9.2) • AHWG on cybersecurity skills (output 9.5)

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, European Cybersecurity Competence Center, International partner (CISA, NIST etc)

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

Key performance indicators: Level of awareness of cybersecurity, cyberhygiene and cyberliteracy across the EU Level of outreach	**Unit (of measurement)**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
9.1 Number of cybersecurity incidents reported having human error as a root cause	Number	Annual	Report	N/A	Baseline to be established in 2023
9.2 Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics					
Social media impressions	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	20.756.630	20.000.000
Social media engagement	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	117.720	150.000
Video views	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	2.021.129	3.000.000
Website visits	Average number	Annual	ENISA website	123.504	150.000
Participation in events	Average number	Annual	Media monitoring	5	10
References	Average number	Annual	Website announcements	40	50
9.3 Number of cybersecurity programmes (courses) and participation rates ([a])					
Total number of students enrolled in the first year of the academic programmes (2020)	Number	Annual	Report47	4 843	6000
Number of male students	%	Annual	Report	80 %	70 %
Number of female students	%	Annual	Report	20 %	30 %
Total number of cybersecurity programmes (2020)	Number	Annual	Report	119	130
Number of postgraduate programmes	%	Annual	Report	6 %	5%
Number of master's programmes	%	Annual	Report	77 %	80 %
Number of bachelor's programmes	%	Annual	Report	17 %	15 %
9.4 Geographical and community coverage of outreach in the EU	Number	Annual			Baseline to be established in 2023

[47] https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

9.5 Level of awareness of cybersecurity across the EU / general public (e.g. EU barometer)		Biennial		N/A	Baseline to be established in 2023

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[48]	NIS	1,00	66.482	0,50	43.688	0,00	0,00	1,50	110.170
Output 9.2	INDEX, CERTI	0,75	42.701	0,75	31.314	0,00	0,00	1,50	74.014
Output 9.3	SITAW, TREX	0,75	-	0,75	26.544	0,00	0,00	1,50	26.544
Output 9.4	TREX	0,10	-	0,90	95.147	0,00	0,00	1,00	95.147
Output 9.5*	INDEX, TREX	0,40	47.441	0,60	59.775	0,00	0,00	1,00	107.216
Output 9.6	INDEX	0,20	38.059	0,80	38.059	0,00	0,00	1,00	76.117
Activity total	FTE: 7,50 - Budget: 489.209								

*[48] Outputs 9.1 and 9.5 would be priority outputs for the consideration of consuming any surplus budget in 2023

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.

OBJECTIVES

- Advance the response to current and emerging cyber risks and threats with the use of effective risk prevention technologies.
- Ensure that the EU strategic research and innovation agenda in cybersecurity is aligned with the needs and priorities of the community.
- Reduce dependence on cybersecurity products and services from outside the Union and to reinforce supply chains within the Union.

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• 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.	• Foresight on emerging and future cybersecurity challenges • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	VALIDATION
10.1 Consolidated cybersecurity research and innovation roadmap across the EU. 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). 10.3 Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment.	The European Cybersecurity Competence Centre and Network of National Coordination Centres and Competence Centre Governing Board (output 10.2 & 10.3) NLO as necessary

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners: Member States (including the National Coordination Centres), EU-IBAs (Including the EC, ECCC and JRC);

Involve / Engage: Market actors - in particular the NIS sectors' stakeholders (e.g. OES); academia and research communities, cybersecurity industry as well as solution and service providers.

Key performance indicators: Contributing to Europe's Strategic Research and Innovation Agenda in the field of cybersecurity.	**Unit (of measurement)**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
10.1 Number of requests from the EU-IBAs (including the ECCC) and MS to contribute, provide advice or participate in activities.	Number	Annual	Report	N/A	Baseline to be established in 2023
10.2 Number of references to ENISA advice and recommendations in the EU Strategic Research and Innovation Agenda including Annual and Multiannual Work programmes.	Number	Annual	Report	N/A	Baseline to be established in 2023
10.3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's advice on cybersecurity research needs and funding priorities (Survey)		Biennial	Survey	N/A	Baseline to be established in 2023

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	0.10	0	0.90	123.453	0,00	0	1	123.453
Output 10.3				1.8	25.490	0,20	5.000	2	30.490
Activity total	FTE: 4 - Budget: 195.371								

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 building of internal capacity for contribution, 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 continue 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

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.

OBJECTIVES

- Increased effectiveness and efficiency in achieving Agency objectives
- Compliant with legal and financial frameworks in the performance of the Agency (build a culture of compliance)
- Protect the Agency's assets and reputation, while reducing risks
- Full climate neutrality of all operations by 2030

RESULTS	**Link to corporate objective:**
Maximize quality and value provided to stakeholders and citizens Building lasting credibility and trust	Sound resource and risk management

OUTPUTS	**VALIDATION**
11.1 Maintain performance management framework including through single administrative practices across the Agency 11.2 Develop and implement annual communications strategy 11.3 Develop and implement risk management plans including IT systems cybersecurity risk assessment, including focus on quality management framework and business processes as well as relevant policies 11.4 Maintain and monitor the implementation of Agency wide IT management processes and develop budgetary management processes 11.5 Manage and provide secretariat for statutory bodies(EB,MB,NLO,AG) 11.6 Obtain and maintain the EU Eco-Management and Audit Scheme (EMAS) certificate through continuous overview of CO2 impact of all	• Management Team • Chairs of statutory bodies (Output 10.5) • Budget Management Committee • IT Management Committee • Intellectual Property Rights Management Committee • Staff Committee ENISA Ethics Committee

operations of the Agency in line with applicable legal framework and publish environment statement	

STAKEHOLDER AND ENGAGEMENT LEVELS

Partners: Members of statutory bodies such as Management Board, Advisory Group and National Liaison Officers

Involve / Engage: All ENISA stakeholders

Key performance indicators: Organisational performance culture Trust in ENISA brand	**Unit (of measure-ment)**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
11.1. Proportion of key performance indicators reaching targets	%	Annual	Report	N/A[49]	65%
11.2. Individual staff contribution to achieving the objectives of the agency via clear link to KPI's in staff career development report (CDR report) (all units aggregated)	%	annual	Objectives 2021	60%	85%
11.3. Exceptions in the risk register	Number	Annual	Internal control	16	11
Deviation from financial regulations	Number	Annual	Internal control	14	10
Deviation from staff regulations	Number	Annual	Internal control	2	1
11.4. Number of complaints filed against ENISA, including number of inquiries/complaints submitted to the European Ombudsman	Number	Annual	Report	19	12
11.5 Number of complaints addressed timely and according to relevant procedures	Number	Annual	Internal control files	N/A	Baseline to be established in 2023
11.6 Number of high risks identified in annual risk assessment exercise	Number	Annual	Internal control files	N/A	Baseline to be established in 2023
11.7 Implementation of risk treatment plans	Number	Annual	Report	N/A	Baseline to be established in 2023
11.8 Number & types of activities at each engagement level[50]	Number	Annual	Report	N/A	Baseline to be

[49] Baselines were available as of 2021 annual activity report therefore proportion of metrics reaching targets will be assessed in the 2022 annual activity report
[50] Relates to the stakeholder strategy and its implementation, refers to activities such as conferences, workshops etc

					established in 2023
11.9. 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 number of observations successfully completed and closed	Number	Annual	Report	4	2
11.10 Level of trust in ENISA		Biennial	Survey	N/A	Baseline to be established in 2023

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	1		5.5	160.850		
Output 11.2	All service packages	2		2	304.000		
Output 11.3	All service packages	0.5		3	197,000		
Output 11.4				1.5	0		
Output 11.5				2	126.500		
Output 11.6				0.5	61.500		
Total	FTEs 18 Budget 849,000						

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 imeplementing 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 frameworks. It will also explore cloud-enabled services that are fit for purpose and provide services in accordance with recognised standards. 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.

OBJECTIVES

- Engaged staff, committed and motivated to deliver, empowered to use fully their talent, skills and competences
- Consistent and regular review of the Agency's resources, to seek appropriate match with the organisation's needs, along with obtaining internal and external efficiency gains across the organisation
- Digitally enabled work-place environment (including home work-space) which promotes performance and balances social and environmental responsibility
- Enable operations at the highest level of security
- Build a culture of continuous improvement, agility, customer centred and can-do attitude

RESULTS	Link to corporate objective:
ENISA as an employer of choice and enabling growth and excellence in a secure environment	Build an agile organisation focused on people

OUTPUTS	VALIDATION
12.1 Manage and provide recurrent, quality support services in the area of resources, security[51] and infrastructure for ENISA staff, employees, corporate partners and visitors 12.2 Develop and implement Agency's corporate strategy (including HR strategy) with emphasis on talent development and growth, innovation and inclusiveness; 12.3 Enhance operational excellence and digitalisation through modern, secure and streamlined ways of working and self-service functionalities 12.4 Provide a secure, safe, modern and welcoming place to work (and telework) including staff welfare 12.5 Set up service provisions standards and service optimisation processes.	• Management Board (Output 12.2) • Management Team • IT Management Committee • Budget Management Committee • Staff Committee

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

STAKEHOLDERS AND ENGAGEMENT LEVELS
Partner: ENISA staff members and EU Institutions, Bodies and Agencies **Involve / Engage**: Private Sector and International Organisations

Key performance indicators: Staff commitment, motivation and satisfaction	**Unit (of measurement)**	**Frequency**	**Data source**	**Results 2021**	**Target 2023**
12.1 . Staff satisfaction survey (including the attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools)	%	Annual	Staff satisfaction survey	72%	75%
12.2-. Quality of ENISA training and career development activities organised for staff	%	Annual	Staff satisfaction survey	49%	55%
12.3. Reasons for staff departure (exit interviews)[52]	**Scale 1–10**	**As required**	**HR files**	**7.1**	**7.5**
12.4 Turnover rates	%	Annual	HR files	3 %	3%
12.5 Establishment plan posts filled	%	Annual	HR files	91%	95%
12. 6. Resilience and quality of ENISA IT systems and services	%	Annual	IT reports and staff satisfaction survey	78%	80%
12.7 Percentage of procurement procedures launched via e-tool (PPMT)	%	Annual	Procurement files		> 80 %
12.8 Percentage of payments made within 30 days	%	Annual	Finance files		> 90%
12.9 Late Payments	%	Annual	Finance files		<10%

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				9	2 138 000		

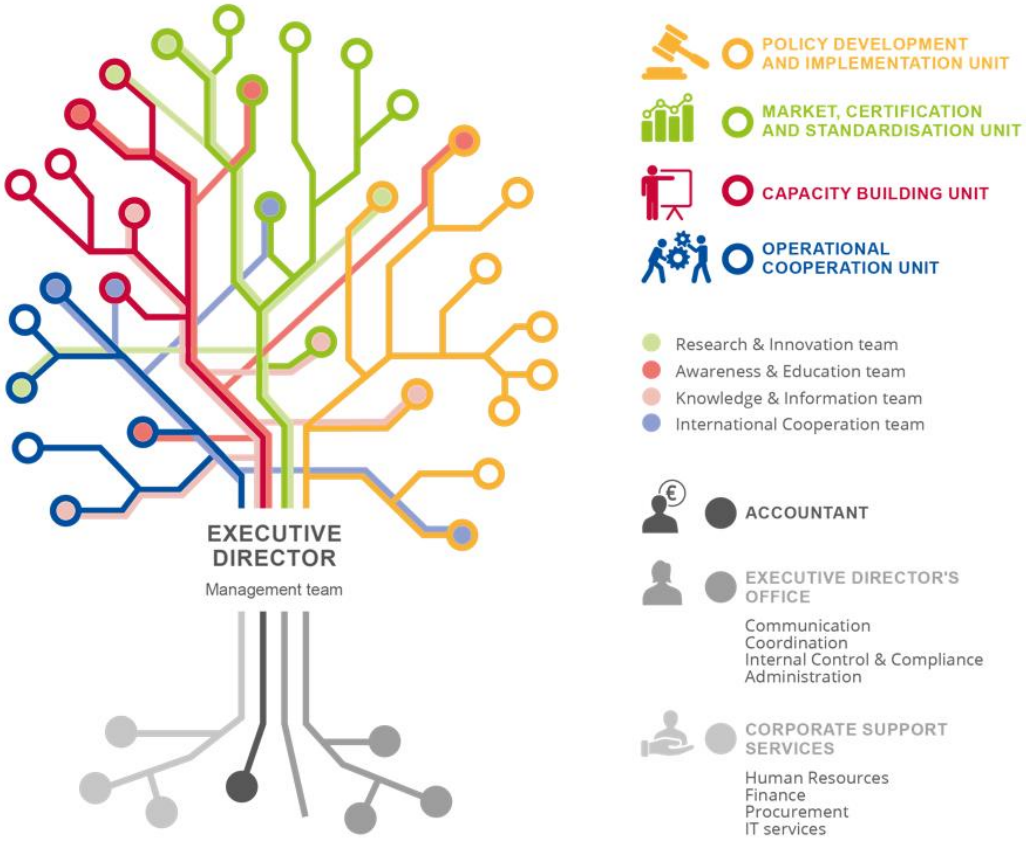
[52] Standardised set of ten questions with a scale of 1 to 10 that provide an opportunity for ENISA to seek feedback about a staff member's experience. The greater the number the better the experience.

Output 12.2				3	383 000		
Output 12.3				1.5	964 000		
Output 12.4				1.5	832 000		
Output 12.5				2	100,000		
Total	FTE 17 – Budget 4,417,000[53]						

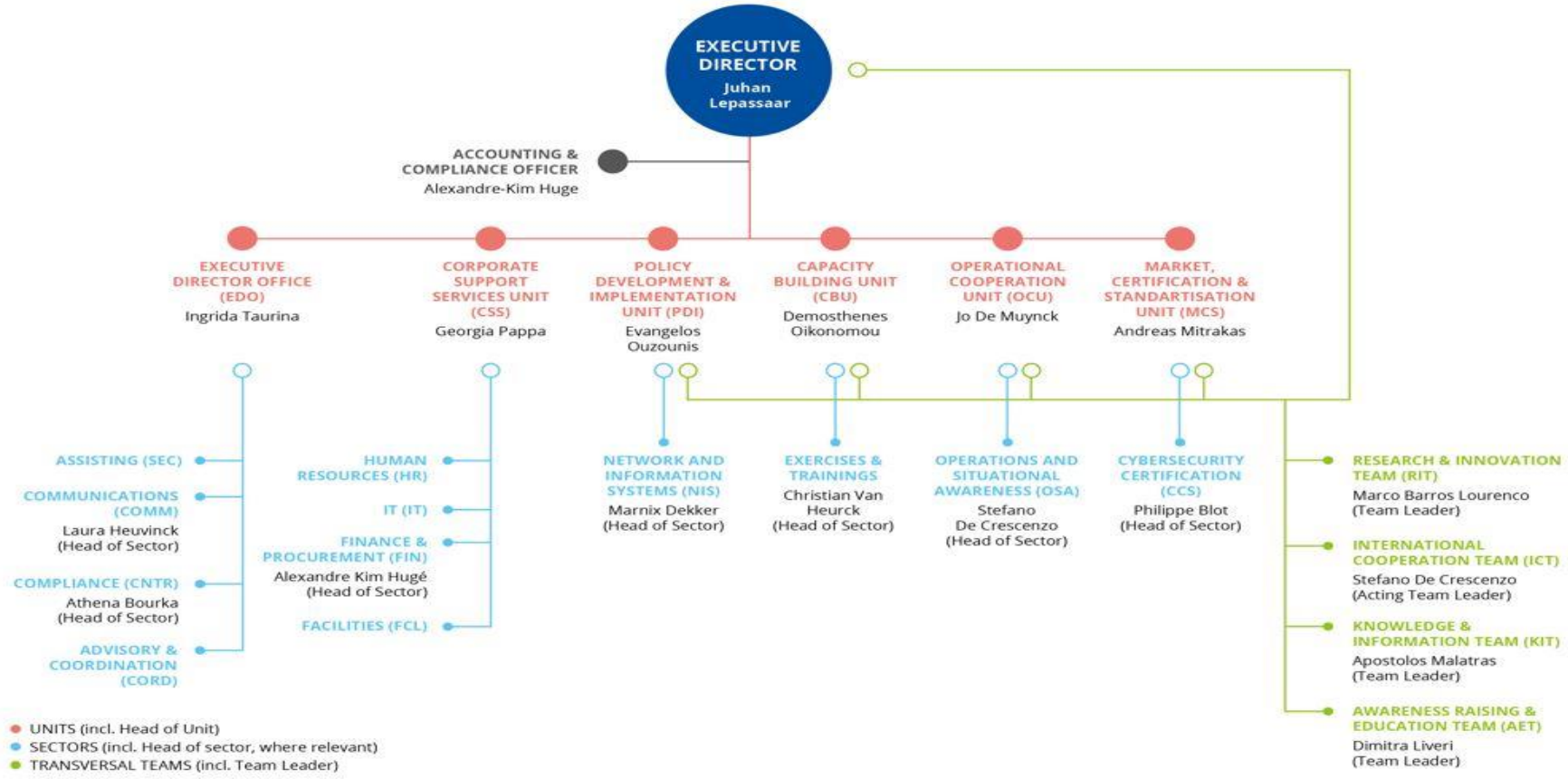
[53] Indicated budget excludes staff (TA, CA, SNE) salaries and allowances

ANNEX

I. ORGANISATION CHART AS OF 01.01.2022



Administrative Organigramme



Status in-house staff (AD;AST;CA;SNEs) on 01.09.2022

ED*	
AD	2
Total	**2**

* ED and accountant

EDO	
AD	7
AST	7
CA	2
SNE	1
Total	**17**

CSS	
AD	2
AST	6
CA	7
SNE	0
Total	**15**

PDI	
AD	11
AST	0
CA	5
SNE	0
Total	**16**

CBU	
AD	7
AST	2
CA	7
SNE	1
Total	**17**

OCU	
AD	9
AST	1
CA	3
SNE	5
Total	**18**

MCS	
AD	14
AST	2
CA	2
SNE	2
Total	**20**

SUMMARY	
AD	**52**
AST	**18**
CA	**26**
SNE	**9**
Total	**105**

II. RESOURCE ALLOCATION PER ACTIVITY 2023 - 2025

The indicative allocation of the total 2023 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 2023-2025 (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 2023.
- 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 (2023)	Activities as referred to in Section 3	Direct and Indirect budget allocation (in EUR)	FTE allocation
Providing assistance on policy development	Activity 1	907.618,48	4,75
Supporting implementation of Union policy and law	Activity 2	2.353.536,42	13,00
Building capacity	Activity 3	3.380.533,35	13,75
Enabling operational cooperation	Activity 4	4.128.083,63	16,50
Contribute to cooperative response at Union and Member States level	Activity 5	2.128.998,78	10,00
Development and maintenance of EU cybersecurity certification framework	Activity 6	1.898.516,44	9,00
Supporting European cybersecurity market and industry	Activity 7	1.085.319,11	6,00
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	1.845.044,44	8,50
Outreach and education	Activity 9	1.400.823,94	7,50
Research and innovation	Activity 10	681.566,05	4,00
Performance and risk management	Activity 11	2.844.126,72	18,00
Staff development and working environment	Activity 12	2.529.327,63	17,00
TOTAL		**25.183.495,00**	**128,00**

III. FINANCIAL RESOURCES 2023 - 2025

Table 1: Revenue

revenues	2022	2023
EU contribution	23.633.000	24.475.757
Other revenue (EFTA)	574.625	707.738
Total	24.207.625	25.183.495

REVENUES	2021 Executed Budget	2022 Adopted budget	VAR 2023 / 2022	Draft Estimated budget 2023	Envisaged 2024	Envisaged 2025
1 REVENUE FROM FEES AND CHARGES						
2 EU CONTRIBUTION	22.248.000	23.633.000	4%	24.475.757	24.610.000	25.010.000
*- of which assigned revenues deriving from previous years' surpluses ** *	*579.113*			*320.868*	*320.868*	*320.868*
- of which Reserve conditional to approval of NIS2 Directive		*610.000*		*610.000*	*610.000*	*610.000*
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	585.060	574.625	23%	707.738	711.672	723.392
- of which EEA/EFTA (excl. Switzerland)	*585.060*	*574.625*	*23%*	*707.738*	*711.672*	*723.392*
- of which Candidate Countries						
4 OTHER CONTRIBUTIONS	317.071	*	N/A	*	*	*
5 ADMINISTRATIVE OPERATIONS						
- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL REVENUES	**23.150.131**	**24.207.625**	**4%**	**25.183.495**	**25.321.672**	**25.733.392**

* - 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	2022		2023	
	Commitment appropriations	Commitment appropriations	Commitment appropriations	Payment appropriations
Title 1	12.494.335	12.494.335	12.719.412	12.719.412
Title 2	2.824.300	2.824.300	3.519.470	3.519.470
Title 3	8.888.990	8.888.990	8.944.613	8.944.613
Total expenditure	**24.207.625**	**24.207.625**	**25.183.495**	**25.183.495**

EXPENDITURE (in EUR)	Commitment and Payment appropriations					
	Executed budget 2021	Adopted Budget 2022 Agency request	Draft estimated budget 2023	VAR 2023 / 2022	Envisaged in 2024	Envisaged in 2025
Title 1. Staff Expenditure	**10.799.493**	**12.494.335**	**12.719.412**	**2%**	**12.789.201**	**12.997.153**
11 Staff in active employment *	8.370.300	10.837.880	11.019.993	2%	11.080.457	11.260.625
12 Recruitment expenditure	306.022	412.000	404.684	-2%	406.904	413.521
13 Socio-medical services and training	1.371.493	853.000	923.735	8%	928.804	943.906
14 Temporary assistance	751.678	391.455	371.000	-5%	373.036	379.101
Title 2. Building, equipment and miscellaneous expenditure	**3.855.317**	**2.824.300**	**3.519.470**	**25%**	**3.538.781**	**3.596.312**
20 Building and associated costs	1.312.041	914.550	1.357.750	48%	1.365.200	1.387.398
21 Movable property and associated costs	271.592	160.000	0	-100%	0	0
22 Current corporate expenditure	686.263	320.000	472.650	48%	475.244	482.961
23 Corporate ICT	1.585.422	1.429.750	1.689.070	18%	1.698.338	1.725.953
Title 3. Operational expenditure	**8.383.370**	**8.888.990**	**8.944.613**	**1%**	**8.993.690**	**9.139.928**
30 Activities related to meetings and missions	504.740	387.000	438.600	13%	441.007	448.177
32 Horizontal operational activities	0	0	0		0	0
36/37 Core operational activities	7.878.630	8.501.990	8.506.013	0%	8.552.684	8.691.750
TOTAL EXPENDITURE	**23.038.179**	**24.207.625**	**25.183.495**	**4%**	**25.321.672**	**25.733.393**

* for years 2022-2025 chapter 11 includes an amount of EUR 610 thou as a reserve conditional to approval of NIS Directive (for salaries of ne

Table 3: Budget outturn and cancellation of appropriations

Budget outturn	2019	2020	**2021**
Revenue actually received (+)	16.740.086	21.801.460	23.058.211
Payments made (-)	-11.980.352	-15.050.421	-17.989.374
Carry-over of appropriations (-)	-4.357.734	-6.200.614	-5.082.548
Cancellation of appropriations carried over (+)	62.522	180.023	209.385
Adjustment for carry-over of assigned revenue appropriations carried over (+)	116.393	10.403	125.622
Exchange rate difference (+/-)	-1.802	-1.291	- -428
Total	**579.113**	**739.560**	**320.868**

III.a Cancellation of appropriations

In 2021, out of an EU budget contribution to ENISA's budget of 22 833 kEUR (C1 funds), 22 721 kEUR were committed, representing a budget execution rate of 99,51%, and a total of 112 kEUR representing 0,49% of the budget was not used. A total of 17 672 kEUR representing 77.4% of the 2021 budget were paid in 2021 and a total of 5 049 kEUR representing 22.11% of the 2021 budget were carried forward into 2022.

IV. HUMAN RESOURCES - QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2023 - 2025

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

Statutory staff and SNE

STAFF	2021			2022	2023	2024	2025
ESTABLISHMENT PLAN POSTS	Authorised Budget	Actually filled as of 31/12/2021	Occupancy rate %	Adopted	Envisaged staff	Envisaged staff	Envisaged staff
Administrators (AD)	57	52	91%	63	63	63	63
Assistants (AST)	19	17	89%	19	19	19	19
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	76	69	91%	82	82	82	82
EXTERNAL STAFF	FTE corresponding to the authorised budget 2021	Executed FTE as of 31/12/2021	Execution Rate %	Adopted FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	30	27	90%	32	32	32	32

Seconded National Experts (SNE)	12	10	83%	12	14	16[54]**	18**
TOTAL External Staff	**42**	**37**	**88%**	**44**	**46**	**48**	**50**
TOTAL STAFF[55]	**118**	**106**	**90%**	**126**	**128**	**130**	**132**

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 31/12/2020	Actually in place as of 31/12/2021
Security	5	5
IT	4	5

- Interim workers

	Actually in place as of 31/12/2020	Actually in place as of 31/12/2021
Number	31	10

[54]** In its budget proposal for the Single Programming Document (SPD) 2023-2025, the Agency asks for an extra 4 SNE posts introduced gradually (2+2 over 2 years) from 2024.
[55] Refers to TAs, CAs and SNEs figures

Table 2: Multi-annual staff policy plan Years 2021-2025[56]

Function group and grade	2021				2022		2023		2024		2025	
	Authorised budget		Actually filled as of 31/12/2021		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		1		1		2		2		2		2
AD 12		5		5		4		4		4		4
AD 11		2				2		2		3		4
AD 10		3		3		4		4		4		3
AD 9		12		9		11		11		14		15
AD8		21		9		22		25		23		24
AD 7		8		12		8		10		9		8
AD 6		4		12		9		4		3		2
AD 5												
AD TOTAL		57		52		63		63		63		63
AST 11												
AST 10												
AST 9												
AST 8		1		1		2		2		3		4
AST 7		4		3		3		4		4		4
AST 6		8		2		8		7		7		7
AST 5		5		4		5		5		5		4
AST 4		1		4		1		1		0		0
AST 3				2								
AST 2				1								
AST 1												
AST TOTAL		19		17		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												

[56] 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	2021				2022		2023		2024		2025	
	Authorised budget		Actually filled as of 31/12/2021		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		76		69		82		82		82		82
GRAND TOTAL	76		69		82		82		82		82	

External personnel

Contract Agents

Contract agents	FTE corresponding to the authorised budget 2021	Executed FTE as of 31/12/2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025
Function Group IV	28	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	30	27	32	32	32	32

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2021	Executed FTE as of 31/12/2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025
TOTAL	12	10	12	14	14[57]**	14*

Table 3: Recruitment forecasts 2023 following retirement / mobility or new requested posts (indicative table)

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

[57]* In its budget proposal for the Single Programming Document (SPD) 2023 – 2025, the Agency asks for an extra 4 SNE posts introduced gradually 2+2 over 2 years) from 2024.

	Due to foreseen retirement/ mobility	New post requested due to additional tasks	Internal (brackets)	External (brackets)	
Expert		n/a	n/a	n/a	n/a
Officer		n/a	n/a	n/a	n/a
Assistant		n/a	n/a	n/a	n/a

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 2016**	**Year 2017**	**Year 2018**	**Year 2019**	**Year 2020**	**Year 2021**	**Actual average over 5 years**	**Average over 5 years (According to decision C(2015)9563)**
AD05	-	-	-	-	-	-	-	2.8
AD06	1	1	2	3	-	1	3,7	2.8
AD07	1	-	-	-	1	-	-	2.8
AD08	1	1	1	-	2	1	4,3	3
AD09	-	-	1	-	-	-	-	4
AD10	-	-	-	-	-	-	-	4
AD11	1	-	-	-	-	-	-	4
AD12	-	-	-	-	-	1	10	6.7
AD13	-	-	-	-	-	-	-	6.7
AST1	-	-	-	-	-	-	-	3
AST2	-	-	-	-	-	-	-	3
AST3	1	1	1	-	-	-	-	3
AST4	1	1	1	-	1	-	-	3
AST5	1	-	1	-	-	1	5,5	4
AST6	1	-	-	-	1	1	3,5	4
AST7	-	-	-	-	-	1	5	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 31.12.2021	HOW MANY STAFF MEMBERS WERE RECLASSIFIED IN YEAR 2021	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	0	-	-	Between 5 and 7 years
	15	2	-	-	Between 4 and 6 years
	14	15	5	3	Between 3 and 5 years
	13	1	-	-	Between 3 and 5 years
CA III	12	1			-
	11	0	-	-	Between 6 and 10 years
	10	5	1	3	Between 5 and 7 years
	9	1	-	-	Between 4 and 6 years
	8	0	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 31.12.2021 statutory staff (only temporary agents and contract agents on 31.12.2021)

		OFFICIAL		TEMPORARY		CONTRACT AGENTS		GRAND TOTAL	
		Staff	**%**	**Staff**	**%**	**Staff**	**%**	**Staff**	**%**
Female	Administrator level	-	-	18	26%	15	-	-	-
	Assistant level (AST & AST/SC)	-	-	11	16%	-	-	-	-
	Total	-	-	29	42%	15	56%	44	46%
Male	Administrator level	-	-	34	49%	12	-	-	-
	Assistant level (AST & AST/SC)	-	-	6	9%	-	-	-	-
	Total	-	-	40	58%	12	44%	52	54%
Grand Total		-	-	69	**100%**	27	**100%**	96	**100%**

TABLE 2: **DATA REGARDING GENDER EVOLUTION OVER 5 YEARS OF THE MIDDLE AND SENIOR MANAGEMENT (31.12.2021)**	**2016**		**31.12.2021**	
	Number	**%**	**Number**	**%**
Female Managers	0	0	3[58]	27%
Male Managers	10	100	8[59]	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 31.12.2021 - statutory staff only

[58] This category comprises Heads of Unit and Team Leaders
[59] 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%	2	8%	7	7%
BG	2	3%	-	-	2	2%
CY	1	1%	2	8%	3	3%
CZ	1	1%	-	-	1	1%
DE	2	3%	-	-	2	2%
Double *60	4	6%	3	12%	7	7%
EE	1	1%	-	-	1	1%
ES	3	4%	1	4%	4	4%
FR	3	4%	1	4%	4	4%
GR	26	37%	12	48%	38	40%
IT	5	7%	-	-	5	5%
LT	-	-	1	4%	1	1%
LV	2	3%	-	-	2	2%
NL	2	3%	-	-	2	2%
PL	3	4%	1	4%	4	4%
PT	3	4%	1	4%	4	4%
RO	7	10%	0	0%	7	7%
SE	1	1%	-	-	1	1%
SK	-	-	1	4%	1	1%
TOTAL	71	100%	25	100%	96	100%

[60] 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	2016		31.12.2021	
	Number	%	Number	%
Greek	27 (out of 68)	39,7	38 (out of 96)	39,6

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[61].

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 is investigating opportunities to strengthen its environmental management as such a new output was introduced in 2022 to carry out an overarching audit on the CO2 impact of all operations of the Agency and develop and implement a targeted action plan The objective of this undertaking is for the Agency to be climate neutrality by 2030.

VII. BUILDING POLICY

Current buildings

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

[61] 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					

Brussels office

In 2020 ENISA put forward a proposal to open a local office in accordance with CSA Art 20 (5). The number of the staff in each local office shall not exceed 10 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located.

The first stage of implementing the Brussels Office, which entailed the set up and furnishing of the ENISA workspace was completed in April 2022 and the office has been operational since then. The office is being used on a daily basis by Brussels based staff, which is a significant benefit for the Operational Cooperation Unit as they are able to communicate easily with the CERT EU Team situated on the same floor. The objective of the second implementation phase, which is currently ongoing, is to obtain accreditation for the secure room, which will enable the agency to handle EU Classified Information (EUCI) in its Brussels premises. The second phase of implementation is likely to continue into Q2 2023.Indicative resources foreseen:

		2023	2024	2025
Head count (FTEs)		**4-10**	**4-10**	**4 - 10**
Budget (one-off & maintenance costs)		**170.000**	**170.000**	**170.000**

VIII. PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education / day care
In accordance with Art. 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff.	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.	A public School of European Education, Type 2, was founded in 2005 by the Greek government in Heraklion –

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.	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.	Crete for the children of the staff of ENISA. There is no European School operating in Athens.

IX. EVALUATIONS

Ex-ante and ex-poste evaluations were issued in 2021 and need for evaluation to be reconsidered during 2023

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

As adopted by the Management Board[62], the Agency's strategy for an effective internal control 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 control, 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 control and to support the achievement of objectives. In this aspect it is needed to consider external and internal communication. External communication provides the specific Agency 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 control 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[63] as recommended by the European Anti-Fraud Office (OLAF)

Following relevant guidance and best practices developed within the EU Agencies network, ENISA initiated in 2022 a thorough review of its internal control framework indicators and overall strategy. The review aims to consolidate input from different sources and integrate the results of various risk assessments within a single internal control

[62] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202019-12%20on%20internal%20controls%20framework.pdf
[63] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-5-on-anti-fraud-strategy

assessment process. The revised ENISA's internal control framework will be put in place 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 [64] 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.

XIII. ANNUAL COOPERATION PLAN 2023

The 2023 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 2023-2025 as a separate document.

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

XX-00-00-000-XX-X

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

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

MB Decision 2022/14 on the Single Programming Document (SPD) 2023-2025

ANNEX 1
ANNUAL COOPERATION PLAN 2023

(Not publicly available)

Final Statement of Estimates 2023 (Budget 2023)

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 2023

The 2023 total revenue amounts to € 25183495 and consists of a subsidy of € 24475757 from the General Budget of the European Union and EFTA countries' contributions € 707738
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 2023

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 2023, which contains 81 Temporary Agent posts.

Total expenditure under Title 1 amounts to	€	12.719.412,14

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to	€	3.519.470,00

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of Work Programme 2023 and amounts to	€	8.944.613,00

3. STATEMENT OF REVENUE 2023

Title	Heading	Voted Appropriations 2021 €	Voted Appropriations 2022 €	Proposed Draft Appropriations 2023 €	Remarks - budget 2023
1	EUROPEAN COMMUNITIES SUBSIDY	22.248.000	23.633.000	24.475.757	Total subsidy of the European Communities
2	THIRD COUNTRIES CONTRIBUTION	585.060	574.625	707.738	Contributions from Third Countries.
3	OTHER CONTRIBUTIONS	640.000	0	0	Subsidy from the Government of Greece
4	ADMINISTRATIVE OPERATIONS	0	0	0	Other expected income.
	GRAND TOTAL	**23.473.060**	**24.207.625**	**25.183.495**	

Article Item	Heading	Voted Appropriations 2021 €	Voted Appropriations 2022 €	Proposed Draft Appropriations 2023 €	Remarks - budget 2023
1	EUROPEAN COMMUNITIES SUBSIDY				
10	EUROPEAN COMMUNITIES SUBSIDY				
100	*European Communities subsidy*	22.248.000	23.633.000	24.475.757	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	22.248.000	23.633.000	24.475.757	
	TITLE 1	**22.248.000**	**23.633.000**	**24.475.757**	
2	THIRD COUNTRIES CONTRIBUTION				
20	THIRD COUNTRIES CONTRIBUTION				
200	*Third Countries contribution*	585.060	574.625	707.738	Contributions from Associated Countries.
	CHAPTER 2 0	585.060	574.625	707.738	
	TITLE 2	**585.060**	**574.625**	**707.738**	
3	OTHER CONTRIBUTIONS				
30	OTHER CONTRIBUTIONS				
300	*Subsidy from the Ministry of Transports of Greece*	640.000	0	0	Subsidy from the Government of Greece.
	CHAPTER 30	640.000	0	0	
	TITLE 3	**640.000**	**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	**23.473.060**	**24.207.625**	**25.183.495**	

4. STATEMENT OF EXPENDITURE 2023

Title	Heading	Voted Appropriations 2021 €	Voted Appropriations 2022 €	Proposed Draft Appropriations 2023 €	Remarks - budget 2023
1	STAFF	10.775.409	12.494.335	12.719.412	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE	3.547.651	2.824.300	3.519.470	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE	9.150.000	8.888.990	8.944.613	Total funding for operational expenditures.
	GRAND TOTAL	**23.473.060**	**24.207.625**	**25.183.495**	
1	STAFF				

11	**STAFF IN ACTIVE EMPLOYMENT**					
110	***Staff holding a post provided for in the establishment plan***					
1100	Basic salaries		6.453.819	8.361.489	8.551.219	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	6.453.819	8.361.489	8.551.219	
111	***Other staff***					
1110	Contract Agents		2.106.500	1.819.391	1.967.658	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)		250.000	657.000	501.116	This appropriation is intended to cover basic salaries and all benefits of SNEs.
		Article 1 1 1	2.356.500	2.476.391	2.468.774	
		CHAPTER 11	**8.810.319**	**10.837.880**	**11.019.993**	
12	**RECRUITMENT/DEPARTURE EXPENDITURE**					
120	***Expenditure related to recruitment***					
1200	Expenditure related to recruitment		49.087	10.000	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	n/a	404.684	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	49.087	10.000	404.684	
121	***Expenditure on entering/leaving and transfer***					
1210	Expenses on Taking Up Duty and on End of Contract		32.000	17.000	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		145.000	204.000	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		72.000	89.000	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		112.000	92.000	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	361.000	402.000	0	
		CHAPTER 1 2	**410.087**	**412.000**	**404.684**	

13	**SOCIO-MEDICAL SERVICES AND TRAINING**					
131	***Medical Service***					
1310	Medical Service		53.882	63.000	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	53.882	63.000	0	
132	***Staff Development***					
1320	Staff Development		280.182	220.000	232.215	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	280.182	220.000	232.215	
133	***Staff Welfare***					
1330	Other welfare expenditure		250.000	40.000	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		500.000	530.000	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	n/a	691.520	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	750.000	570.000	691.520	
		CHAPTER 1 3	**1.084.064**	**853.000**	**923.735**	
14	**TEMPORARY ASSISTANCE**					
140	***European Commission Management Costs***					
1400	EC Management Costs		70.939	70.000	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	70.939	70.000	0	
142	***Temporary Assistance***					
1420	External Temporary Staffing		400.000	321.455	371.000	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
		Article 1 4 2	400.000	321.455	371.000	
		CHAPTER 1 4	**470.939**	**391.455**	**371.000**	
		Total Title 1	**10.775.409**	**12.494.335**	**12.719.412**	
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**					
20	**BUILDINGS AND ASSOCIATED COSTS**					
200	**Buildings and associated costs**					
2000	Rent of buildings		640.000	78.151	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	n/a	1.357.750	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	76.050	145.317	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		120.000	250.083	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		50.000	40.000	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		140.000	157.590	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		378.558	243.409	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	1.404.608	914.550	1.357.750	
		CHAPTER 2 0	**1.404.608**	**914.550**	**1.357.750**	
21	**MOVABLE PROPERTY AND ASSOCIATED COSTS**					
210	***Technical Equipment and installations***					
2100	Technical Equipment and services		30.000	10.000	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	30.000	10.000	0	
211	***Furniture***					
2110	Furniture		49.000	125.000	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	49.000	125.000	0	
212	***Transport Equipment***					
2121	Maintenance and Repairs of transport equipment		10.000	10.000	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	10.000	0	
213	***Library and Press***					
2130	Books, Newspapers and Periodicals		10.000	15.000	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	10.000	15.000	0	
		CHAPTER 2 1	**99.000**	**160.000**	**0**	
22	**CURRENT CORPORATE AND ADMINISTRATIVE EXPENDITURE**					
220	***Stationery, postal and telecomunications***					
2200	Stationery and other office supplies		30.000	27.000	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		20.000	22.000	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	50.000	49.000	0	
221	***Financial charges***					
2210	Bank charges and interest paid		1.000	1.000	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	1.000	0	

222	***Consultancy and other outsourced services***					
2220	Consultancy and other outsourced services (incl. legal services)		747.696	270.000	379.650	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	747.696	270.000	379.650	
223	***Corporate and Administrative Expenditures***					
2230	Corporate and Administrative Expenditures		n/a	n/a	93.000	This appropriation is intended to cover corporate and administrative expenditure such as the costs of purchasing, leasing, and repairs of furniture, the costs of maintenance and repairs of transport equipment as well as insurance and fuel, the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions, the costs of office stationery and the purchase of office kitchen consumables, post office and special courrier costs, bank charges, interest paid and other financial and banking costs and other costs of corporate administrative nature.
		Article 2 2 3	0	0	93.000	
		CHAPTER 2 2	**798.696**	**320.000**	**472.650**	
23	**ICT**					
231	***Core and Corporate ICT expenditure***					
2310	Corporate ICT recurrent costs		585.347	1.065.000	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		660.000	364.750	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	n/a	1.689.070	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	1.245.347	1.429.750	1.689.070	
		CHAPTER 2 3	**1.245.347**	**1.429.750**	**1.689.070**	
		Total Title 2	**3.547.651**	**2.824.300**	**3.519.470**	
3	**OPERATIONAL EXPENDITURE**					
30	**ACTIVITIES RELATED TO OUTREACH AND MEETINGS**					
300	***Outreach, meetings and representation expenses***					
3001	Outreach, meetings, translations and representation expenses		650.000	387.000	438.600	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 10-11 as defined in the SPD 2021-2023 mainly covering horizontal tasks and other administrative services.
		Article 3 0 0	650.000	387.000	438.600	
		CHAPTER 3 0	**650.000**	**387.000**	**438.600**	

37	**CORE OPERATIONAL ACTIVITIES**				
371	***Activity 1 - Providing assistance on policy development***				
3710	Activity 1 - Providing assistance on policy development	280.000	363.000	330.262	This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT and mission costs).
	Article 3 7 1	280.000	363.000	330.262	
372	***Activity 2 - Supporting implementation of Union policy and law***				
3720	Activity 2 - Supporting implementation of Union policy and law	985.000	798.475	773.404	This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT and mission costs).
	Article 3 7 2	985.000	798.475	773.404	
373	***Activity 3 - Capacity building***				
3730	Activity 3 - Capacity building	1.400.000	1.921.265	1.709.239	This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs).
	Article 3 7 3	1.400.000	1.921.265	1.709.239	
374	***Activity 4 - Enabling operational cooperation***				
3740	Activity 4 - Enabling operational cooperation	1.110.000	1.703.350	2.122.530	This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT and mission costs).
	Article 3 7 4	1.110.000	1.703.350	2.122.530	
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	1.200.000	824.500	913.512	This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT and mission costs).
	Article 3 7 5	1.200.000	824.500	913.512	
376	***Activity 6 - Development and maintenance of EU cybersecurity certification framework***				
3760	Activity 6 - Development and maintenance of EU cybersecurity certification framework	870.000	1.025.750	804.578	This appropriation is intended to cover direct operational costs relevant to the Activity 6 (including operational ICT and mission costs).
	Article 3 7 6	870.000	1.025.750	804.578	
377	***Activity 7 - Supporting European cybersecurity market and industry***				
3770	Activity 7 - Supporting European cybersecurity market and industry	490.000	373.800	356.027	This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT and mission costs).
	Article 3 7 7	490.000	373.800	356.027	
378	***Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities***				
3780	Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities	1.155.000	1.051.950	811.881	This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT and mission costs).
	Article 3 7 8	1.155.000	1.051.950	811.881	
379	***Activity 9 - Outreach and education***				
3790	Activity 9 - Outreach and education	1.010.000	439.900	489.209	This appropriation is intended to cover direct operational costs relevant to the Activity 9 (including operational ICT and mission costs).
	Article 3 7 9	1.010.000	439.900	489.209	
370	***Activity 10 - Advise on Research and Innovation Needs and priorities***				
3700	Activity 10 - Advise on Research and Innovation Needs and priorities	1.010.000	439.900	195.371	This appropriation is intended to cover direct operational costs relevant to the Activity 10 (including operational ICT and mission costs).
	Article 3 7 0	1.010.000	439.900	195.371	
	CHAPTER 3 7	**8.500.000**	**8.501.990**	**8.506.013**	
	TITLE 3	**9.150.000**	**8.888.990**	**8.944.613**	
	GRAND TOTAL	**23.473.060**	**24.207.625**	**25.183.495**	

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

ANNEX 3 - Final Establishment plan 2023[1]

Category and grade	Establishment plan in voted EU Budget 2022		Establishment plan 2023	
	Off.	TA	Off.	TA
AD 16				
AD 15		1		1
AD 14				
AD 13		2		2
AD 12		4		4
AD 11		2		2
AD 10		4		4
AD 9		11		11
AD 8		22		25
AD 7		8		10
AD 6		9		4
AD 5				
Total AD		**63**		**63**
AST 11				
AST 10				
AST 9				
AST 8		2		2
AST 7		3		4
AST 6		8		7
AST 5		5		5
AST 4		1		1
AST 3				
AST 2				
AST 1				
Total AST		**19**		**19**
AST/SC1				
AST/SC2				
AST/SC3				
AST/SC4				
AST/SC5				
AST/SC6				

[1] The change in the number of establishment plan up to 10% requested for year 2023 is modified as per Art 38 of the ENISA Financial Regulation.

Total AST/SC				
TOTAL		**82**		**82**