



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

# ENISA SINGLE PROGRAMMING DOCUMENT 2024 -2026

Including multiannual planning, 2024 work  
programme and multiannual staff planning



JANUARY 2024

## CONTACT

For contacting ENISA please use the following details:  
info@enisa.europa.eu  
website: [www.enisa.europa.eu](http://www.enisa.europa.eu)

## LEGAL NOTICE

[This publication presents the European Union Agency for Cybersecurity \(ENISA\) Single Programming Document 2024-2026 as approved by the Management Board in Decision No MB/2023/10. The Management Board may amend the Work Programme 2024-2026 at any time. ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source. Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.](#)

## COPYRIGHT NOTICE

[© European Union Agency for Cybersecurity \(ENISA\), 2024.](#)  
[This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International \(CC BY 4.0\) licence \(https://creativecommons.org/licenses/by/4.0/\). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".](#)  
[Copyright for the image on the cover and internal pages: © Shutterstock](#)  
[For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.](#)

[Luxembourg: Publications Office of the European Union, 2024](#)

<b>Linguistic version</b>	<b>Catalogue number</b>	<b>ISBN</b>	<b>ISSN</b>	<b>DOI</b>
<b>BOOK</b>	TP-AH-24-001-EN-C	978-92-9204-664-4	2467-4397	10.2824/338913
<b>PDF</b>	TP-AH-24-001-EN-N	978-92-9204-663-7	2467-4176	10.2824/010827



# ENISA SINGLE PROGRAMMING DOCUMENT 2024–2026

EUROPEAN UNION AGENCY  
FOR CYBERSECURITY



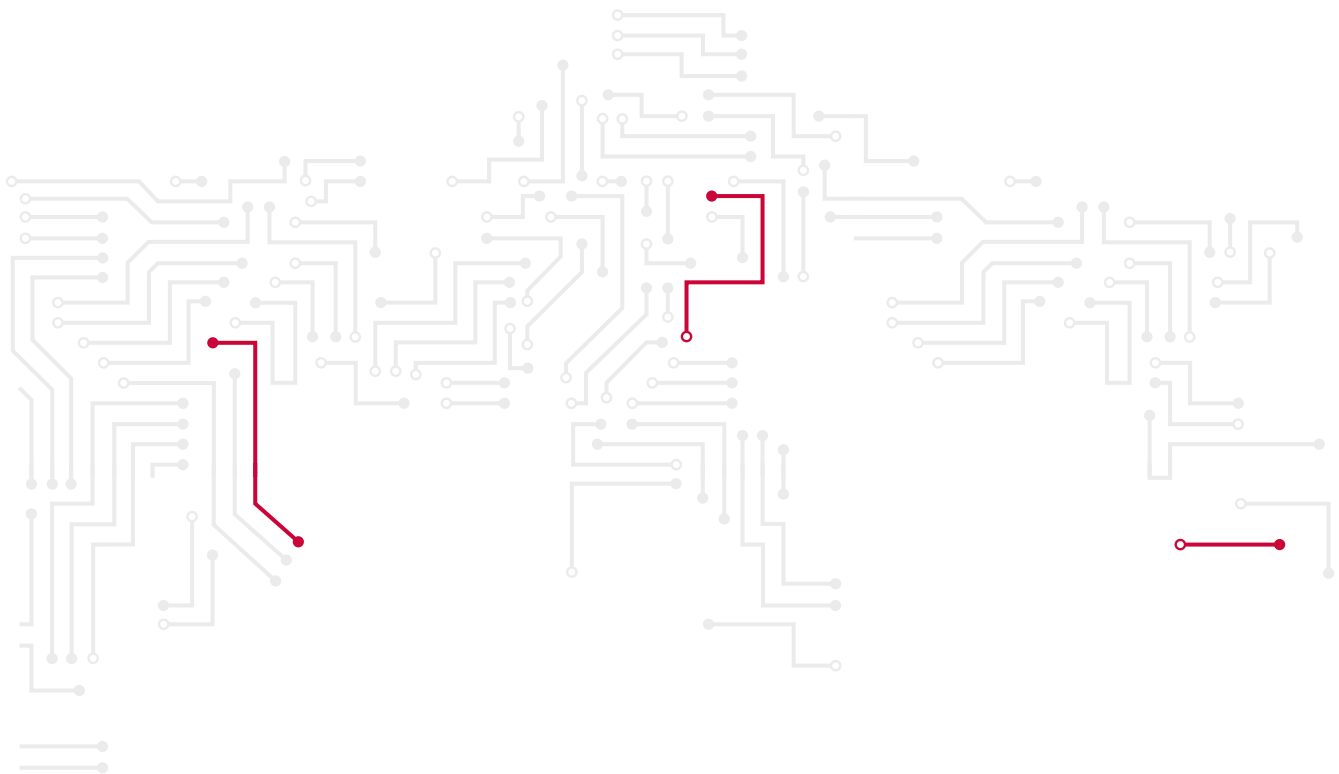
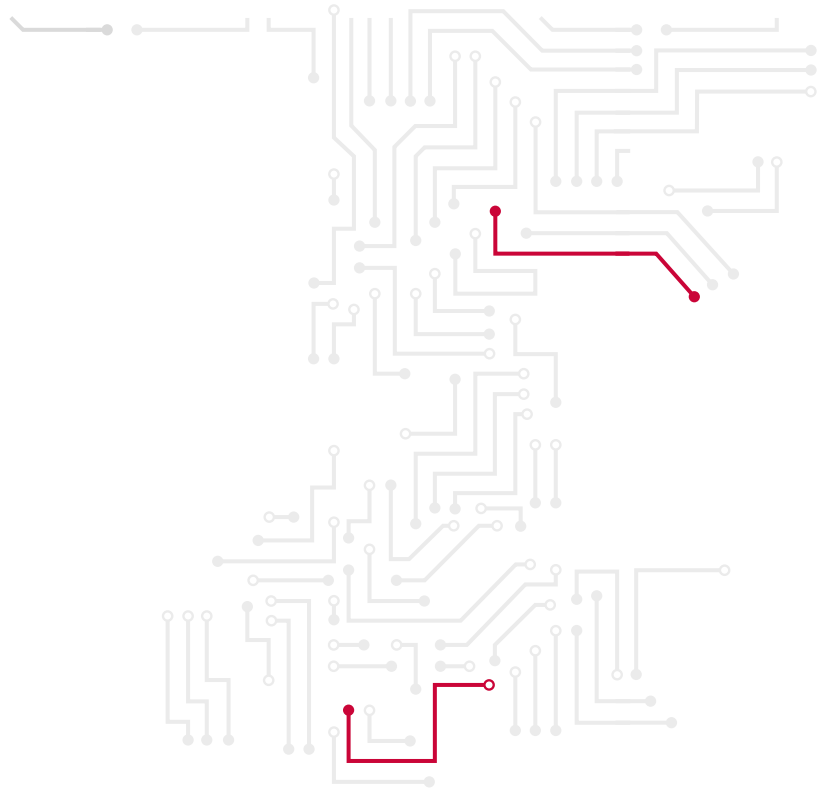


# TABLE OF CONTENTS

<b>SECTION I</b> <b>GENERAL CONTEXT</b>	<b>15</b>
<b>SECTION II</b> <b>MULTIANNUAL PROGRAMMING 2024–2026</b>	<b>28</b>
<b>2.1. MULTIANNUAL WORK PROGRAMME</b>	<b>28</b>
<b>2.2. HUMAN AND FINANCIAL RESOURCES – OUTLOOK FOR 2024–2026</b>	<b>37</b>
2.2.1. Overview of the past and current situations	<b>37</b>
2.2.2. Outlook for 2024–2026	<b>40</b>
2.2.3. Resource programming for 2024–2026	<b>40</b>
2.2.3.1. Financial resources	<b>40</b>
2.2.3.2. Human resources	<b>40</b>
2.2.4. Strategy for achieving efficiency gains	<b>42</b>
2.2.4.1. Strategy to achieve operational efficiency gains	<b>33</b>
2.2.4.2. Strategy to achieve corporate and administrative efficiency gains	
<b>SECTION III</b> <b>WORK PROGRAMME FOR 2024</b>	<b>50</b>
<b>3.1. OPERATIONAL ACTIVITIES</b>	<b>51</b>
<b>3.2. CORPORATE ACTIVITIES</b>	<b>86</b>
<b>ANNEX 1</b> <b>ORGANISATION CHART AS OF 1 JANUARY 2021</b>	<b>97</b>
<b>ANNEX 2</b> <b>RESOURCE ALLOCATION PER ACTIVITY 2024–2026</b>	<b>100</b>
<b>ANNEX 3</b> <b>FINANCIAL RESOURCES 2024–2026</b>	<b>102</b>
<b>ANNEX 4</b> <b>HUMAN RESOURCES – QUANTITATIVE</b>	<b>105</b>



<b>ANNEX 5</b> <b>HUMAN RESOURCES – QUALITATIVE</b>	<b>109</b>
<b>ANNEX 6</b> <b>ENVIRONMENT MANAGEMENT</b>	<b>114</b>
<b>ANNEX 7</b> <b>BUILDING POLICY</b>	<b>115</b>
<b>ANNEX 8</b> <b>PRIVILEGES AND IMMUNITIES</b>	<b>116</b>
<b>ANNEX 9</b> <b>EVALUATIONS</b>	<b>117</b>
<b>ANNEX 10</b> <b>STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS</b>	<b>118</b>
<b>ANNEX 11</b> <b>PLAN FOR GRANTS, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS</b>	<b>119</b>
<b>ANNEX 12</b> <b>STRATEGY FOR COOPERATION WITH NON-EU COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS</b>	<b>120</b>
<b>ANNEX 13</b> <b>ANNUAL COOPERATION PLAN 2024</b>	<b>121</b>





# ABBREVIATIONS

<b>AAR</b>	Annual activity report	<b>EUCI</b>	EU classified information
<b>ABAC</b>	Accruals-based accounting	<b>EU-CyCLONe</b>	Cyber Crisis Liaison Organisation Network
<b>AD</b>	Administrator	<b>EUDIW</b>	European digital identity wallet
<b>AHWG</b>	Ad hoc working group	<b>EUIBAs</b>	European institutions, bodies and agencies
<b>AI</b>	Artificial intelligence	<b>EU-LISA</b>	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
<b>AST</b>	Assistant		
<b>CA</b>	Contract agenda	<b>FTE</b>	Full-time equivalent
<b>CAB</b>	Conformity Assessment Body	<b>HoU</b>	Head of unit
<b>Cedefop</b>	European Centre for the Development of Vocational Training	<b>HQ</b>	headquarters
<b>CEN</b>	European Committee for Standardization	<b>ICT</b>	Information and communication technology
<b>CENELEC</b>	European Committee for Electrotechnical Standardization	<b>INDEX</b>	Cybersecurity index service package
<b>CERT-EU</b>	Computer Emergency Response Team for EU institutions, bodies and agencies	<b>ISAC</b>	Information sharing and analysis centre
<b>CO<sub>2</sub></b>	Carbon dioxide	<b>IT</b>	Information technology
<b>CRA</b>	Cyber resilience act	<b>JCAR</b>	Joint cyber assessment report
<b>CSA</b>	Cybersecurity Act	<b>KPI</b>	Key performance indicator
<b>CSIRT</b>	Computer Security Incidence Response Team	<b>L &amp; D</b>	Learning and development
<b>DDoS</b>	Distributed denial of service	<b>MoU</b>	Memorandum of understanding
<b>DGA</b>	Data Governance Act	<b>MT</b>	Management Team
<b>DORA</b>	Digital Operational Resilience Act	<b>NCCA</b>	National Cybersecurity Certification Authority
<b>DSP</b>	Digital service providers	<b>NIS</b>	Networks and Information Systems
<b>EC3</b>	European Cybercrime Centre	<b>NISD</b>	NIS Directive
<b>ECCC</b>	Eu Cybersecurity Competence Centre	<b>NIS2</b>	NIS2 Directive
<b>ECCG</b>	European Cybersecurity Certification Group	<b>NIS CG</b>	NIS Cooperation Group
<b>ECSC</b>	European cybersecurity challenge	<b>NLO</b>	National Liaison Officers
<b>ECSF</b>	European cybersecurity skills framework	<b>OECD</b>	Organisation for Economic Co-operation and Development
<b>ECSM</b>	European cybersecurity month	<b>OES</b>	Operators of essential services
<b>ED</b>	Executive director	<b>pentest</b>	penetration tests
<b>EEAS</b>	European External Action Service	<b>PPMT</b>	Public Procurement Management Tool
<b>eIDAS</b>	Electronic identification and trust services	<b>R &amp; I</b>	Research and innovation
<b>EMAS</b>	eco-management and audit scheme	<b>SC</b>	Secretary
<b>ENISA</b>	European Union Agency for Cybersecurity	<b>SCCG</b>	Stakeholder Cybersecurity Certification Group
<b>ETL</b>	ENISA Threat Landscape	<b>SITAW</b>	Situational awareness service package
<b>EUAN</b>	EU Agencies Network	<b>SLA</b>	Service-level agreement
		<b>SMEs</b>	Small and medium-sized enterprises
		<b>SNE</b>	Seconded national expert
		<b>SOCs</b>	Security Operation Centres
		<b>SOP</b>	Standard Operating Procedure
		<b>SPD</b>	Single Programming Document
		<b>TA</b>	Temporary agent
		<b>tnCO2eq</b>	tonnes of carbon dioxide equivalent



## FOREWORD

This year, The European Union Agency for Cybersecurity (ENISA) will be celebrating 20 years since its establishment in 2004. As it will celebrate its joint two-decade-long contributions in raising resilience and cybersecurity across the EU – together with Member States (MSs), EU partners and allies worldwide – ENISA also needs to acknowledge that cyber threats have continued to increase globally and the world itself has become much more unstable and unpredictable since its conception.

The threat landscape has been severely impacted over the past 2 years by the Russian war of aggression and other geopolitical tensions via distributed denial-of-service (DDoS) and ransomware attacks, a huge rise in information manipulation, and attacks against data to be used for extortion. The motivation of the aggressor continues to be either to destroy critical infrastructures and render them unavailable, thus impacting the target's resilience, or to dissuade and manipulate public opinion through misinformation and information manipulation. It is necessary to keep that in mind in 2024, which is an important juncture in the EU as its functioning is underpinned by free and fair elections.

Thus, besides building on ENISA's accumulated expertise and strengths, it is important to further enhance its proactive capabilities at the service of the MSs in 2024. The agency has introduced a new activity within this single programming document (SPD) with the aim of putting the ENISA support action on a firmer ground, enabling it to better organise its assistance to MSs. In this way, ENISA can better help the MSs in their efforts to improve the capability to respond to cyber threats and incidents while providing

them with knowledge and expertise and increasing preparedness in key sectors. Here the agency acknowledges the importance of the additional financial resources made available to it by the European Commission, without which this activity would not be possible.

The agency will also strengthen its capabilities and capacities in supporting MSs with the implementation of Directive (EU) 2022/2555 (the second network and information systems directive (NIS2)) – which will need to be fully transposed by September 2024 – including by significantly increasing its human resources dedicated to this activity (+ 43 % compared to 2022). This is in spite of the strain on its human resources, which will be further put under pressure once and if legislative initiatives such as the cyber resilience act (CRA) or the cyber solidarity act are adopted during the current multiannual programming period (2024–2026).

The agency, through its current multiannual work programme, will continue to promote a whole-of-society approach towards cybersecurity, focusing on areas which add the most value to the MSs and to the community at large. As 2024 will also mark the final effective year of its current strategy, it will, together with its Management Board (MB), launch a review of ENISA strategy. These discussions, together with the envisaged adoption of the first ever state of cybersecurity in the EU report under Article 18 of NIS2, will enable the agency to adjust its programming document and organisation, so it can direct its strategic focus to the areas which matter most for achieving its aspiration for a high common level of cybersecurity across the EU.

**Juhan Lepassaar**  
Executive Director



# MISSION STATEMENT

The mission of 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 MSs 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 MSs and the EU institutions and agencies. It strives to ensure the 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

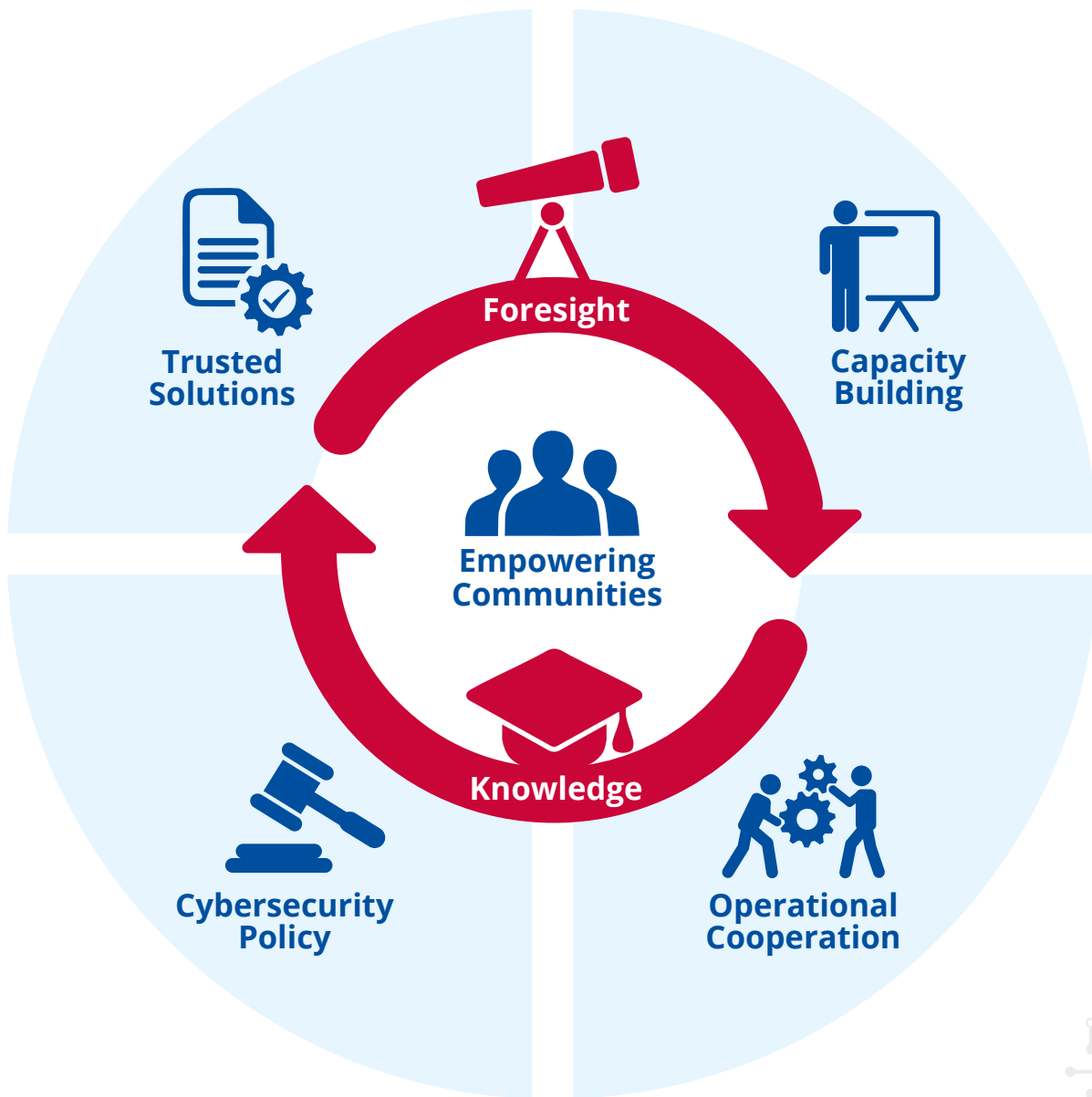
Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity 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. Cyberattacks 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 MSs 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 information and communications technology (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 MSs 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 the 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 in digital solutions and the wider digital environment.

## FORESIGHT

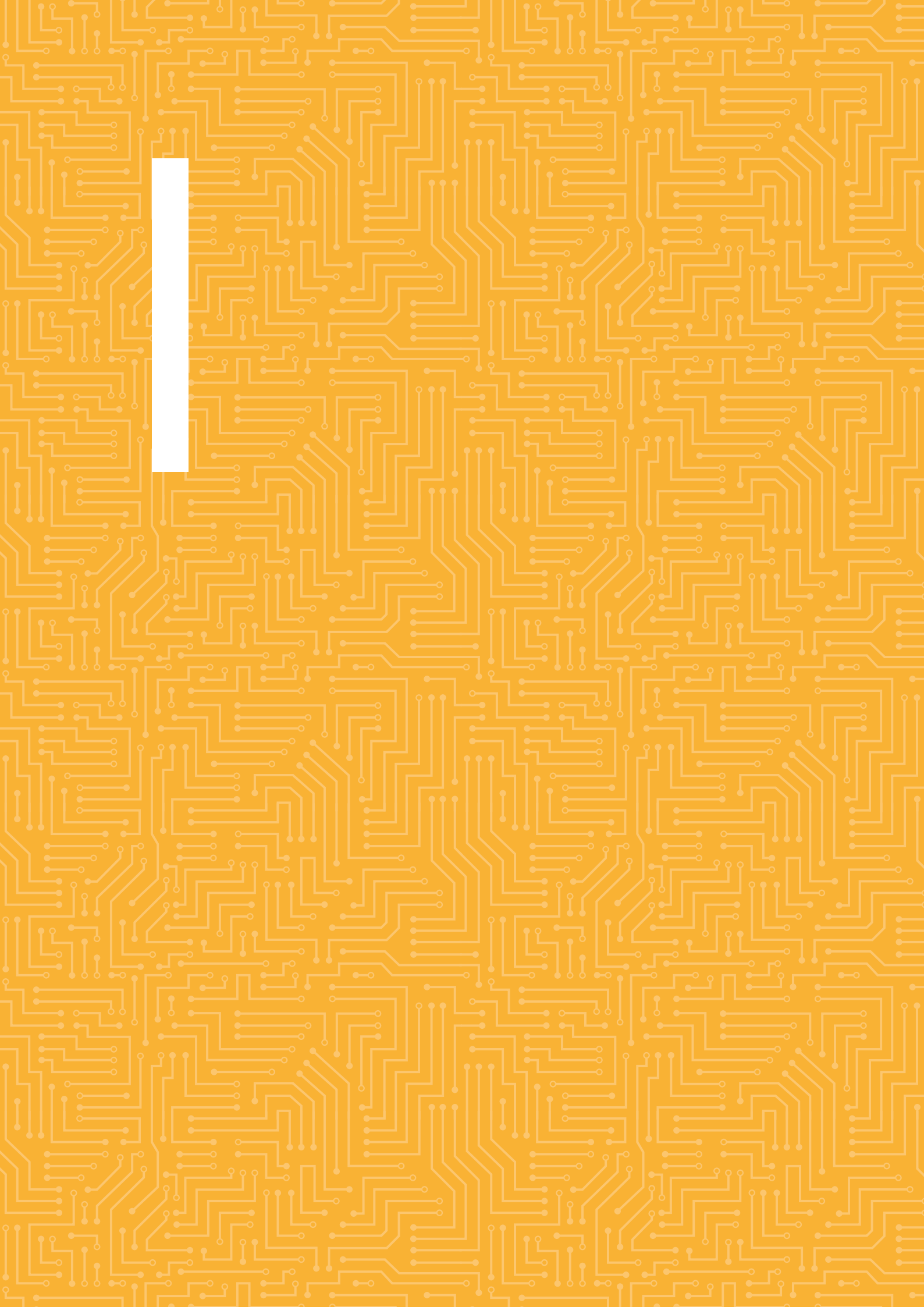
Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policymakers would be able to define early mitigation strategies that improve the EU's resilience 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 objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge is clearly needed. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.





# SECTION I

## GENERAL CONTEXT

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

The European Union Agency for Cybersecurity's (ENISA) annual threat landscape (ETL) <sup>(1)</sup> for 2023 marks the 11th iteration of this flagship report and was published in October 2023. ETL 2023 looked at threats across EU and the world in the period starting July 2022 and finishing in July 2023. According to ETL 2023, distributed denial of service (DDoS) and ransomware rank the highest among the prime threats, with social engineering, data-related threats, information manipulation, supply chain and malware following. Moreover, there has been a rise in threat actors professionalising their as-a-service programmes, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extorting them, advancing their illicit enterprises. In ETL 2023, it was observed that threat actor groups have an increased interest and exhibit an increasing capability in supply chain attacks by using employees as entry points. Threat actors will continue to

target employees with elevated privileges, such as developers or system administrators. In addition, information manipulation as a key element of Russia's war of aggression against Ukraine has become prominent, whereas in 2022–2023 internet shutdowns and the complexity of DDoS attacks were at an all-time high.

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

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

---

1- ENISA Threat Landscape 2022 — ENISA (europa.eu)

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 Member States (MSs). It is in the context of such challenges that ENISA is exploring ways to improve this reporting of incidents. Directive (EU) 2022/2555 (the second network and information systems directive (NIS2)) is changing and harmonising the way cybersecurity incidents are notified. The new provisions will aim to support a better mapping and understanding of the relevant incidents.

### **NIS INVESTMENTS 2023**

The ENISA NIS investments study aims at providing policymakers with evidence to assess the effectiveness of the existing EU cybersecurity framework specifically through data on how operators of essential services (OES) and digital service providers (DSP) identified under the NIS directive (NISD) invest their cybersecurity budgets and how the NISD has influenced this investment. The present report, to be published in November 2023, marks the fourth iteration of this report focusing on NIS investments. OES or DSP in the EU earmarks 7.1 % of its IT investments for information security (IS), while the average value is 7.6 %. When analysing this normalised dataset with historically available data, an increase of 0.4 % is observed compared to the median IT spending in 2021. This is still lower than the 2020 figures where the median IS vs IT spend ratio was 7.7 %. Still, any historical

analysis must be done while considering the slight differences in the samples between the years of study and the differences in the macro environment.

When looking at cybersecurity skills and resources, the security domain with the most information security (IS) full-time equivalents (FTEs) is cybersecurity operations with 40 % of the IS FTEs, followed by IT security architecture and engineering with 23 % of the IS FTEs, and cybersecurity governance and risk management with 21 %. Cybersecurity operations also comes out as the security domain with the most anticipated hires over the next 2 years (56 %), followed by IT security architecture and engineering (42 %) and cybersecurity governance and risk (36 %). For organisations with a specific IS budget, the median training budget is €100 000, with an average of €333 000 influenced by larger organisations with bigger budgets. In 2024 the Commission will carry out an assessment and issue a recommendation to the Management Board (MB) regarding the extension of the mandate of the Executive Director (ED). The current mandate of the ED ends in October 2024.

### **POLICY CONTEXT**

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





Policy file	Status of policy file	Background and ENISA role / plans
The EU Cybersecurity Act	Amendment	<p>On 18 April 2023, the Commission proposed a targeted amendment to the EU CSA (ENISA's founding regulation).</p> <p>The proposed targeted amendment aims to enable, by means of Commission implementing acts, the adoption of European cybersecurity certification schemes for 'managed security services'. This is in addition to ICT products, services and processes, which are already covered under the CSA. Such security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents.</p> <p>There is a link between the proposed amendment to the CSA and the proposal for a cyber solidarity act published by the Commission as part of the same package, as the EU Cybersecurity Reserve is envisaged to consist of trusted Managed Security Service Providers.</p>
NIS2	Adopted	<p>The European Parliament and the Council of the European Union approved legislation that sets clearer rules for entities in a wider range of sectors. NIS2 reinforces and extends the existing approach under the NIS1 directive, strengthening and streamlining the cybersecurity risk management and incident reporting provisions, and extending the scope by adding additional sectors, such as space or telecom (important for securing satellite communications, a vital infrastructure in remote rural areas, but also as a fail over in times of a natural disaster or military conflict). NIS2 underlines the special role of telecoms as a highly mature sector, a conduit for cyberattacks, and a possible filter, protecting less mature and harder to protect sectors such as health care. In addition, the NIS2 ambitions need to be supported, for instance to improve incident reporting, to create a better situational picture, of vulnerability disclosure policies and an EU vulnerability database, of supply chain security and other coordinated EU-wide cybersecurity risk assessments, including expanding the scope in terms of sectors covered, and of 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. MSs have 21 months to transpose NIS2 into national law and to implement it. In parallel, ENISA is developing its service and expertise for this with the introduction of service catalogue based on existing NIS1 expertise that is reflected in this single programming document (SPD).</p> <p>ENISA is already invested in activities linked to the development and implementation of NIS2, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the implementation of the directive in the coming years, using existing resources and building on these wherever necessary.</p>



Policy file	Status of policy file	Background and ENISA role / plans
Regulation on digital operational resilience for the financial sector (DORA)	Adopted	In parallel with NIS2, in December 2022 the Parliament and the Council adopted DORA (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector). The regulation aims to ensure that all participants in 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 cyberattacks and other risks. The regulation aims to ensure that all participants in 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 cyberattacks and other risks. DORA requires financial entities to ensure that they can withstand all types of ICT-related disruptions and threats. ENISA is actively supporting the mapping of cyber legislation initiatives in the finance sector and works closely with the Commission and relevant EU bodies on cybersecurity aspects of DORA including crisis management, incident reporting and information sharing.
Cyber diplomacy toolbox	Adopted	In addition, to support MS and European institutions, bodies and agencies (EUIBAs) in deterring and responding to cyberattacks from non-EU countries, the EU adopted a framework for a joint EU diplomatic response to malicious cyber activities, in the Council conclusions of 19 June 2017 <sup>(2)</sup> . The European External Action Service (EEAS) recently published updated implementation guidelines for the cyber diplomacy toolbox detailing specific steps MSs could take <sup>(3)</sup> . The guidelines underline the importance of measures taken by MSs under the NISD to improve resilience, the role of ENISA in establishing information-sharing channels with industry to gain situational awareness, and the importance of cooperation between the Cyber Crisis Liaison Organisation Network (EU-Cyclone), the Computer Security Incidence Response Team (CSIRT) network, ENISA, the Computer Emergency Response Team for EU institutions, bodies and agencies (CERT-EU) and the European Union Agency for Law Enforcement Cooperation, and EEAS Single Intelligence Analysis Capacity, to ensure that internal and external EU initiatives are coherent.

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

<sup>(3)</sup> Revised Implementing Guidelines of the Cyber Diplomacy Toolbox – 10289/23.

Policy file	Status of policy file	Background and ENISA role / plans
The EU Cyber Solidarity Act	Proposal	<p>On 18 April 2023, the Commission proposed the EU cyber solidarity act, to improve the preparedness, detection and response to cybersecurity incidents across the EU.</p> <p>The EU cyber solidarity act aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The proposal includes (a) the deployment of a pan-European infrastructure of security operations centres ('European Cyber Shield') to build and enhance common detection and situational awareness capabilities; (b) the creation of a Cyber Emergency Mechanism to support MSs in the preparation for, response to and immediate recovery from significant and large-scale cybersecurity incidents, including supporting preparedness measures, creating an EU cybersecurity reserve and supporting mutual assistance; and (c) the establishment of a Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents.</p> <p>The EU Cyber Shield and the Cyber Emergency Mechanism of this regulation will be supported by funding under the 'Cybersecurity and Trust' strategic objective of the Digital Europe programme, the founding regulation of which is amended accordingly via the cyber solidarity act proposal.</p> <p>ENISA's proposed role in the implementation of the cyber solidarity act is outlined in a number of articles. This includes ENISA being consulted in the identification of sectors/subsectors for which coordinated preparedness testing should be conducted. Furthermore, ENISA – in cooperation with the NIS Cooperation Group (NIS CG), the Commission and the High Representative of the Union for Foreign Affairs and Security Policy – shall develop common risk scenarios and methodologies for the coordinated testing exercises, and ENISA may be entrusted with the operation and administration of the EU Cybersecurity Reserve, in full or in part, funded through a contribution agreement from the Commission. ENISA is also intended to play a role in preparing a mapping of the services needed, as well as a similar mapping to identify the needs of third countries eligible for support from the EU Cybersecurity Reserve. In addition, requests for support from the EU Cybersecurity Reserve shall be transmitted to the Commission and ENISA, and ENISA – in cooperation with the Commission and the NIS CG – shall develop a template to facilitate the submission of requests for support. ENISA may also be requested to prepare agreement templates and, at the request of the Commission, EU-CyCLONe or the CSIRTs network, ENISA shall review and assess threats, vulnerabilities and mitigation measures with respect to a specific significant or large-scale cybersecurity incident, after which ENISA shall deliver an incident review report to the CSIRTs network, EU-CyCLONe and the Commission to support them in carrying out their tasks.</p>

Policy file	Status of policy file	Background and ENISA role / plans
Artificial Intelligence act	Proposal	<p>With the EU's artificial intelligence (AI) agenda advancing rapidly following the Commission proposal on AI <sup>(4)</sup> and 2021 coordinated plan on artificial intelligence <sup>(5)</sup>, the EU is addressing the major technological, ethical, legal and socioeconomic challenges to put AI at the service of people in the EU 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 the availability, safety or resilience of future AI services and applications.</p> <p>Building on ENISA's efforts towards securing AI / machine learning, the agency may continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2024. For this, ENISA will systematically monitor existing initiatives from the MSs in this area and continue supporting the Commission and MSs by providing good security practices and guidelines.</p>
Cybersecurity Regulation for EUIBAs	Proposal	<p>In March 2022, the Commission proposed a new regulation <sup>(6)</sup> with rules to increase cybersecurity in all EU institutions, by establishing a governance framework for all EUIBAs, including the identification of specific functions and responsibilities (e.g. local cybersecurity officer), the development of a maturity assessment and a cybersecurity plan to monitor the implementation of appropriate and proportionate security measures, the creation of an Interinstitutional Cybersecurity Board in charge of monitoring the implementation of the regulation as well as overseeing the priorities of CERT-EU, enabling easier information sharing on cyber threats and improving the efficiency of measures 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, vulnerabilities and incidents.</p> <p>A proposed regulation <sup>(7)</sup> on IS in the institutions, bodies, offices and agencies of the EU was also put forward earlier in 2022 to create a minimum set of IS 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 MSs, based on standardised practices and measures to protect information flows. The regulation will also be applicable to ENISA and will require that the agency take measures to further enhance its own cybersecurity posture.</p>

<sup>(4)</sup> Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts (COM(2021) 206 final).

<sup>(5)</sup> <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>

<sup>(6)</sup> Cybersecurity – [Uniform rules for EU institutions, bodies and agencies \(europa.eu\)](https://europa.eu)

<sup>(7)</sup> 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)

Policy file	Status of policy file	Background and ENISA role / plans
<p>Cyber Resilience Act (CRA)</p>	<p>Proposal</p>	<p>In her 2021 State of the Union address, President von der Leyen underlined that the EU should strive to become a leader in cybersecurity, announcing in that context a new CRA. The act would add in particular to the existing baseline cybersecurity framework of NIS2 and the CSA. The act, with its EU cybersecurity certification framework, proposes the establishment of common European cybersecurity requirements for products with digital elements that are placed on the internal market, by introducing mandatory essential requirements for products with digital elements and obligations for manufacturers, importers and distributors (e.g. vulnerability handling). Products with digital elements create opportunities for EU economies and societies. However, they also lead to new challenges – when everything is connected, a cybersecurity incident can affect an entire system, disrupting economic and social activities.</p> <p>The CRA proposal was published on 15 September 2022. The proposed scope currently includes 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.</p> <p>The CRA proposal sets out a role for ENISA in the implementation of the act. ENISA's proposed role includes receiving notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents that have an impact on the security of those products, preparing a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements, at the request of the Commission. Conducting evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, proposing joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance of products and submitting information relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level to EU-CyCLONe. Depending on the tasks assigned to ENISA based on the final adopted text of the CRA, significant additional resources may be required.</p> <p>ENISA has provided expert opinion in the preparation process for the CRA proposal, including, through its Cybersecurity Policy Observatory, in support of the impact assessment that accompanied the proposal and will also provide support in later stages (post-impact assessment) by contributing to elements of the legislative proposal such as risk categorisation, security requirements and, notably, to the preparation of the standardisation process, as well as in relation to the interplay between the CRA and certification schemes based on the CSA.</p>

Policy file	Status of policy file	Background and ENISA role / plans
Network Code on Cybersecurity	Proposal	<p>The Network Code on Cybersecurity aims to set sector-specific rules for the cybersecurity of cross-border electricity flows across MSs. 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 the Commission's request to the European Network of Transmission System Operators for Electricity 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 organisational measures. The code contains many references to and sets out new leading and supporting tasks for ENISA, among others the facilitation of an early warning system, support for the Agency for the Cooperation of Energy Regulators in monitoring the implementation of the code and support for the European Network of Transmission System Operators for Electricity and EU Distribution System Operators entity with organising sector-specific exercises.</p>
Horizontal Rule – Part IS	Adopted	<p>This sectorial legislative initiative consists of a new implementing regulation and a new delegated regulation regarding IS management systems for organisations and competent authorities (Horizontal Rule – Part IS).</p> <p>It also introduces amendments (through one implementing act and one delegated act) to the already existing Regulations (EU) No 748/2012, No 1321/2014, 2017/373, 2015/340, No 139/2014, No 1178/2011, No 965/2012 and 2021/664. The purpose of these amendments is to introduce requirements to comply with the IS management requirements introduced in the new implementing and delegated regulations, and to add the elements necessary for the competent authorities to perform their certification and oversight activities.</p> <p>The objective is to efficiently contribute to the protection of the aviation system from IS risks, and to make it more resilient to IS events and incidents. Specifically, the Horizontal Rule introduces additional rules to fill in existing gaps in the policy framework in order to address the safety impact of IS risks in a comprehensive and standardised manner across all civil aviation domains.</p> <p>ENISA is currently contributing to the activities of the working groups established to support the implementation of the regulation, e.g. concerning the development of acceptable means of compliance and guidance material.</p>

Policy file	Status of policy file	Background and ENISA role / plans
<p>Other:</p> <ul style="list-style-type: none"> <li>• eIDAS 2 regulation</li> <li>• Delegated Regulation on cybersecurity under the Radio Equipment Directive</li> <li>• Data Act</li> <li>• Chips Act</li> <li>• DSA</li> <li>• DMA</li> <li>• European Health Data Space</li> </ul>	<p>Proposal</p>	<p><b>eIDAS 2 regulation</b></p> <p>Digital identity and trust services are crucial for the EU digital market because they allow citizens and businesses to carry out transactions online in a safe and trusted way. In 2020, the Commission reviewed the electronic identification and trust services for electronic transactions in the internal market (eIDAS) regulation (Regulation (EU) No 910/2014) and identified factors hindering the adoption of electronic identification mechanisms. In June 2021, the Commission made a proposal for a revised regulation establishing a European digital identity framework and a European digital identity wallet (EUDIW), to be available for all EU citizens on a voluntary basis and usable for online transactions not only with government entities, but also with businesses. In the 2024–2026 period, ENISA will support MSs and the Commission with the development of the European digital identity framework and the EUDIWs, as set out in the regulation establishing a framework for a European digital identity in addition to promoting the exchange of good practises and capacity building of relevant stakeholders. The regulation establishing a framework for a European digital identity also expands the list of qualified trust services with electronic attestations of attributes, distributed ledgers and electronic archiving and management of remote devices for the creation of electronic signatures and seals. NIS2 states that the cybersecurity obligations laid down in this directive should be considered complementary to the requirements imposed on trust service providers under the eIDAS regulation. ENISA will support MSs and the Commission with this transition, to ensure that the trust service providers and the national authorities can benefit from the NIS2 ecosystem.</p> <p><b>Delegated Regulation on cybersecurity under the Radio Equipment Directive</b></p> <p>The Commission adopted Delegated Regulation (EU) 2022/30 for certain categories of radio equipment to increase its level of cybersecurity (protection of networks, privacy and protection from fraud).</p> <p>The Commission has issued a standardisation request to the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (Cenelec) to develop relevant harmonised standards in support of the EU requirements on cybersecurity of radio equipment. In this respect, it has been established that the aforementioned European standardisation organisations will have to ensure coherence of the developed harmonised standards with the EU cybersecurity certification schemes developed by ENISA, since they can have the same scope, such as internet-of-things devices or 5G network equipment. Therefore, cooperative work between ENISA and the standardisation organisations is envisaged.</p> <p><b>Chips Act</b></p> <p>On 8 February 2022, the Commission proposed a comprehensive set of measures for strengthening the EU's semiconductor ecosystem, the European chips act <sup>(8)</sup> 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 key digital technologies joint undertaking, and a recommendation to MSs promoting measures to monitor and mitigate disruptions in the semiconductor supply chain. Supply chain security, including cybersecurity aspects, is an important cross-cutting issue for stakeholders.</p>

<sup>(8)</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Chips Act for Europe (COM(2022) 45 final), 8 February 2022; Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) (COM(2022) 46 final), 8 February 2022; COM(2022) 782. Commission Recommendation (EU) 2022/210 of 8 February 2022 on a common Union toolbox to address semiconductor shortages and an EU mechanism for monitoring the semiconductor ecosystem (OJ L 35, 17.2.2022, p. 17)

## NON LEGISLATIVE POLICY DEVELOPMENTS

### ENISA cybersecurity support action

During the course of 2023 ENISA has developed and implemented the cybersecurity support action to support MSs in the short term in view of the immediate and elevated threat of malicious cyber activities due to the ongoing Russian war of aggression against Ukraine. This mechanism aims to complement and not duplicate efforts by MSs and those at the EU level to increase the level of protection and resilience against cyber threats by assisting MSs in their efforts to improve their capability to respond to cyber threats and incidents. It provides them with knowledge and expertise and increases preparedness in key sectors. The Commission has indicated that ENISA would continue the cybersecurity support action with a further contribution agreement of EUR 20 million in 2023, with an agreement for implementation and finalising by 31 December 2026 <sup>(9)</sup>. The work programme now includes a specific activity earmarked to undertake the cybersecurity support action, highlighting the objectives, outputs and resourcing foreseen during 2024 and taking into account lessons learned from the implementation in 2023.

### EU crisis management framework

The EU cybersecurity sector does not yet have a common space to work together across different communities and fields which allow the existing networks to tap into their full potential. The recent geopolitical situations confirmed the need for a joint response from the MSs and the EU institutions, bodies, offices and agencies to incidents and cyberattacks and to build on the work started in Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit for a coordinated response to incidents and crises and the Council conclusions of 19 October 2021 on the EU coordinated response to large-scale cybersecurity incidents and crises, and Commission Recommendation (EU) 2017/1584.<sup>(10)</sup>

ENISA will contribute by enhancing the EU cyber crisis management framework following NIS2 and the latest Council recommendation of 8 December 2022

on an EU-wide coordinated approach to strengthen the resilience of critical infrastructure, and taking into consideration both the blueprint and the Joint Cyber Unit recommendations, in line with and according to the roles defined in the ongoing discussions among MSs and EU operational actors.

### Cyber Defence Policy

In November 2022 the Commission and the High Representative, Josep Borrell Fontelles, put forward a joint communication <sup>(11)</sup> on an EU cyber defence policy and an action plan to enhance cooperation and investments in cyber defence to better detect, deter, protect and defend against a growing number of cyberattacks. Areas under consideration requiring potential support from ENISA include building preparedness and response measures across the EU, such as the testing of essential entities operating critical infrastructure for potential vulnerabilities based on EU risk assessments, as well as incident response measures to mitigate the impact of serious incidents and to support immediate recovery and/or restore the functioning of essential services. The Council conclusions of 22 May 2023 on the EU policy on cyber defence emphasise the importance of establishing mutual beneficial cooperation between this centre and other EUIBAs, in particular ENISA and CERT-EU, and invites MSs to exchange information on best practices to develop a skilled cybersecurity workforce with the support and expertise of ENISA.

### Cybersecurity Skills Academy

On 18 April 2023, as part of a cyber package, the Commission adopted a communication on the Cybersecurity Skills Academy inviting actors to take action to close the cybersecurity workforce skills gap. The academy aims at fostering knowledge generation through education and training by working on a common language on cybersecurity role profiles and associated skills, namely the European cybersecurity skills framework (ECSF), and also including pilots for attestation schemes for cybersecurity competences; ensuring a better channelling and visibility of available funding opportunities for skills-related activities in order to maximise their impact; calling on stakeholders to take action by making concrete cybersecurity pledges and integrating cybersecurity skills into their national strategies; defining indicators

<sup>(9)</sup>- The contribution agreement is being finalised. Dates and amount are currently estimated.

<sup>(10)</sup> <https://eur-lex.europa.eu/legal-content/en/aLL/?uri=CELEX:32017H1584>

<sup>(11)</sup>- [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_22\\_6642/IP\\_22\\_6642\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_6642/IP_22_6642_EN.pdf)



to monitor the evolution of the market and to better address the needs on one hand, and on the other, the offer of training, as well as the better directing of funds towards cybersecurity needs.

### **Implementation of the EU cybersecurity certification framework**

ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework by preparing the candidate schemes and supporting their maintenance once adopted. It is supported in this task by area experts and operates in collaboration with the National Cybersecurity Certification Authorities (NCCAs) in the MSs. It is expected that the draft candidate cybersecurity certification schemes proposed by ENISA will be adopted by Commission implementing regulations. The adopted schemes will allow for the conformity assessment of digital products, services and processes in the digital single market under those schemes, which can contribute to increasing the level of stakeholder trust in digital solutions in the EU. Currently, ENISA has prepared a candidate cybersecurity certification scheme in line with common criteria which is currently being considered for voting in the committee of the dedicated implementing act by the Commission and the MSs, likely by Q4 2023. Following this, the draft candidate cybersecurity certification scheme on cloud services will be submitted to the European Cybersecurity Certification Group (ECCG) for its opinion and adoption in committee will likely follow.

Furthermore, an ad hoc working group (AHWG) has been supporting ENISA in drafting the candidate cybersecurity certification scheme for 5G networks. Finalising the candidate schemes for specialised product categories under the EU common criteria scheme and for cloud services is just the first step and will likely bring about benefits in terms of recognition and trust across public services, business and citizens during the period starting in 2024.

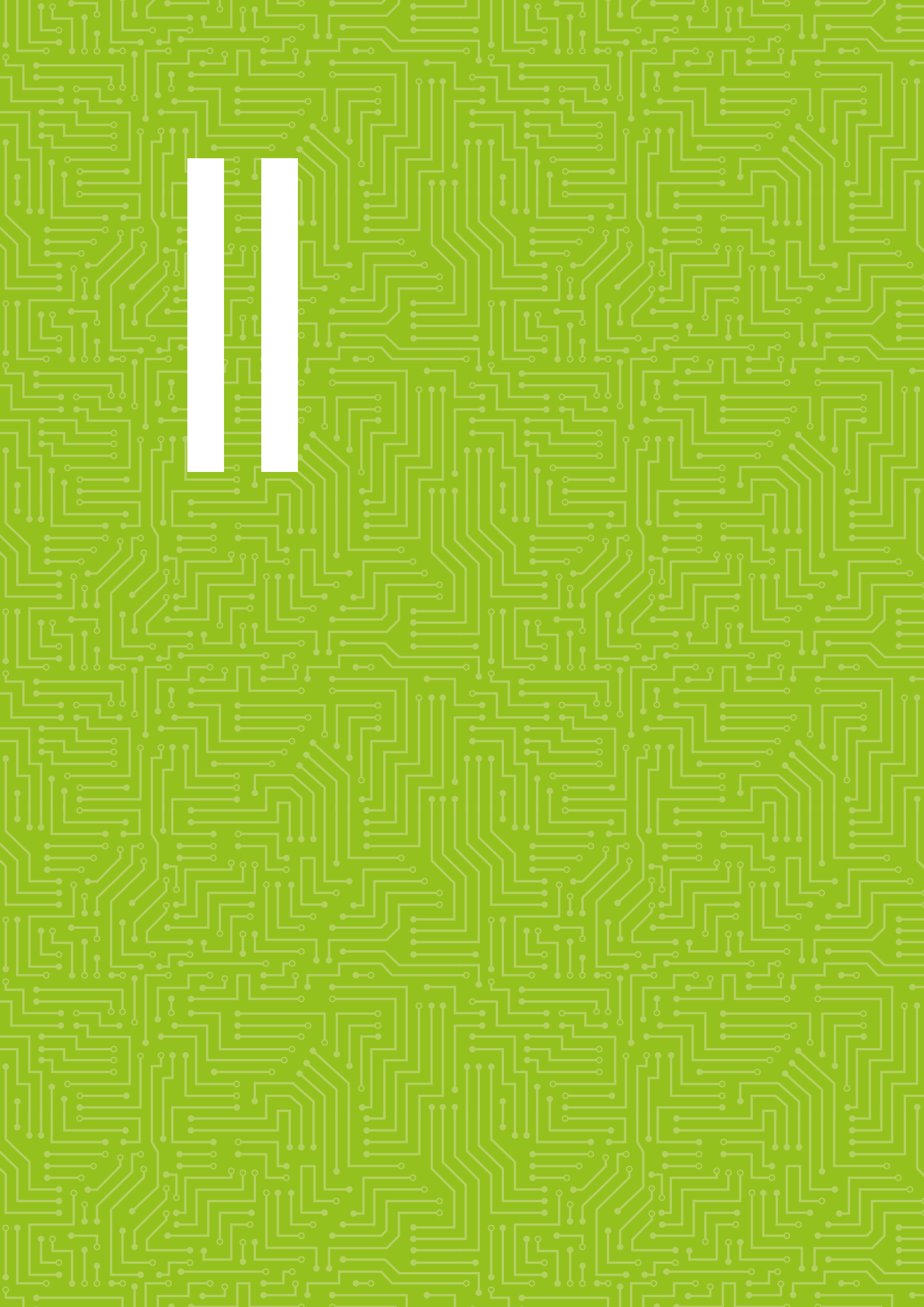
In relation to the digital identity framework, ENISA continues to support the development of a certification strategy matching the expectations, which requires MSs to issue an EUDIW based on common technical standards following mandatory conformity assessment and the voluntary nature of certification within the European cybersecurity certification framework, as stipulated in the CSA. This strategy shall make the best reuse of existing

relevant cybersecurity certification schemes under development and seeks to identify potential new certification iterations of schemes likely to contribute to the certification of the EUDIW. ENISA is currently responding to a request from the Commission for support with respect to the EUDIW.

ENISA will also support the development of certification means that would allow the demonstration of compliance with certain requirements of Article 21 of the NIS2 directive, as this regulation stipulates that MSs may require entities to use particular ICT products, services and processes, either developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.

In terms of the Union rolling work programme that is pending publication by the Commission, ENISA stands ready to support the Commission with the current and future editions of the programme. The adopted schemes will also be mapped with the requirements of the CRA to provide the means for the conformity assessment of digital products, services and processes in the digital single market, in a way that ensures compliance with the CRA requirements can also be attested. This approach sets the stage to for other legal instruments on cybersecurity to use the synergetic effects of the cybersecurity certification framework. ENISA is currently responding to a request from the Commission for support with respect to CRA.





## SECTION II

# MULTIANNUAL PROGRAMMING 2024–2026

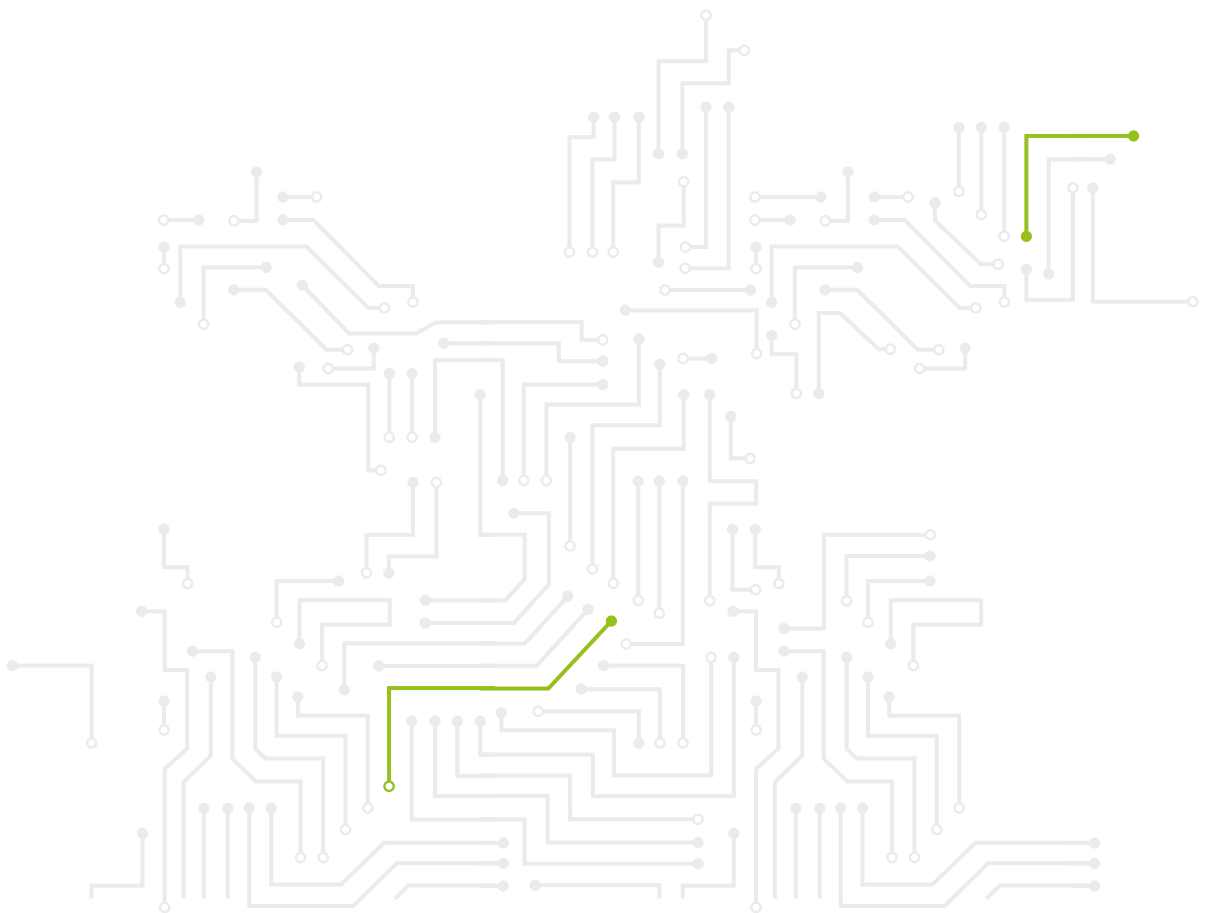
For decades, Europe has taken steps to improve digital security and trust through policies and initiatives. The MB of ENISA adopted a new strategy for the agency in June 2020, which builds on the CSA and outlines how the agency will strive to meet the expectations of the cybersecurity ecosystem from a medium- to long-term perspective, in a manner that is open, innovative, agile, and 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 make Europe more secure. Most importantly, the ENISA strategy outlines seven strategic objectives which are derived from the CSA and which set the expected medium- to long-term goals for the agency.

### 2.1. MULTIANNUAL WORK PROGRAMME

The following table maps the strategic objectives stemming from ENISA’s strategy <sup>(12)</sup> against the respective articles of the CSA. It also 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 by the ENISA MB as from 1 July 2024.

---

<sup>(12)</sup>- The ENISA strategy entered into force on 31 July 2020 and the MB shall launch a review procedure, if relevant, as from 1 July 2024.



(18) Large scale and cross border.

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	Indicator
<b>SO1</b> <b>Empowered and engaged communities across the cybersecurity ecosystem</b>	Activities 1-10	Articles 5-12	<p>Empowered ecosystem encompassing MS authorities, EUIBAs, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure.</p> <p>An EU-wide, state-of-the-art body of knowledge on cybersecurity concepts and practices, which builds cooperation among key actors in cybersecurity, promotes lessons learned and EU expertise, and creates new synergies</p>	<p>The % gap between demand and supply of cybersecurity skilled professionals.</p> <p>General level of cybersecurity awareness and cyber hygiene among citizens and entities <sup>(13)</sup>.</p>
<b>SO2</b> <b>Cybersecurity as an integral part of EU policies</b>	Activities 1 and 2	Article 5	<p>Cybersecurity aspects are considered and embedded across EU and national policies.</p>	<p>Uptake of policy recommendations adopted within the biennial report on the state of cybersecurity in the EU <sup>(14)</sup>.</p> <p>Effectiveness of EU relevant policy initiatives taking cybersecurity into consideration.</p>
			<ul style="list-style-type: none"> <li>• Consistent implementation of EU policy and law in the area of cybersecurity</li> <li>• EU cybersecurity policy implementation reflects sectoral specificities and needs</li> <li>• Wider adoption and implementation of good practices</li> </ul>	<p>Level of maturity of cybersecurity capabilities and resources across the EU at the sector level <sup>(15)</sup>.</p>
<b>SO3</b> <b>Effective cooperation amongst operational actors within the Union in case of massive <sup>(16)</sup> cyber incidents</b>	Activities 4, 5a and 5b	Article 7	<ul style="list-style-type: none"> <li>• All communities (EU institutions and Member States) use a rationalised and coherent set of standard operating procedures (SOPs) for cyber crisis management</li> <li>• Efficient tools and methodologies for effective cyber crisis management</li> </ul>	<p>Level of cooperation and availability, utilisation and trust of EU level networks, tools and databases.</p>
			<ul style="list-style-type: none"> <li>• MSs and institutions cooperating effectively during large-scale, cross-border incidents or crises</li> <li>• Public informed on a regular basis of important cybersecurity developments</li> <li>• Stakeholders aware of current cybersecurity situation</li> </ul>	<p>The risk level due to cyber threats is understood and decision-makers are able to prioritise resources to manage the risk.</p>
			<p>Improve MS capabilities to respond to cyber threats and incidents</p>	<p>EU level of preparedness and response to large-scale cross-border incidents.</p>

<sup>(13)</sup> Article 18(1), point (c), of NIS2.

<sup>(14)</sup> As part of the report on the state of cybersecurity in the EU, ENISA 'shall include particular policy recommendations with a view to addressing shortcomings and increasing the level of cybersecurity across the Union' (Article 18(2) of NIS2).

<sup>(15)</sup> As part of the report on the state of cybersecurity in the EU in Article 18(1), point (e), of NIS2.

<sup>(16)</sup> Large scale and cross border.

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	Indicator
<b>SO4</b> <b>Cutting-edge competences and capabilities in cybersecurity across the Union</b>	Activities 3 and 9	Article 6 and Article 7 (5)	<ul style="list-style-type: none"> <li>Enhanced capabilities across the community</li> <li>Increased cooperation between communities</li> </ul>	<p>Aggregated assessment of the level of cybersecurity capabilities in the public and private sectors across the EU <sup>(17)</sup>.</p> <p>Aggregated assessment of the level of maturity of national cybersecurity capabilities and resources as well as the extent to which MS national cybersecurity strategies are aligned <sup>(18)</sup>.</p>
		Articles 10 and 12	<ul style="list-style-type: none"> <li>Greater understanding of cybersecurity risks and practices</li> <li>Stronger European cybersecurity through higher global resilience</li> </ul>	<p>The % gap between demand and supply of cybersecurity skilled professionals.</p> <p>General level of cybersecurity awareness and cyber hygiene among citizens and entities.</p>
<b>SO5</b> <b>High level of trust in secure digital solutions</b>	Activities 6 and 7	Article 8	<ul style="list-style-type: none"> <li>Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework versus schemes' requests and schemes' adopted.</li> <li>Smooth transition to the EU cybersecurity certification framework</li> <li>Certified ICT products, services and processes are preferred by consumers/industry and where relevant, OES or DSP under the NIS1 directive, and entities within the scope of NIS2</li> </ul>	Citizens trust in ICT certified and non-certified solutions in the EU market.
			<ul style="list-style-type: none"> <li>Contribution towards understanding market dynamics</li> <li>A more competitive European cybersecurity industry, small and medium-sized enterprises (SMEs) and start-ups</li> </ul>	Monitor metrics such as number of certificates issued under an EU scheme; number of companies interested in EU certification; growth observed in the number of conformity assessment bodies (CABs) or EU certification functions thereof recorded in the MS.

<sup>(17)</sup> As part of the report on the state of cybersecurity in the EU in Article 18(1), point (b), of NIS2.

<sup>(18)</sup> As part of the report on the state of cybersecurity in the EU in Article 18(1), point (e), of NIS2.

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	Indicator
<b>S06</b> <b>Foresight on emerging and future cybersecurity challenges</b>	Activities 10 & 8	Articles 9 and 11	<ul style="list-style-type: none"> <li>• Research and development of cybersecurity technology reflecting the needs and priorities of the EU.</li> <li>• Funding the development of cybersecurity technologies that meet the EU's ambition to become more resilient, autonomous and competitive..</li> </ul>	Overall EU investment in research and innovation (R & I) activities addressing emerging cybersecurity challenges.
<b>S07</b> <b>Efficient and effective cybersecurity information and knowledge management for Europe</b>	Activity 8	Article 9	<ul style="list-style-type: none"> <li>• Decisions about cybersecurity take into consideration information and knowledge concerning the current and evolving cybersecurity threat landscape</li> <li>• Stakeholders receive relevant and timely information for policy- and decision-making.</li> </ul>	EU-level cybersecurity risk assessment and cyber threat landscape (adopted in accordance with Article 18(1) point a) NIS2

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

**Community mindset.** 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 its working environment, as well as the expectations of its stakeholders.

**Responsibility.** ENISA takes 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.

These 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 encapsulated into two corporate objectives, which form the baseline from which the multiannual activities of the SPD will be delivered.

## ENISA CORPORATE STRATEGY

ENISA's corporate vision is to make available a contemporary and attractive workplace for all, based on trust and inclusion, while developing and transforming itself into a dynamic, service-oriented organisation, an organisation that continuously improves its operational and administrative efficiency by redesigning its operational and administrative processes, and optimising its structures, services and use of resources. ENISA aims to ensure that it does the right things (effectiveness) in the right way (efficiency) and capitalises efficiency gains before reinforcing any area of work with extra resources. In order to address this vision, the ENISA corporate strategy sets forth objectives with environment, social and governance criteria in mind, across three

interconnected strategic dimensions, which will drive the agency and guide the development of its corporate objectives, activities and resource planning: people-centric approach, sustainable governance and service delivery.

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

The strategy aims to accelerate the tendency towards flexibility and digitalisation of the workplace so that it becomes a key factor in the transition to a green administration, by ensuring that staff work in a green and sustainable work environment. ENISA

will continue to enhance its secure operational environment, aiming at the highest level compatible with its mission and responsibilities, and strive towards excellence in its infrastructure services based on best practices and frameworks. ENISA will also explore cloud-enabled services that are fit for purpose and provide services in accordance with recognised standards.

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

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

Strategic dimension	Objectives	Activity's to achieve objectives	Key goals (KPIs/means to measure the KIs)
<b>People centric organisation</b>	Effective workforce planning and management	Activity 13	<ul style="list-style-type: none"> <li>• Agency's internal workforce needs for the year n until n+2 are defined and presented to the MB together with the first draft SPD for those years as per annual/internal procedures..</li> <li>• Effective FTEs used for SPD activities (as reported in annual activity report (AAR) by end of year n) do not diverge from planned FTEs in SPD (as endorsed by MB in the beginning of year n) by more than 5 % according to annual/internal procedures..</li> <li>• 95 % of agency's staffing posts (temporary agent (TA), contract agent (CA), seconded national expert (SNE)) are filled by the end of the year according to its annual recruitment results</li> <li>• Vacated staff posts are fulfilled in less than 300 days according to its annual recruitment results.</li> <li>• All assignments of staff are reviewed regularly every 3 years during the agency's annual/internal procedures.</li> <li>• Aggregate loss of FTE across the agency due to absences (excluding long-term sick leave) is less than three FTEs annually during its annual/internal process</li> </ul>
	Efficient talent acquisition, development and retainment	Activity 13	<ul style="list-style-type: none"> <li>• Agency has established clear competency targets in line with its established needs and has reviewed them in an annual appraisal exercise.</li> <li>• All selection criteria used for the published and internal vacancies are solely based on established competencies described in the annual/recruitment process.</li> <li>• Agency's proficiency levels across target competencies have increased over the set period according to annual appraisal exercises.</li> <li>• 50 % of agency's established workforce needs are addressed through internal talent development (including internal mobility, competitions and appointment) according to its annual internal process.</li> <li>• Jobholder satisfaction with the guidance and support received from their reporting officers in achieving learning and development goals is high according to the biennial staff satisfaction survey.</li> <li>• High level of staff satisfaction with learning opportunities offered and knowledge-sharing options according to the biennial staff satisfaction survey.</li> <li>• High level of positive peer-review assessments in career development reports in the annual internal process.</li> </ul>
	Caring and inclusive modern organisation	Activity 13	<ul style="list-style-type: none"> <li>• High aggregate staff satisfaction with psychological safety level according to annual staff satisfaction survey.</li> <li>• High aggregate staff satisfaction with workspace and related services according to biennial staff satisfaction survey.</li> <li>• Agency obtains EU Agencies Network Certificate of Excellence in Diversity and Inclusion by the end of 2025 according to external audit and certification process.</li> <li>• High level of satisfaction with agency's workplace integration, wellness and health programmes, engagement and community mindset for staff according to annual staff satisfaction survey.</li> <li>• Staff stress level is decreasing from 2022 levels and is sustained at low levels after 2025 according to annual staff satisfaction survey.</li> </ul>



Strategic dimension	Objectives	Activity's to achieve objectives	Key goals (KPIs/means to measure the KIs)
<b>Service centric organisation</b>	Ensure efficient corporate services	Activities 11 & 13	<ul style="list-style-type: none"> <li>• High satisfaction with essential corporate support services found through an annual MT survey.</li> <li>• High satisfaction with demand driven or optional corporate support services found through an annual MT survey.</li> <li>• Number of procurement procedures merged, combined or used in interinstitutional FWCs found through an annual internal procedure.</li> <li>• The percentage of staff (measured in FTEs) engaged in shared corporate service activities within the Agency found through an annual internal procedure.</li> <li>• The percentage of staff (measured in FTEs) engaged in shared corporate service activities beyond the Agency with other EUIBAs (under SLAs, MoUs or other arrangements) found through an annual internal procedure</li> </ul>
	Introduce digital solutions that maximise synergies and collaboration within the Agency	Activities 11 & 13	<ul style="list-style-type: none"> <li>• Implement (replace or develop) at least five user-centered, cloud-based, corporate solutions or tools fit for purpose and in line with ENISA's IT strategy and relevant business needs by Q4 2025.</li> <li>• Limited disruption of continuity of services across all corporate support service areas measured by annual assessment.</li> <li>• To have IT support service standards as technical KPIs in place by Q2 2025 and to have them continuously monitored and observed, to support the maintenance and development of operational IT systems through an annual review.</li> <li>• All on-premises systems are maintained within risk levels established by the business owners and all corrective measures recommended by periodic risk assessments are implemented as found in an annual review.</li> </ul>
	Continuous innovation and service excellence	Activity 11	<ul style="list-style-type: none"> <li>• The percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have not been reviewed less than 3 years ago as found by an annual review.</li> <li>• Percentage of corporate rules (MB and ED decisions), processes (SOPs) and policies which have been last reviewed more than 4 years ago as found in an annual review.</li> </ul>
	Developing service propositions with additional external resourcing	Activities 11 & 13	<ul style="list-style-type: none"> <li>• At least three SLAs signed and in operation with EUIBAs covering ENISA's operational services with additional resourcing from beneficiaries by 2025.</li> </ul>

Strategic dimension	Objectives	Activity's to achieve objectives	Key goals (KPIs/means to measure the KIs)
<b>Sustainable organisation</b>	Ensure ENISA is climate neutral by 2030	Activity 11	<ul style="list-style-type: none"> <li>Acquire an eco-management and audit scheme (EMAS) certificate by Q4 2023.</li> <li>50 % of participants in ENISA's organised events and meetings to participate online by 2025, rising to 75 % by 2030.</li> <li>50 % of ENISA events and meetings to be organised as hybrid or online by 2025, rising to 75 % by 2030.</li> <li>Initiate and by the end of 2024 agree a tripartite MoU with the Hellenic Authorities and the landlord of the ENISA headquarters (HQ) building to reduce the climate impact of the HQ building at least 40 % by 2029, by installing solar panels on the non-classified part of the building, or procure a green building for the agency by then.</li> <li>Offset all residual emissions generated through ENISA operations from 2024 onwards.</li> </ul>
	Promote and enhance ecologic sustainability across all the Agency's operations	Activities 11 & 13	<ul style="list-style-type: none"> <li>Recycle all ENISA residual waste created in its HQ and local offices by 2025.</li> <li>Implement ecological sustainability and climate neutrality criteria for procuring event management and support and for facilities management and support services from external contractors by 2025.</li> <li>Implement ecological sustainability and climate neutrality criteria for all ENISA tenders for corporate service contractors by 2027 and by 2029 for operational activities.</li> <li>Understand best practices in sustainable IT solutions, define an agency-wide approach and include it in the IT Strategy.</li> </ul>
	Develop efficient framework for continuous governance to safeguard high level of IT and physical security	Activity 11	<ul style="list-style-type: none"> <li>Review the Agency's IT strategy and align it with the objectives of the corporate strategy by Q3 2024.</li> <li>Put in place a relevant policy for security compliance for IT and for physical security (including for required EUCI levels) for all relevant internal and external services with a high level of adherence to this KPI from 2025 onwards.</li> <li>The agency should be in a position to handle EUCI at the level of SECRET UE/EU SECRET and be accredited as being able to do so by Q4 2024.</li> <li>20% of the total IT budget to be allocated to information security proportional to the level of risks across various IT systems within the Agency by Q4 2024.</li> <li>Implement relevant security requirements and criteria for all relevant ENISA tenders for corporate services by Q1 2025.</li> </ul>

## 2.2. HUMAN AND FINANCIAL RESOURCES – OUTLOOK FOR 2024–2026

### 2.2.1. Overview of the past and current situations

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

#### 2.2.1.1. Recruiting new talent and increasing operational capacities

The agency has taken significant strides to improve the fulfilment of its establishment plan, with the rate increasing from 77 % in 2019 to 87 % in 2022 and to 96 % as at 1 September 2023. It is expected to increase to 100 % by the end of 2023 (not including possible resignations) <sup>(19)</sup>. This is despite the increasing competition for cybersecurity talent <sup>(20)</sup> and – compared to the private sector and the living standard of more economically advanced MSs – the

uncompetitive overall salary and support package which the agency can offer.

In parallel, the agency has also taken persistent measures over the past 3 years to rebalance the allocation of posts towards operational units in expense of corporate units. This follows the reorganisation of the agency under the direction of MB Decision No MB/2020/9, in accordance with which all support and corporate functions (including administrative and secretarial support) were concentrated in corporate units from 1 January 2020 onwards, leaving in operational units only the posts with a purpose entirely linked with operational tasks and functions (Title II Chapter II in the CSA).

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

**Table 1.**

Allocated staff policy plan posts	01.01.2021	%	01.01.2022	%	01.01.2023	%
Operational units	70	59.3	78	61.9	90	70.3
Corporate units	44	37.3	37	29.4	36	28.1
unallocated <sup>(21)</sup> (of which reserve)	4(2)	3.4	11(9) <sup>(22)</sup>	8.7	2(0)	1.6
TOTAL	118	100	126	100	128	100

#### 2.2.1.2. Utilising internal and external synergies

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

#### Identifying priorities and de-prioritisation of actions in the 2024 work programme.

The agency sought guidance from the MB for its 2024 work programme during strategic discussions at the MB meeting in June 2023. The MB members were requested to identify which areas of its work programme ENISA should act on more versus those that it should act on less, based on the lessons learned from the 2022 annual activity report. The

<sup>(19)</sup>- Individual sets of KPIs have been introduced since 1 January 2023 to all managers to ensure rapid fulfilment of all open posts allocated to the unit.

<sup>(20)</sup>-Demand for skilled professionals in the field of cybersecurity is growing, with [some estimates of the Joint Research Centre](#) pointing to a shortage of 1 million cybersecurity employees within the EU and 3.5 million worldwide.

<sup>(21)</sup>- Including two posts held by the ED and the Accounting Officer.

<sup>(22)</sup>-Includes posts which became available after the adoption of NIS2 in late November 2022.

current draft of the work programme has taken the strategic guidance from the MB into consideration and resources have been allocated according to the feedback received. The negative priorities of reduced scope, suppressed outputs and/or postponed projects amount to a shortfall in resources of EUR 3.8 million and 15 FTEs for the 2024 work programme.

**Shared operational functions and partnerships.**

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

**Shared administrative and corporate services and partnerships.**

On 20 December 2022, the agency signed an SLA to create synergies with the ECCC in the field of R & I as well as in administration, namely accounting, data

protection and IS. Shared service agreements are currently in place with the European Union Intellectual Property Office and with the European Centre for the Development of Vocational Training (Cedefop) to streamline procurement, shared financial services, human resources and IT solutions, and in the area of data protection. The agency will continue to build upon its shared services strategy and upon the partnership model with other EUIBAs.

**2.2.1.3. Current resource gaps and challenges**

In 2022, the agency was able to rise to the challenge posed by the Russian war of aggression against Ukraine, partially thanks to additional budgetary resources allocated by the Commission in response to the call of the informal council in Nevers to establish and expand ENISA support services dramatically. However, the additional funds did not include any additional posts to its establishment plan or staff policy plan, forcing ENISA to internally reallocate its human resources. To meet these challenges, the agency was also forced to suppress outputs set out in the original draft 2023–2025 SPD, postpone projects and/or reduce the scope of projects in 2023, due to budgetary shortfall of more than 3 million.

**Table 2.**

Budget implementation	2020 <sup>(23)</sup>	%	2021 <sup>(24)</sup>	%	2022	%
Voted budget	21 149 120	100.00	22 833 060	100.00	24 207 625	100.00
Additional budget	-	-	-	-	15 000 000	63.57
Total budget	21 149 120	100.00	22 833 060	100.00	39 207 625	163.57
Implemented budget	20 588 320	97.35	22 721 149	99.51	39 179 406	100.00

<sup>(23)</sup> ENISA Annual Activity Report 2020, <https://www.enisa.europa.eu/publications/corporate-documents/enisa-consolidated-annual-activity-report-2020>.

<sup>(24)</sup> ENISA Annual Activity Report 2021, <https://www.enisa.europa.eu/publications/corporate-documents/enisa-annual-activity-report-2021.pdf>.

In 2022, the agency received few additional FTEs to address new tasks. Firstly, for tasks foreseen in NIS2, the resources which were approved constituted a slight increase of budget EUR 610 000 per year and five new posts (a 4 % increase). It should be noted, however, that most MSs have responded to NIS2 by significantly increasing the staff numbers of their national cybersecurity agencies, and though ENISA does not fulfil the regulatory duties like national agencies do, the allocated appropriations fall far short of the initial needs which the agency put forward during consultations with the Commission (10–12 posts). Nor were the final additional resources qualitatively fit for purpose – the agency requested higher grades of posts, given the high level of new tasks requiring specialised expertise. However, the new posts were graded as entry level.

Secondly, recognising its growing need to have increased capabilities to support operational cooperation, resilience and capabilities at the EU level, and expand the scope of relevant services which

ENISA offers to the MSs, the Commission has taken two steps. Firstly, it allocated two additional SNE posts to ENISA to facilitate operational cooperation with MSs and, in 2023, injected an additional EUR 15 000 000 to ENISA to scale up and expand its ex ante and ex post services to the MSs (tasks related to Articles 6 and 7 of the CSA) in response to the higher threat due to Russian aggression. Both these steps should be acknowledged and welcomed. However, both in terms of human resources and in terms of budget, those additional resources are insufficient compared to the scale of the task or the level of demand for ENISA services. Preliminary lessons learned from the implementation of the cybersecurity support action were presented to the MB during the MB meeting in June, highlighting that the actual FTE allocation for the 2023 ENISA support action was 20 % to 30 % higher than originally estimated (around 15 FTEs) and as such adequate resourcing will need to be reflected in the potential continuation of the cybersecurity support action during and after 2024.

### 2.2.2. Outlook for the years 2024-2026

The 2021–2027 multiannual financial framework laying down the EU's long term budget could not foresee the cumulative effect that the rapidly deteriorating cybersecurity threat landscape – including due to the Russian war of aggression which increased the EU's attack surface and presented new challenges to managing supply-chain security – and new legislative initiatives such as NIS2, the proposed CRA, DORA, etc. will have on ENISA's ability to meet the ever-increasing demands with its limited resources.

The agency was only able to fulfil its operational mandate in response to Russian aggression partially thanks to additional budgetary resourcing stemming from the cybersecurity support action, but did not receive any significant additional posts to its establishment plan. Thus, with the long term outlook of the EU threat landscape remaining bleak, the agency cannot, under its current normal budgetary and human resource limits, maintain even this minimum level of support going forward without jeopardising its other priorities, such as increasing assistance to the EU and MSs to support the transposition of NIS2 or support actual deployment of new certification schemas.

Secondly, though welcome in substance, no new resources have been given to the agency within legislative proposals of the Commission that nevertheless provide new tasks for ENISA. For example, within the CRA proposal, which is currently undergoing co-decision procedures, despite the fact that the Commission estimated that ENISA would need about 4.5 FTEs to fulfil these new tasks, the Commission suggested they be reallocated from existing resources, e.g. that ENISA would deprioritise other activities. In parallel, in the cyber solidarity act proposal, the Commission again estimates that new assignments need about 7 FTEs to be implemented and again propose that these 7 FTEs are reallocated from existing resources of ENISA, which should then

be deprioritised. In addition, numerous sectorial proposals or commitments (DORA referring to ENISA 14 times, the Electricity Code referring to ENISA 32 times regarding tasks, declarations with non-EU countries <sup>(25)</sup>, etc.) rightly try to leverage ENISA expertise in upgrading the cybersecurity posture of other sectors, policies or partners. However, those proposals do not acknowledge that even this would mean that the agency must then dedicate time and expertise – e.g. human capital – to fulfil these expectations, putting a further strain on the agency's limited resources.

Acknowledging ENISA's exceptional operational mandate, the Commission has indicated its desire that ENISA continue the cybersecurity support action with a further contribution agreement of EUR 20 000 000 in 2024 with an agreement for finalising on 31 December 2025. While ENISA in the short term demonstrated the required agility and flexibility to perform such new tasks, if they potentially become permanent ENISA should also be entrusted with additional resources, in the form of allowing it to temporarily surpass the CA post levels foreseen in the staff policy plan, in order to execute the support action efficiently without drastically deprioritising resources from other activities.

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

---

(25) Tirana Declaration, 6 December 2022, EU–Western Balkans Summit, Paragraph 26: 'As cyber threats know no borders, we will work together to enhance our collective cyber security. Recent large scale cyber-attacks demonstrate the need for enhanced engagement, building on existing programmes and on cooperation with the EU Agency for Cybersecurity (ENISA).

### 2.2.3. Resource programming for the years 2024 -2026

#### 2.2.3.1. Financial resources

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

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

These factors mean that the agency's operational budget (Title III) without the potential additional funds for the support action will not be maintained at the 2023 level and will decrease approximately 16.93 %

(from the 2023 level). The identified impacts are detailed under each activity in the draft SPD.

#### 2.2.3.2. Human resources

The MB has mandated the agency to highlight in its SPD those parts of the conclusions of the 2022 AAR, which together with the recent Commission's legislative initiatives indicates significant resource constraints which the agency will face in the multiannual programming period. The current establishment plan foresees no change in the number of posts allocated to ENISA (82 posts), although the agency has been entrusted and is expected to be further entrusted with new and enhanced tasks. Therefore, the agency has undertaken a thorough assessment of its internal human resourcing needs for the programming period of 2024–2026, taking into account the near-term expected legislative and political developments, as well as the heightened level of threat of the cybersecurity landscape<sup>(26)</sup>. While the agency acknowledges that this overall initial assessment of a 44.5 FTE gap compared to existing resources due to new tasks and developments should be further clarified, it points out that the critical and highly critical FTE needs related to current additional tasks reflected in its 2022 AAR and new legislative tasks within the programming period (2024–2026) amount to the equivalent of 21 FTEs.

As highlighted in the 2022 AAR adopted by the MB, a total of 10.5 FTEs were transferred from other work programme activities to deliver the support action in preparation for its implementation over the course of 2023. This represented 15.9 % of the total operational human resource used by ENISA in 2022. As a result, ENISA had to deprioritise and/or scale down other activities in 2023, and the expected continuation of the support action into 2024 and 2025 would result in ENISA needing to keep deprioritising its operations in other areas for the duration of the multiannual programming period, to be able to retain the human resourcing the support action requires.

The outcome of legislative processes might also put further strain on ENISA's human resources during the

<sup>(26)</sup> Following the decision of the MT of ENISA to conduct the internal workforce needs assessment for 2023–2025, the heads of unit (HoU) and permanent team leaders (TLs) were requested to put forward their initial analysis in three parts. Firstly, by indicating main challenges which affect their unit/team in implementing the annual and multiannual objectives and priorities enshrined in the draft SPD of 2023–2025, and if relevant linking those challenges with reported gaps or shortcomings within the adopted 2021 AAR or the comments from MB members during the discussion in June 2022. Secondly, they were requested to define the medium- and long-term needs of their units and teams by outlining the main legislative, political and cybersecurity developments and trends and how these overall challenges will change the tasks and responsibilities of the unit/team for the coming years (2023, 2024, 2025), and assessing the overall human resources needs in the long term (n+3) including key competences (maximum five) that the unit should develop/strengthen (on the basis of the existing ENISA competencies map). Finally, they were requested to define additional functions which the unit/team should be able to perform in the short term (n+1), indicating the competencies (and their level) which are intrinsic to those functions. They were also requested to indicate whether to fulfil new functions via internal mobility or recruitment and put forward proposals on how to restructure or suppress existing functions within the unit/team if the additional resource requests cannot be addressed by the agency..



forthcoming multiannual programming period and would require the agency to scale down its current operational activities even further, as noted above in Section 2.2 'Outlook for the years 2024–2026'.

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

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

Though the agency has actively pursued, and will continue to pursue, a number of avenues to build and exploit efficiency gains internally and also externally by developing joint operational and administrative services with other EUIBAs (CERT-EU, the ECCC, eu-LISA, Cedefop and the EU Agencies Network (EUAN)), the efficiencies actually gained from these joint approaches – in terms of freed-up FTEs – will, and also in the future, cover only a fraction of the assessed shortfalls in additional FTE needs.

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

Thus, by the end of 2024, if the already-announced legislative and political expectations towards the

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

Article 38.2 of the ENISA Financial Rules allows the opportunity to 'offset the effects of part-time work'. ENISA will explore this option in 2024 and may use this option in the future to offset long-term absences and part-time work with short term CA contracts.

#### **2.2.4. Strategy for achieving efficiency gains**

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

##### **2.2.4.1. Strategy to achieve operational efficiency gains**

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

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



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

**Activity 2:** the MoU with the European Railway Agency is planned for signing in Q4 2023 and an extension of the current MoU with the European Banking Authority and others to align ENISA's support for MSs under the critical sectors of NIS2. Activities of the EU bodies in these sectors is also planned, to facilitate the exchange of good practices with OECD nations and other EU policy initiatives under implementation.

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

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

**Activities 6 and 7:** formalisation of a cooperation arrangement with CEN–Cenelec and the European Telecommunications Standards Institute and a joint cybersecurity market observatory with the ECCC.

**Activity 8:** Working together with the three DORA European supervisory authorities (the European Banking Authority, European Securities and Markets Authority and European Insurance and Occupational Pensions Authority) concerning the implementation of incident reporting under DORA and its alignment with the corresponding NIS2 requirements. In the context of the EU–US cyber dialogue, relevant workstream

on incident reporting with US counterparts (the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency) to map relevant initiatives. Regular discussions with Eurostat and the Commission concerning the implementation and operationalisation of the EU cybersecurity index and its comprising qualitative and quantitative indicators.

**Activity 9:** developing joint objectives (with relevant programming KPIs) with the ECCC to help to tackle the skills gap in cybersecurity under the ECSF as foreseen in the Commission's communication on 'European Cybersecurity Skills Academy'. In addition, utilising the new cooperation arrangements with the Cybersecurity and Infrastructure Security Agency, the North Atlantic Treaty Organization and Ukraine to enrich EU cybersecurity knowledge and information.

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

The agency continues to implement its work programme by the systematic use of its statutory bodies (the National Liaison Officers (NLO) Network and the ENISA Advisory Group), as well as other statutory groups ENISA is involved in (the Stakeholder Cybersecurity Certification Group (SCCG) as set out in Article 22 of the CSA, the NIS CG and its workstreams, and expert groups created under EU law) and its own ad hoc expert groups, where appropriate to avoid duplication of efforts, build synergies, and peer-review the scope and direction of measures taken by the agency to implement its SPD outputs, as well as to validate the results. In this way the agency will fulfil its obligation as outlined in Article 3(3) of the CSA, to avoid the duplication of MS activities and taking into consideration existing MS expertise. Hence, all activities listed under Section 3.1. and 3.2. in this SPD contain an indication of how specific deliverables and other measures taken to fulfil the outputs will be validated and peer-reviewed or consulted on with relevant external experts.

### 2.2.4.2.. Strategy to achieve corporate and administrative efficiency gains

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

The corporate strategy (including HR strategy) presents a vision for a contemporary, flexible and values-driven organisation that empowers staff to deliver outstanding results for people across the EU and beyond. This strategy addresses ENISA's ambition to perform at the highest level in the interests of Europeans and the needs of its staff members to have an attractive workplace and a fulfilling career where excellence and effort are rewarded. Founded on Commission strategies and practices <sup>(27)</sup>, ENISA will strive to maximise the efficiency of its resources by maintaining its focus on developing a flexible, highly skilled and fit-for-purpose workforce that will support ENISA's goals to enhance its capabilities in future-readiness and continue its path towards an agile, knowledge-based and matrix organisational structure. This strategy aims to accelerate the tendency towards flexibility and digitalisation of the workplace so that it becomes a key factor in the transition to a green administration, by ensuring that staff work in a green and sustainable work environment. The strategy also aims to enhance personal accountability, responsibility and growth, and sets out a common vision in which all staff will work in a trust-based environment through the introduction of new technologies that facilitate modern and flexible work practices.

As ENISA aspires to become a trusted partner at the EU level, it will continue to provide customer-focused, multi-disciplinary teams that demonstrate a customer-centric, can-do and agile attitude. Open and dynamic workspaces, matrix type operational set ups and collaborative IT tools will facilitate an integrated culture that will be able to act rapidly to increasingly complex policy challenges beyond the remit of a single service or unit. While the strategy reflects ENISA's broader corporate and long-term vision, it is also aligned with and supported by ENISA's internal control framework (ICF), which is designed to provide reasonable assurance regarding the achievement of objectives set out in ENISA's financial regulation and retain credibility with the Commission

and MSs. While implementing the path in this direction, ENISA will need to review and redesign its processes, policies and SOPs, promote self-service functionalities and build on collaborative ways of working, while redesigning job roles and investing in staff development. The founding principles of the strategy will be implemented via the SPD and annual work plans.

In order to enable the achievement of the above, the corporate strategy sets the following benchmarks which affect the agency's budgetary and human resource planning in 2024–2026:

- The agency's investment into talent development is a minimum 4 % of expenditure foreseen for the salaries of staff in active employment;
- The agency's welfare (excluding medical) expenditure is at a maximum of 5 % of expenditure foreseen for the salaries of staff in active employment;
- The agency's expenditure on movable property and related costs for retaining a modern workplace is at a maximum of 1 % of expenditure foreseen for the salaries of staff in active employment;
- Corporate overhead which shall be budgeted from the expenditure of all operational activities to ensure technical support for essential corporate services shall not be higher than 7 % of the aggregated operational budget (Title III);
- The agency dedicates at least 20 % of its total investments to core, corporate and operational IT systems in order to ensure the cybersecurity of these systems;
- Starting from 2024, the agency will offset 100 % of its carbon dioxide (CO<sub>2</sub>), methane and nitrous oxide emissions (Approximately 150 tonnes) which will be generated across all its activities and as a result of its operations in the relevant budgetary period.

Beyond setting these benchmarks, the corporate strategy aims to ensure that the agency acts in the right way and exhaust efficiency gains before reinforcing areas of work with extra resources. Such initiatives should be seen as a holistic package and

<sup>(27)</sup> People first – Modernising the European Commission; Towards a Next Generation Digital Commission; Commission welcomes political agreement on the European Year of Skills – Employment, Social Affairs & Inclusion – European Commission; 2021–2027 strategy for the EUAN.

cover different pillars such as activity and resources/ service categorisation, capitalisation on shared services, strategic workforce planning, and business and service optimisation.

### 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 to anticipating and addressing staffing gaps in order to build agile workforce needs and allocate resources where priorities are. To do so, ENISA is revamping its internal strategic workforce planning framework, with the aim to consolidate 'hard' workforce data with 'soft' competency aspects, to 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 No MB/2020/9 are met, ENISA aims to identify the level of in-house resources in terms of numbers of staff and their skills and competences, review its job evaluation and job framework, and in general redesign its staffing policy while determining future workforce needs, based not only on workload indicators and workforce plans but also on 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 sector.

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

ENISA will introduce modern HR practices to support talent development as outlined in the corporate strategy, in particular prioritising the change and revision of some key MB decisions such as learning and development (L & D), middle management, appraisal and reclassification. It will further invest in building partnerships with accredited providers and in competency development for both technical and soft skills. In parallel, ENISA will further proceed with its pilot of 2023 in linking L & D with the results of multi-source feedback evaluation and provide and introduce a job complexity and job grade standards.

### Business process review and service optimisation

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

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

- Exploring and piloting changes in service levels and modalities, to improve added value and cost efficiency, such as shifting from owned to leased solutions or 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 productivity, by removing redundant steps and capitalising on new technologies such as making use of DG Digital Services' services and tools,
- Reviewing ICT infrastructure and related technologies to reduce duplication of components and optimise maintenance and

capital replacements, such as for storage, or move towards cloud-based solutions.

Besides the above, most of ENISA's administrative tasks are supported by EU tools such as accrual-based accounting (ABAC), and Sysper for human resource management, for missions and for document approvals and registry. Over the course of 2023, ENISA onboarded Advanced Records System, Missions Integrated Processing System, Public Procurement Management Tool (PPMT), ServiceNow as a key ticketing and service management tool, and an online recruitment platform, Allegro, as well as continuing to progress with onboarding Sysper modules, switching to a web-based ABAC platform and expanding the usage of ABAC functionalities. The agency has also started exploring to introduce new modules on contract management and redesign financial workflows via PPMT / Advanced Records System.

In 2023, the agency has continued supporting the EUAN in relation to the implementation of cybersecurity requirements proposed in the draft regulation on common binding rules on cybersecurity for EUIBAs, namely through a concept of shared services on cybersecurity risk management, such as the concept of a virtual chief information security officer. This concept is being developed in close cooperation with CERT-EU and another six EU agencies <sup>(28)</sup> that volunteered to join this initiative.

In its corporate functions, ENISA further seeks to rationalise its internal processes to improve its overall efficiency and to benchmark its activities with the best practices implemented by other EU institutions and agencies. In the area of facility management and security, in 2023 ENISA completed the review of facility and security service. In applying further efficiencies in the area, as of 2024 onwards, the agency aims to merge and simplify its administrative expense as a result of using a multitude of contracts and reduce the usage of FWCs by applying integrated service models for soft services (security and facility management and audio visual). This will be further supported by exploring additional modules of ServiceNow and integrating facility management and security requests via all-inclusive service packages.

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

### **Capitalising on shared services**

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

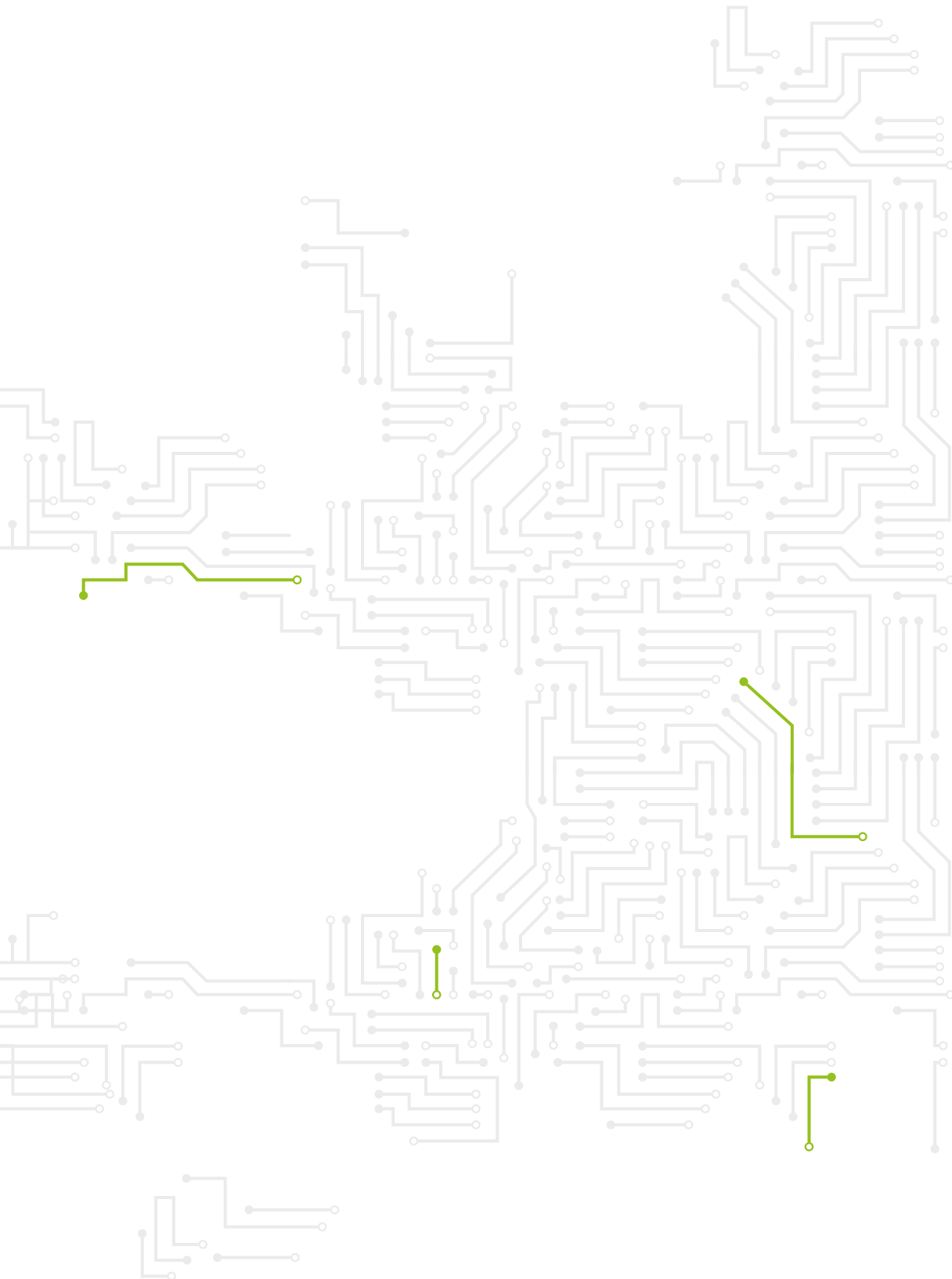
- Sharing services with other agencies and/or the Commission, including interagency and interinstitutional procurements, common services with Cedefop and the ECCC and use of Commission ICT solutions such as those for human and financial resources management; in particular sharing accounting and data protection with the ECCC as of January 2023.
- Explore further synergies with other EUIBAs in running joint calls and competitions of HR and engage in shaping job-sharing or secondment regimes with other EUIBAs;
- Prioritise the introduction of modern HR information systems and join forces with the Commission on the new HR transformation roadmap and other modern cloud-based solutions.
- Explore further synergies with the Paymaster's Office on reimbursement of experts and the European Personnel Selection Office on running calls and accessing reserve lists.
- Contributing to further promoting shared services among agencies through the

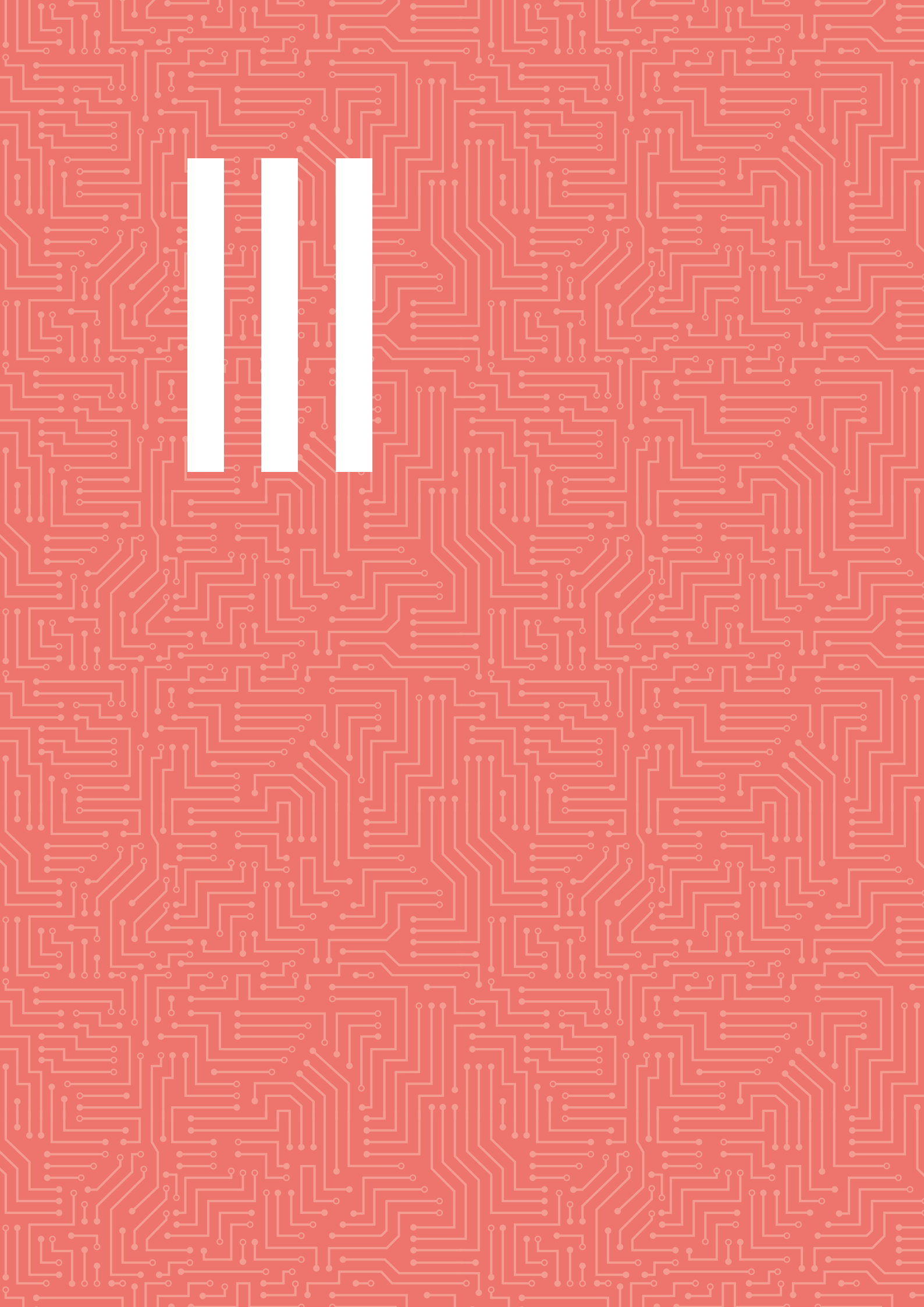
---

<sup>(28)</sup> eu-LISA, the European Training Foundation, the European Maritime Safety Agency, the European Public Prosecutor's Office, the European Institute of Innovation & Technology, Cedefop, CERT-EU and The Trans European Services for Telematics between Administrations System..

different networks, particularly in the areas of procurement, HR, ICT, risk and performance management, data protection, IS, accounting, etc.

- Contributing to the improvement and piloting of IT services with the Directorate-General (DG) for Human Resources and Security, and DG Digital Services in the area of HR and financial management;





## SECTION III

# WORK PROGRAMME FOR 2024

This is the main body of the work programme describing, per operational and corporate activity, what the agency aims to deliver in the respective year towards achieving its strategy and the expected results. In total, 11 operational activities and three corporate activities have been identified to support the implementation of ENISA's mandate in 2024.

The activities of the work programme seek to mirror and align with the tasks set out in Chapter 2 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's work programme. On 29 March 2022, the MT adopted ENISA's stakeholders strategy. This strategy lays down the main principles and approach towards stakeholders' engagement at the agency-wide level. The implementation of the stakeholders strategy is linked with the implementation of the 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' have a 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 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 KPIs and related metrics for measuring the performance of the activities. These metrics are set out in the SPD 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 formula, whereas qualitative metrics are those that are more of a subjective opinion based on the information received – however, even these are quantified in order to be interpreted and measured. The work programme for 2024 includes indicators for measuring strategic objectives, indicators and targets for measuring the activity objectives and indicators at the output level to measure the performance of the outputs. Many of the proposed indicators have been taken from the cybersecurity index pilot run by ENISA in 2022 and will eventually be superseded by NIS2 indicators to monitor high-level progress towards general objectives.



### 3.1. OPERATIONAL ACTIVITIES

## ACTIVITY 1: Providing assistance on policy development



#### Overview of activity



The activity seeks to bolster policy initiatives in novel/emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. ENISA will support the Commission and MSs on new policy initiatives <sup>(29)</sup> through evidence-based input into the policy development process. ENISA, in coordination with the Commission and MSs, will also conduct policy monitoring to support them in identifying potential areas for policy development based on technological, societal and economic trends, identify gaps, overlaps and synergies among policy initiatives under development, and also develop monitoring capabilities and tools to regularly and consistently be able to provide advice on the effectiveness of the existing EU policy and law in accordance with the EU's institutional competencies in the area via the cybersecurity policy assessment service.

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

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

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

#### Link to strategic objective (ENISA strategy)



- Cybersecurity as an integral part of EU policies

#### Indicator for strategic objectives



1. Uptake of policy recommendations adopted within the biennial report on the state of cybersecurity in the EU <sup>(30)</sup>.
2. Effectiveness of EU relevant policy initiatives taking cybersecurity into consideration

Activity Objectives	Csa Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
1. A Improve the effectiveness and consistency of EU cybersecurity policies	Art.5 CSA	2026	Assessment of ENISA advice and its influence on EU policy (stakeholder centric survey)	75 % stakeholder satisfaction from ENISA's advice and influence (among EU policymakers)

<sup>(29)</sup> Policy initiatives such as the CRA and the CSA as well as initiatives on AI, 5G, the Data Governance Act (DGA) / big data, data spaces, digital resilience and response to current and future crises.

<sup>(30)</sup> As part of the report on the state of cybersecurity in the EU, ENISA 'shall include particular policy recommendations with a view to addressing shortcomings and increasing the level of cybersecurity across the Union (Article 18(2) of NIS2).

OUTPUTS	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
1.1 Advise the Commission and MSs on reviewing the effectiveness of current cybersecurity policy frameworks	Stakeholders will use evidence to understand how implemented policies have affected the targeted entities	DG Communications Networks, Content and Technology NIS CG NLOs	Stakeholder satisfaction <sup>(21)</sup>	Biennial (Survey)	93%	>90%
			Number of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	21	30
1.2 Advise the EC and MS on new policy development, as well as carrying out preparatory work	Stakeholders will use ENISA's advice to develop effective and consistent EU cybersecurity policies	DG CONNECT and other DGs or EUIBAs depending on policy file owner.	Stakeholder satisfaction	Biennial (Survey)	93%	>90%
			Number of EU policies supported by ENISA	Annual (internal report)	7	5
			Number of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	21	30
1.3 Monitor and analyse new and emerging policy areas	Stakeholders are informed in a timely manner about gaps, overlaps and inconsistencies across EU policy initiatives under development	NLOs NIS CG DG Communications Networks, Content and Technology and other DGs or EUIBAs depending on the policy file owner	Stakeholder satisfaction	Biennial (Survey)	93%	>90%

## Stakeholders and engagement levels



**Partners:** DG Communications Networks, Content and Technology, other DGs and agencies, the NIS CG and relevant work streams, ENISA NLOs

**Involve / Engage:** OES and DSP under NIS1 and overall entities within the scope of NIS2 and industry associations/representatives, national competent authorities, other formally established groups

RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 1.1	INDEX, SITAW, NIS, CERTI	0.95	300 000	0.00	7 135	0.20	0	1.15	307 135
Output 1.2	NIS, CERTI	2.00	8 000	0.25	7 000	0.10	0	2.35	15 000
Output 1.3	NIS, CERTI	0.75	18 000	0.25	17 000	0.00	0	1	35 000
Activity total		FTE: 4.50 Budget: 357 135							
Actual resources used in previous year (2022)		FTE: 4.8 Budget: 354 406							

<sup>(21)</sup> Stakeholder satisfaction conducted every 2 years to measure the uptake of results / outcome, added value, duplication of ENISA work, etc. by stakeholders.

## ACTIVITY 2: Supporting implementation of Union policy and law



### Overview of activity



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

As part of this activity, ENISA provides support to the NIS CG, its workstreams and the implementation of its work programme. In this period the focus is on supporting the NIS2 transposition, the NIS2 implementing acts, and the implementation of new tasks under NIS2, like the EU registry for digital infrastructure entities. As part of this activity, ENISA also supports the EU risk evaluation processes (Nevers, Council cyber risk posture <sup>(32)</sup>), follows up on the 5G toolbox (a previous EU risk evaluation), delivers a methodology for EU risk evaluations and the building of sectorial risk scenarios, delivers sectorial situational awareness, and runs a yearly 360 degree survey (NIS360) for assessing maturity and criticality of sectors across the board.

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

Besides NIS2 implementation, activity 2 also provides support to MSs and EU institutions on the implementation of DORA, which is *lex specialis* in the finance sector, with the goal of aligning the NIS2 and DORA implementation. The agency also supports cybersecurity aspects of policy implementation in the areas of digital identity (electronic identification) and EUDIWs, the Network Code on Cybersecurity and the DGA, and covers holistically data protection and privacy issues.

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

### Link to strategic objective (ENISA strategy)



- SO2. Cybersecurity as an integral part of EU policies

### Indicator for strategic objectives



- Level of maturity of cybersecurity capabilities and resources across the EU at the sector level <sup>(33)</sup>

<sup>(32)</sup> [st09364-en22.pdf](#) (europa.eu)

<sup>(33)</sup> As part of the report on the state of cybersecurity in the EU in Article 18(1), point (e), of NIS2.

Activity Objectives	Csa Article And Other Eu Policy Priorities	Timeframe Of Objective	Indicator	Target
2.A Effective implementation of the NISD	Article 5 CSA and NIS2	First target: end 2024 and then continuously	• Cybersecurity index area 'Policy' – indicator 2.3 'Implementation of cybersecurity related directives'	• 75 % of MSs have implemented NIS2 by the end of 2024
2.B Improve maturity of NIS sectors	Article 5 CSA and NIS2	2026	• Average maturity of critical sectors • Average maturity of less critical sectors – source NIS360.	• One immature NIS1 sector increases maturity score • One mature NIS1 sector increases maturity score
2.C Improve alignment between NIS2 and DORA	Article 5 CSA	2026	• Level of alignment between main NIS2 provisions (incident reporting and security measures) and DORA provisions in survey of JC-DOR and NIS CG	• 75 % of respondents say NIS2 and DORA are aligned on these topics



#### OUTPUTS



#### Expected results of output



#### Validation



#### Output indicator



#### Frequency (data source)



#### Latest results



#### Target 2024

2.1 Support MSs and the Commission in the implementation of the NIS CG work programme and the NISD	MSs will use ENISA advice to implement the NISD.	DG Communications Networks, Content and Technology, NIS CG	Stakeholder satisfaction <sup>(24)</sup>	Biennial (Survey)	94%	>90%
			EU register for digital entities is used by all MSs	Biennial (Survey)	n/a	Used by all MS
			Coordinated vulnerability disclosure (CVD) guidance is implemented by MS and all MS are on the CVD map	Biennial (Survey)	n/a	Used by all MS
2.2 Support MSs with EU-wide risk evaluations and EU toolboxes scenarios	<ul style="list-style-type: none"> <li>Support EU-wide risk evaluations and risk scenarios</li> <li>Follow-up of previous EU-wide risk assessments (5G, Nevers)</li> <li>Sectorial situational awareness reporting</li> </ul>	DG Communications Networks, Content and Technology, NIS CG	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of stakeholders involved in the NIS360	Annual (internal count)	n/a	120
			Number of sectorial situational awareness reports	Annual (internal count)	6	12
2.3 Improve cybersecurity and resilience of the NIS sectors	Stakeholders use the NIS service packages to improve security and resilience of the sectors	DG Communications Networks, Content and Technology, NIS CG, sectorial DGs, sectorial EU agencies	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)	Annual (internal count)	3	4
			Number and frequency of services delivered to NIS sectors according to the maturity of the sector	Annual (internal count)	21	24

<sup>(24)</sup> Results/outcome taken up, added value, duplication of existing work, etc. and effectiveness of ENISA guidance in helping MSs implement their tasks and deliver the NIS CG work programme

## Stakeholders and engagement levels



**Partners:** DG Communications Networks, Content and Technology, NIS CG, national competent authorities, sectorial DGs, sectorial EU agencies

**Involve / Engage:** NLOs, OES and DSP under NIS1 and overall entities within the scope of NIS2 and industry associations/representatives

RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 2.1	NIS, SITAW	4.00	183 268	0.25	39 500	0.25		4.50	222 768
Output 2.2	NIS, SITAW, TREX	3.75	167 500	0.25		0.25		4.25	167 500
Output 2.3	NIS, SITAW, CERTI, TREX	3.00	330 000	0.50				3.50	330 000
Activity total	FTE: 12.25 Budget: 720 268								
Actual resources used in previous year (2022)	FTE: 9.75 Budget: 780 925								

## ACTIVITY 3: Building capacity



---

### Overview of activity



This activity seeks to improve and develop the capabilities of MSs, EUIBAs and various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the EU. 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 cybersecurity strategies.

Measures to support this activity include the organisation of large scale exercises, sectorial exercises and training <sup>(35)</sup>.

In addition, the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem including cross-border information sharing, and assist in reviewing and developing national and EU-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 Article 6 and Article 7(5) of the CSA.

Compared to the outputs under activity 3 of previous years, in 2024 due to reduced funds it was decided to suppress the following outputs.

- **Output 3.4.** Following the development of the risk management framework by ENISA, the next steps are following an iterative approach to review the framework and update it. This process may obviously also be carried out on a less frequent than annual basis.
- **Output 3.5.** In 2022 and 2023, the main role of ENISA was to support the Commission in launching the initiatives in support of security operation centres (SOCs). This activity has now been taken over mainly by the ECCC.

Regarding output 3.6, the addition of private sector sponsors supporting the activities of Team Europe allows ENISA to reduce the amount of spending in this domain.

---

<sup>(35)</sup> CSIRT trainings and 'capture the flag' and 'attach defence' competitions.

### Link to strategic objectives (ENISA STRATEGY)



- SO4: Cutting-edge competences and capabilities in cybersecurity across the Union

### Indicator for strategic objectives



- Aggregated assessment of the level of cybersecurity capabilities in the public and private sectors across the EU <sup>(36)</sup>
- Aggregated assessment of the level of maturity of national cybersecurity capabilities and resources as well as the extent to which MS national cybersecurity strategies are aligned <sup>(37)</sup>

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
3.A Increase the level of alignment and cooperation within and between MSs as well as sectors and EUIBAs	Articles 6 and 9 CSA	2024	<ul style="list-style-type: none"> <li>• Number of MSs that use ENISA support and tools for the implementation review and update of their national cybersecurity strategy.</li> </ul>	<ul style="list-style-type: none"> <li>• All MSs that have reviewed their national cybersecurity strategy use ENISA support and tools.</li> </ul>
3.B Prepare and test capabilities to respond to cybersecurity incidents	Article 6 CSA	2024	<ul style="list-style-type: none"> <li>• Proportion of beneficiaries who take part in relevant ENISA exercises and trainings</li> <li>• Added-value of ENISA exercises and training</li> </ul>	<ul style="list-style-type: none"> <li>• All MSs participate in Cyber Europe 2024</li> <li>• &gt;80 % of EUIBAs have participated in JASPER exercises over 3 years (number of participants in 2024 increases compared to 2023)</li> <li>• 90 % of participants see positive added value</li> </ul>
3.C Increase skill sets and align cybersecurity competencies	Article 6 CSA	2024	<ul style="list-style-type: none"> <li>• Assessment of average level of cybersecurity technical competences of participants in European cybersecurity challenge finals</li> <li>• Number of participants that take part in national competitions improving cybersecurity skills and capabilities</li> <li>• Level of alignment of cybersecurity competences across the EU</li> </ul>	<ul style="list-style-type: none"> <li>• A relevant metric is in the process of being developed in the ENISA security index</li> <li>• More than 10 000 participants take part in the annual 'capture the flag' competitions that are organised prior to the European cybersecurity challenge (ECSC) final</li> <li>• MS national competence frameworks are aligned with the ECSF</li> </ul>

<sup>(36)</sup> As part of the report on the state of cybersecurity in the EU in Article 18(1), point (b), of NIS2.

<sup>(37)</sup> As part of the report on the state of cybersecurity in the EU in Article 18(1), point (e), of NIS2.

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
3.1 Assist MSs to develop, implement and assess national cybersecurity strategies	<ul style="list-style-type: none"> <li>Increase the level of preparedness and cooperation</li> <li>Prepare capabilities to respond to cybersecurity incidents</li> <li>Increase skill sets</li> <li>Align cybersecurity competencies</li> <li>Improved national cybersecurity strategies</li> </ul>	NLO subgroup on national cybersecurity strategies	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			<ul style="list-style-type: none"> <li>Maturity of national cybersecurity strategies,</li> <li>information sharing and analysis centres (ISACs), SOCs, etc.</li> </ul>	Annual (Report)	n/a	n/a
3.2 Organise large scale biennial exercises and sectorial exercises	<ul style="list-style-type: none"> <li>Increase the level of preparedness and cooperation</li> <li>Prepare and test capabilities to respond to cybersecurity incidents</li> <li>Stakeholder test and improve capabilities and increase capacity</li> </ul>	<ul style="list-style-type: none"> <li>NLO Network (as necessary)</li> <li>CSIRTs Network (as applicable)</li> <li>EU-CyCLONe members (as applicable)</li> <li>NIS Cooperation Group (as applicable)</li> <li>EU ISACs (as applicable)</li> <li>NLO subgroup of Cyber Europe planners (as applicable)</li> </ul>	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Evaluation of capacity building actions by participants in exercises and trainings	Annual (report)	<ul style="list-style-type: none"> <li>40 % high usefulness</li> <li>53.5 % medium usefulness</li> <li>6.5 % low usefulness</li> </ul>	>50% high usefulness
			Number of participants in trainings and organized by ENISA	Annual (report)		>500 (incl online exercises)
3.3 Organise trainings and other activities to support and develop the maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS CG, EU-CyCLONe and work streams, ISACs and other communities	<ul style="list-style-type: none"> <li>Increase the level of preparedness</li> <li>Prepare capabilities to respond to cybersecurity incidents</li> <li>Increase skill sets</li> <li>Stakeholders improve capabilities and skill set</li> </ul>	<ul style="list-style-type: none"> <li>NLO Network (as necessary)</li> <li>CSIRTs Network (as applicable)</li> <li>EU-CyCLONe members (as applicable)</li> <li>NIS CG (as necessary)</li> <li>EU ISACs (as applicable)</li> <li>NLO subgroup of Cyber Europe planners (as necessary)</li> </ul>	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Number of participants in training and in challenges organised by ENISA	Annual (report)	n/a	>1 000 (including online training)
3.4 Organise and support cybersecurity challenges including the ECSC	<ul style="list-style-type: none"> <li>Align cybersecurity competencies</li> <li>Increase skill sets</li> </ul>	ECSC Steering Committee (NLO Subgroup)	Stakeholder satisfaction	Biennial (Survey)	91%	90%

## Stakeholders and engagement levels



**Involve / Engage:** Cybersecurity professionals, private industry sectors (OES such as health, transport, etc. or generally entities within the scope of NIS2), EU institutions and bodies, CSIRTs Network and related operational communities, European ISACs, EU-CyCLONe members, NIS CG, blueprint stakeholders, and SOCs, including national and cross-border SOCs



RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 3.1	TREX, INDEX	2.00	70.000	0,00	0	0.00	0	2.00	70 000
Output 3.2 <sup>(38)</sup>	TREX, NIS	3.35	500 000	0,00	0	0.00	0	3.35	500 000
Output 3.3	TREX	4.30	546 591	0,00	0	0.00	0	4.30	546 591
Output 3.4	TREX TREX	2.3	120 000	0,00	0	0.50	0	2.8	120 000
Activity total	FTE: 12.45 Budget: EUR 1 236 591 <sup>(39)</sup>								
Actual resources used in previous year (2022)	FTE: 10.32 Budget: EUR 1 921 221 <sup>(40)</sup>								

<sup>(38)</sup> By the end of 2023, ENISA expects to sign a new multiannual SLA with eu-LISA to provide support on exercises.

<sup>(39)</sup> In addition EUR 120 000 from SLA with eu-LISA (see Annex XI).

<sup>(40)</sup> Carried over into 2023: EUR 328 339.

## ACTIVITY 4: Enabling operational cooperation



### Overview of activity

The activity supports operational cooperation among MSs, EU institutions, bodies, offices and agencies and between operational activities. The main goal of the activity is to provide support and assistance in order to ensure the efficient functioning of EU operational networks and cyber crisis management mechanisms. ENISA, as mandated by NIS2, provides the organisational support and tools for both the technical (EU CSIRTs Network) and operational layer (EU CyCLONe) of EU operational cooperation networks. As part of 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 and the EU vulnerability database. Thus, this activity could also prepare some of ENISA's proposed tasks in coordinating information and notification about vulnerabilities at the EU level as outlined in the Commission's legislative initiative on CRA.

In addition, measures include facilitating synergies with and between the different national cybersecurity communities (including the civilian, law enforcement, cyber diplomacy and cyber defence communities) and EU actors – notably CERT-EU, the European Cybercrime Centre (EC3) and EEAS – with a view to exchanging know-how and best practices, providing advice and issuing guidance.

ENISA will contribute to the next steps in enhancing the EU cyber crisis management framework following NIS2 and the 2022 Council recommendation on an EU-wide coordinated approach to strengthen the resilience of critical infrastructure, complementing the EU coordinated response to large-scale cybersecurity incidents and crises. In addition, this activity supports the ENISA cybersecurity support action.

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

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

**Link to strategic objectives  
(ENISA STRATEGY)**



- SO3: Effective cooperation amongst operational actors within the Union in case of massive cyber incidents

**Indicator for strategic objectives**



- Level of cooperation and availability, (disruptions) and utilisation and trust of EU-level networks, tools and databases.

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
4.A. Enable trust and effective cooperation and operations of CSIRTs Network and EU-CyCLONE members.	Article 7 & NIS2	2024	<ul style="list-style-type: none"> <li>• Satisfaction with scalable ENISA support</li> <li>• Maturity of operational communities</li> </ul>	<ul style="list-style-type: none"> <li>• 80 % satisfaction of stakeholders</li> <li>• Average overall level of maturity increases year by year</li> </ul>
4.B. Ensure a high level of coordination of the vulnerability disclosure services within the EU.	Article 7 and NIS2	2026	<ul style="list-style-type: none"> <li>• EU vulnerability database usage and added-value</li> </ul>	<ul style="list-style-type: none"> <li>• EU vulnerability disclosure services are gradually available (numbering services in place) and aligned with national mechanisms</li> <li>• EU vulnerability database is functional and aligned with national mechanisms</li> </ul>
4.C. Robust and secure tools/platforms are established, and actively utilised to facilitate seamless operational collaboration at the EU level.	Article 7 and NIS2	2024	<ul style="list-style-type: none"> <li>• Continuous operations and use of secure communication tools and platforms for EU-CyCLONE and Cooperation Network including the use of regular checks and controls</li> </ul>	<ul style="list-style-type: none"> <li>• No significant disruption or incidents in the working of operational tools and platforms recorded against standard checks and controls</li> <li>• Beneficiaries use the tools</li> </ul>



Outputs

Expected results of output

Validation

Output indicator

Frequency (data source)

Latest results

Target 2024

4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs Network and EU-CyCLONE members.	Enhanced information sharing and cooperation among the CSIRTs Network and EU-CyCLONE members	CSIRTs Network and EU-CyCLONE members	Stakeholder satisfaction	Biennial (Survey)	89%	>90%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (Report)	n/a	
4.2 Design and architect processes and tools to build an EU vulnerability database in close cooperation with the MSs	ENISA provides numbering services for common vulnerabilities and exposures with a view to gradually establishing the EU vulnerability database.	CSIRTs Network and NIS CG.	Stakeholder satisfaction	Biennial (Survey)	89%	>90%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (Report)		
4.3. Operate, maintain and promote operational cooperation infrastructure for the EU cybersecurity communities.	Usage of the available tools	CSIRTs Network and EU-CyCLONE members.	Stakeholder satisfaction	Biennial (Survey)	89%	>90%
			Number of users, both new and recurring, and usage per platform/tool/ SOP provided by ENISA			
			CSIRTs active users % increase year on year		19%	
			CSIRTs number of exchanges/ interactions % increase year on year	Annual (Report)	104%	>5% increase
			EU-CyCLONE active users % increase year on year		2%	
EU-CyCLONE number of exchanges/ interactions % increase year on year		548%				

## Stakeholders and engagement levels

**Partners:** Blueprint actors, EU decision-makers, institutions, agencies and bodies, CSIRTs Network members, EU-CyCLONE members, SOCs including national and cross-border SOCs

**Involve/engage:** NIS CG, OES and DSP, ISACs

RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 4.1	NIS, SITAW	3.5	144 567	0	299 557	0	0	3.5	444 124
Output 4.2	NIS, SITAW	3.5	266 474	0	0	0	0	3.5	266 474
Output 4.3	SITAW, NIS	3.5	786 908	0	278 988	0	0	3.5	1 065 896
Activity total	FTE: 10.50 Budget: EUR 1 776 494								
Actual resources used in previous year (2022)	FTE: 5 Budget: EUR 1 682 555 <sup>(401)</sup>								

---

<sup>(401)</sup> Carried over into 2023: EUR 602 393.

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



### Overview of activity



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

The activity includes the development of a regular in-depth EU cybersecurity technical situation report in accordance with Article 7(6) CSA, also known as the joint cyber assessment report (JCAR), regular weekly open-source intelligence reports, a joint rapid report together with CERT-EU and other ad hoc reports as needed.

The activity supports the EU institutions, bodies, offices and agencies in public communication relating to incidents and crises. The activity also supports MSs with respect to operational cooperation within the CSIRTs Network and EU-CyCLONe by providing at their request advice to a specific cyber threat, assisting in the assessment of incidents, facilitating technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities, including through the EU vulnerability database (under development in output 4.2).

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

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

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

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

### Link to strategic objectives (ENISA STRATEGY)










- SO3: Effective operational cooperation within the Union in the case of massive (large-scale, cross-border) cyber incidents

### Indicator for strategic objectives



- Risk level due to cyber threats is understood by the cybersecurity communities at the EU level and decision-makers are able to prioritise actions to manage the risk

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
5a.A Threat and information are disseminated in a timely and accurate manner and/or available on demand	Article 7	2025	<ul style="list-style-type: none"> <li>Recipients are informed accurately and in a timely manner about the latest threat, vulnerabilities and incidents</li> <li>Usefulness of situational reports</li> </ul>	<ul style="list-style-type: none"> <li>At least 80 % of recipients found the information to be communicated accurately and in a timely manner based on the level of confidence of the information</li> <li>At least 80 % of recipients found the reports useful</li> </ul>
5a.B Improved common situational awareness through joint assessment, threat and risk analysis	Article 7	2025	<ul style="list-style-type: none"> <li>Stakeholders ability to make informed decisions based on joint situational reports</li> <li>Usefulness and timeliness of joint situational reports</li> </ul>	<ul style="list-style-type: none"> <li>100% quarterly JCAR reports have been issued on time</li> <li>At least 80% of recipients find the reports useful</li> </ul>
5a.C Information exchange to augment EU common situational awareness through cooperation with private sector and non-EU entities	Article 7	2026	<ul style="list-style-type: none"> <li>Cyber partnership programme is established</li> <li>Information coming from private sector partners and non-EU entities are part of operational cycle of situational awareness production</li> </ul>	<ul style="list-style-type: none"> <li>90 % of selected entities are enrolled in the ENISA cyber partnership programme</li> <li>90 % of the participating entities are actively contributing by exchanging information</li> </ul>

 Outputs	 Expected Results Of Output	 Validation	 Output Indicator	 Frequency (Data Source)	 Latest Results	 Target 2024
5a.1 Collect, organise and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports and threats, and support consolidation and exchange of information on strategic, operational and technical levels <sup>(42)</sup>	<ul style="list-style-type: none"> <li>Establishment of a threat information management platform</li> <li>Production of briefings, reports and summaries of incidents, threats and vulnerabilities</li> <li>Increased understanding and timely access to information regarding latest threats, incidents and vulnerabilities</li> </ul>	CSIRT Network, EU CyCLONE, EUIBAS, national authorities within MSs subscribed to the products	Stakeholder satisfaction	Biennial (Survey)	84%	>90%
			Timeliness and Accuracy of reports	Annual (survey)	n/a	
5a.2 Provide analysis and risk assessment jointly with other operational partners including EUIBAS, MSs, industry partners and non-EU partners	<ul style="list-style-type: none"> <li>EU joint assessment and reports, sectorial analysis, threat and risk analysis <sup>(43)</sup></li> <li>Recipients receive accurate and timely assessment of threat actors and associated risk to the EU internal market</li> </ul>	CSIRT Network, EU CyCLONE, EUIBAS, Horizontal Working Party on Cyber Issues, MB	Stakeholder satisfaction	Biennial (Survey)	84%	>90%
			Number of contributing MSs and relevant EUIBAS	Annual (survey)	n/a	
5a.3 Maintain, develop and promote ENISA cyber partnership programme aimed at information exchange to support the agency's understanding of threats, vulnerabilities, incidents and cybersecurity events	<ul style="list-style-type: none"> <li>Establishment and operationalisation of the cyber partnership programme</li> <li>ENISA situational awareness leverages private sector partnerships to augment context and understanding of threats, vulnerabilities and incidents</li> </ul>	CSIRT Network, EU CyCLONE, EUIBAS, Horizontal Working Party on Cyber Issues, MB	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Number of new and total partners in the ENISA partnership programme	Annual (report)	n/a 6	10/4
			Percentage of requests for information answered by members of partnership programme	Annual (report)	n/a	80%

<sup>(42)</sup> Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.

<sup>(43)</sup> Including JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and DG Communications Networks, Content and Technology Situation Centre.

## Stakeholders and engagement levels



**Partners:** EU MSs (including CSIRTs Network members and EU-CyCLONe), EUIBAs, other technical and operational blueprint actors, partnership programme for 5.3 (with trusted vendors, suppliers and partners)

**Involve / Engage:** Other type of CSIRTs and product security incident response teams

RESOURCE FORECAST 2024									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 5a.1	SITAW, INDEX-,NIS	4	1 280 459 <sup>(44)</sup>	0	0	0	0	4	1 280 459
Output 5a.2	SITAW, INDEX-,NIS	4		0	0	0	0	4	
Output 5a.3	SITAW	1.25	37 000	0	0	0	0	1.25	37 000
Activity total	FTE: 9.25 Budget: EUR 1 317 459 <sup>(45)</sup>								
Actual resources used in previous year (2022)	FTE: 7.35 Budget: EUR 842 992 <sup>(46)</sup>								

<sup>(44)</sup> Includes allocation of EUR 450 000 from the contribution agreement related to the cybersecurity support action, refer to Annex XI and activity 5b for further information.

<sup>(45)</sup> Includes allocation of EUR 450 000 from the contribution agreement related to the cybersecurity support action, refer to Annex XI and activity 5b for further information.

<sup>(46)</sup> Carried over into 2023: EUR 276 749.



## ACTIVITY 5b:

# Contribute to cooperative response at Union and Member States level through ex-ante and ex-post services provision



### Overview of activity



The activity contributes to further developing preparedness and response capabilities at the EU and MS level to large-scale cross-border incidents or crises related to cybersecurity through the implementation and delivery of ex ante and ex post services. It implements the cybersecurity support action, through which the agency provides penetration tests (pentest), threat hunting, risk monitoring and assessment, and customised exercise, and supports the MSs with incident response.

The agency will leverage upon the lessons learned and the mechanisms that have been put in place during the first year of the cybersecurity support action in 2023. This will refocus the service catalogue and the processes/methodologies will be further adapted to better suit the needs of the MSs, allowing for more flexibility and scalability.

The types and level of services are agreed with a single point of contact within each MS and final beneficiary entity.

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

This activity is resourced through the use of 10 CAs to be absorbed as a direct cost of the programme and financed through the Commission contribution agreement. ENISA will not be able to resource this activity with the current establishment plan. The budget for this activity is intended for 2024 through 2025 <sup>(47)</sup>.

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

### Link to strategic objectives (ENISA STRATEGY)



- SO3: Effective operational cooperation within the Union in the case of massive (large-scale, cross-border) cyber incidents








### Indicator for strategic objectives



- Level of preparedness and response to large-scale cross-border incidents

<sup>(47)</sup> Information on FTE calculation and budget amount are pending final determination of the contribution agreement between the Commission (DG Communications Networks, Content and Technology) and ENISA.

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
5b.A Enhanced preparedness and effective incident response	Article 7	2025	Ability of ENISA to support EU Member States to further develop preparedness and response capabilities through implementation and delivery of ex-ante and ex-post services delivery	>4 <sup>(48)</sup>

 OUTPUTS	 Expected results of output	 Validation	 Output indicator	 Frequency (data source)	 Latest results	 Target 2024
5b.1 Pentest and threat hunting services towards selected entities within EU MSs <sup>(49)</sup>	Pentest and threat hunting services are delivered timely and accurately to MSs	MSs, DG Communications Networks, Content and Technology, beneficiaries	% of MSs requesting the service Satisfaction score	Annual	n/a	50% >4
5b.2 Customised exercise and training for selected entities within EU MSs <sup>(50)</sup>	Customised exercise and training services are delivered timely and accurately to MSs.	MSs, DG Communications Networks, Content and Technology, beneficiaries	% of MSs requesting the service Satisfaction score		n/a	50% >4
5b.3 Risk monitoring and assessment for selected entities within EU MSs <sup>(51)</sup>	ENISA is able to provide regular risk monitoring of specific targets or at the national level, including by leveraging commercial off-the-shelf platforms, as well as providing specific risk assessments and threat landscapes as requested by MSs	MSs, DG Communications Networks, Content and Technology, beneficiaries	% of MSs requesting the service Satisfaction score		n/a	50% >4
5b.4 Support incident response and incident management of selected entities within EU MSs <sup>(52)</sup>	ENISA provides 24/7 support for incident response to MSs	MSs, DG Communications Networks, Content and Technology, beneficiaries	% of MSs requesting the service Support was provided in a timely manner Satisfaction Score		n/a	50% >4

## Stakeholders and engagement levels



**Partners:** EU MSs, selected beneficiary entities, Commission

**Involve / Engage:** EU-CyCLONe, CSIRT Network, DG Communications Networks, Content and Technology

<sup>(48)</sup> Target response to qualitative survey regarding ENISA's ability to support MSs on a scale of 1 to 5, with 5 being the highest rating.

<sup>(49)</sup> Beneficiaries of the activity 5b services are specified in the [Contribution Agreement].

<sup>(50)</sup> Beneficiaries of the activity 5b services are specified in the [Contribution Agreement].

<sup>(51)</sup> Beneficiaries of the activity 5b services are specific in the [Contribution Agreement].

<sup>(52)</sup> Beneficiaries of the activity 5b services are specific in the [Contribution Agreement].

RESOURCE FORECAST 2024									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service) <sup>(53)</sup>		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 5b.1	SITAW, NIS, INDEX, TREX	3.5 <sup>(54)</sup>	19.55 million <sup>(55)</sup>						19.55 million
Output 5b.2	SITAW, NIS, INDEX, TREX								
Output 5b.3	SITAW, NIS, INDEX, TREX								
Output 5b.4	SITAW, NIS, INDEX, TREX								
Activity total	3.5 FTE and 19 550 000 budget <sup>(56)</sup>								

<sup>(53)</sup> Cyber support action programme.

<sup>(54)</sup> This activity is resourced through the use of 10 CAs to be absorbed as a direct cost of the programme and financed through the Commission contribution agreement. The actual resources count will be available after finalisation of the contribution agreement between the Commission (DG Communications Networks, Content and Technology) and ENISA. The FTE represents the contribution of ENISA based on the current establishment plan.

<sup>(55)</sup> Information on FTE calculation and budget amount are pending final determination of the contribution agreement between the Commission (DG Communications Networks, Content and Technology) and ENISA. The budget for this activity is to be intended for 2024 through 2025. In addition, 450 000 allocated to activity 5a.

<sup>(56)</sup> Minus 450 000 allocated to activity 5a, please refer to Annex XI for further details regarding the contribution agreement.

# ACTIVITY 6: Development and maintenance of EU cybersecurity certification framework



## Overview of activity



This activity encompasses measures 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 programme. Measures also include maintaining and evaluating adopted cybersecurity certification schemes and participating in peer reviews. In addition, in this activity, ENISA assists the Commission with regard to the ECCG, co-chairing and providing the secretariat for the SCCG; ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Article 50 of the CSA. As from 2024, ENISA seeks to support the cybersecurity certification stakeholders with an online platform that has been set up by the Commission. Furthermore, ENISA contributes to the cybersecurity framework by analysing pertinent aspects of certification along the lines of legislation adopted, notably NIS2 and the DGA as well as legal instruments in the legislative process that include the amendment to the CSA, CRA, EUDIW, AI Act, Chips Act, Data Act, amendment of CSA regarding managed security services certification, etc.

The work undertaken under output 7.4 has been absorbed into output 6.2.

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

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

## Link to strategic objectives (ENISA STRATEGY)










- SO5 High level of trust in secure digital solutions

## Indicator for strategic objectives



- Citizens trust in ICT certified and non-certified solutions in the EU market

Activity Objectives	CSA Article And Other EU Policy Priorities	Time-frame Of Objective	Indicator	Target
6.A Improve the certification requirements concerning security posture management of certified products, services, processes and gradually of managed security services	Article 8 and Title III	2025	<ul style="list-style-type: none"> <li>Monitor ENISA take-up of technical standards and technical specifications in support of EU legislation (document monitoring)</li> </ul>	Applicable standards and cybersecurity requirements have been considered by ENISA to promulgate better cybersecurity certification schemes
6.B Efficient and effective implementation of the European cybersecurity certification framework	Article 8 and Title III	2025	<ul style="list-style-type: none"> <li>Number of stakeholders (public and private) in the internal market, implementing the cybersecurity certification framework for their digital solutions</li> </ul>	A scheme is implemented in a timely manner across all relevant market sectors
6.C Increase use and uptake of European cybersecurity certification	Article 8 and Title III	2024	<ul style="list-style-type: none"> <li>Number of schemes and additional requests addressed to ENISA by the Commission</li> <li>Number of schemes and additional requests processed by ENISA</li> <li>Uptake of certified digital solutions (products, services, processes and gradually managed security services) using certification schemes under the CSA framework as well as other directly applicable instruments, i.e. CRA, EUDIW, etc.</li> </ul>	High number of private and public entities and/or market sectors relevant to a given scheme taking up certification after the entry into force of the implementing act
6.D Increase trust in ICT products, services and processes	Article 8 and Title III	2025	<ul style="list-style-type: none"> <li>Number of certificates issued and published under an EU certification scheme; high utilisation rate in the market</li> </ul>	High degree of visibility and utilisation of EU cybersecurity certificates

 <b>Outputs</b>	 <b>Expected results of output</b>	 <b>Validation</b>	 <b>Output indicator</b>	 <b>Frequency (data source)</b>	 <b>Latest results</b>	 <b>Target 2024</b>
6.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes	<ul style="list-style-type: none"> <li>Scheme meets stakeholder requirements, notably of the MSs and the Commission</li> <li>Take-up of schemes by stakeholders</li> <li>Timely delivery of all schemes requested in cooperation with the Commission</li> <li>Statutory bodies and AHWGs actively involved</li> </ul>	<ul style="list-style-type: none"> <li>AHWGs on certification</li> <li>ECCG</li> <li>European Commission</li> </ul>	Stakeholder satisfaction	Biennial (survey)	82%	75%
			Number of opinions of stakeholders managed	Annual (report)	n/a	100 opinion items per scheme
			Number of people/ organisations engaged in the preparation of certification schemes	Annual (report)	n/a	At least 20 AHWG members from third-party experts; at least 15 MSs joining AHWGs
6.2 Implementing and maintenance of the established schemes including evaluation of adopted schemes, participation in peer reviews etc. and monitoring the dependencies and vulnerabilities of ICT products and services	<ul style="list-style-type: none"> <li>Review of schemes to improve efficiency and effectiveness</li> <li>Take-up of schemes by stakeholders</li> </ul>	AHWGs on certification ECCG European Commission	Stakeholder satisfaction	Biennial	82%	75%
			ENISA response to consolidated monitoring and maintenance requirements of schemes adopted	Triennial (survey)	n/a	75%
			Satisfaction of ENISA's role in NCCA peer reviews	Triennial (survey)	n/a	75%
6.3 Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks		ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			Feedback from statutory bodies including NCCAs on ENISA's role	Annual (survey)	n/a	75%
6.4 Developing and maintaining the necessary provisions, tools and services concerning the EU's cybersecurity certification framework (including the certification website, supporting the Commission in relation to the core stakeholders service platform of the Connecting Europe Facility for collaboration, publication, promotion of the implementation of the cybersecurity certification framework etc.)	<ul style="list-style-type: none"> <li>Supporting transparency and trust of ICT products, services and processes</li> <li>Stakeholders' engagement and promotion of certification</li> </ul>	ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			User satisfaction concerning the certification website services	Annual (survey)	n/a	75%
			Usage of certification website	Annual (report)	n/a	75%

## Stakeholders and engagement levels



**Partners:** EU MSs (including NCCAs and the ECCG), Commission, EUIBAS, Selected stakeholders as represented in the SCCG

**Involve/ Engage:** Private sector stakeholders with an interest in cybersecurity certification, CABs, national accreditation bodies, consumer organisations

RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 6.1	CERTI, NIS	4.65	400 000	0.7		0.5	0	5.85	400 000
Output 6.2	CERTI	1.9	53 000	0	-	0	0	1.9	53 000
Output 6.3	CERTI	0.5		0		0	0	0.5	-
Output 6.4	CERTI	1.1	118 896	0.15		0	0	1.25	118 896
Activity total	FTE: 9.5 Budget: EUR 571 896								
Actual resources used in previous year (2022)	FTE: 8.35 Budget: EUR 959 343 <sup>(57)</sup>								

<sup>(57)</sup> Carried over into 2023: EUR 277 604 (73) Carried over into 2023: EUR 277 604

# ACTIVITY 7: Supporting the European cybersecurity market and industry



## Overview of activity



This activity seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence on external markets, increase the capacity of the EU and reinforce supply chains to the benefit of internal market. It involves measures to promote and implement ‘security by design’ and ‘security by default’ measures in ICT products, services and processes, including through standardisation. Therefore, this activity also seeks to lay the groundwork for a robust role for ENISA in the CRA, notably in terms of market analysis, preparation of market sweeps and reporting of exploited vulnerabilities etc. Measures 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, and performing regular analysis of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein. Platforms for collaboration among the cybersecurity market players, improve visibility of trustworthy and secure ICT solutions in the digital single market.

Output 7.4 has been absorbed into output 6.2

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

## Link to strategic objectives (ENISA STRATEGY)



- SO5 High level of trust in secure digital solutions








## Indicator for strategic objectives



- Monitor metrics such as number of certificates issued under an EU scheme; number of companies interested in EU certification; and growth observed in the number of CABs or EU certification functions thereof recorded in the MS

Activity Objectives	CSA article and other EU policy priorities	Timeframe Of Objective	Indicator	Target
7.A Foster a robust European cybersecurity industry and market	Article 8 and Title III CSA CRA proposal	2024	<ul style="list-style-type: none"> <li>• Stakeholders' satisfaction (survey)</li> <li>• State of the EU cybersecurity industry and market for products and services (index)</li> <li>• Industry perception of the internal market (survey)</li> </ul>	Improved ability of ENISA and the EU to analyse the EU cybersecurity market
7.B Improve the conditions for the functioning of the internal market	Article 8 and Title III CSA CRA proposal	2025	<ul style="list-style-type: none"> <li>• Better informed choices by users of products in market niches analysed</li> </ul>	Improve stakeholders' understanding of the cybersecurity market conditions in the EU



 Outputs	 Expected results of output	 Validation	 Output indicator	 Frequency (data source)	 Latest results	 Target 2024
7.1. Market analysis on the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes	Improved understanding of the market/ industry	<ul style="list-style-type: none"> <li>AHWGs cybersecurity market analysis</li> <li>ECCG (as necessary)</li> <li>SCCG</li> <li>Advisory Group</li> <li>NLO (as necessary)</li> </ul>	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Cybersecurity market analysis; cybersecurity product and services analysis; analysis of vulnerabilities and dependencies in ICT products and services as appropriate; analysis of other relevant market areas	Annual (report)	n/a	All reports produced as planned (Y out of Y reports)
7.2. Monitoring developments in related areas of standardisation, analysis of standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification	Alignment with standards	<ul style="list-style-type: none"> <li>SCCG</li> <li>Advisory Group</li> <li>NLO (as necessary)</li> </ul>	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Reports on analysis of standardisation aspects of cybersecurity including cybersecurity certification	Annual (report)	n/a	All reports produced as planned (Y out of Y reports)

### Stakeholders and engagement levels



**Partners:** EU MSs (including entities with an interest in cybersecurity market monitoring e.g. NCCAs, national standardisation organisations), Commission, EUIBAs, European standardisation organisations (CEN, Cenelec, the European Telecommunications Standards Institute), private sector or ad hoc standards-setting organisations, European Cybersecurity Competence Centre.

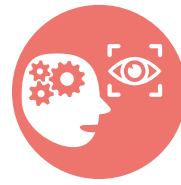
**Involve/ Engage:** Private sector stakeholders with an interest in the cybersecurity market and/or standardisation, International Organization for Standardization / International Electrotechnical Committee, consumer organisations

RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 7.1	CERTI, INDEX, CERTI	4.15	130 000	0.1	0	0	0	4.25	130 000
Output 7.2	CERTI, NIS	2.75	136 666		0	0	0	2.75	136.666
Activity total		FTE: 7 Budget: 266.666							
Actual resources used in previous year (2022)		FTE: 4.35 Budget: EUR 366 473 <sup>(58)</sup>							

<sup>(58)</sup> Carried over into 2023: EUR 105 230.

# ACTIVITY 8:

## Knowledge on emerging cybersecurity challenges and opportunities



### Overview of activity



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

These activities leverage on expertise of relevant legal, regulatory, economic and societal 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 EU.

As part of this activity the agency will map threat landscapes and provide topic-specific, as well as general, assessments on the expected societal, legal, economic, technological and regulatory impact, with targeted recommendations to MSs and EU institutions, bodies, offices and agencies.

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

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

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

This activity leads ENISA's efforts towards delivering the INDEX service package, while in parallel contributing to the delivery of the NIS, TREX and SITAW service packages.

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

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

### Link to strategic objectives (ENISA STRATEGY)










- SO6. Foresight on emerging and future cybersecurity challenges
- SO7. Efficient and effective cybersecurity information and knowledge management for Europe

### Indicator for strategic objectives



- EU level cybersecurity risk assessment and cyber threat landscape (adopted in accordance with Article 18(1) point a) NIS2

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
8.A Knowledge and uptake of future challenges and opportunities by MS and EU actors	Article 9 CSA	2025	<ul style="list-style-type: none"> <li>Cybersecurity index indicator 'emerging technology threats are considered by national risk assessments'</li> <li>Level of the acceptance of the report of the state of cybersecurity in the EU</li> </ul>	<ul style="list-style-type: none"> <li>European Parliament positive adoption</li> <li>High take-up of the report by MS and EU actors</li> <li>All MSs have considered at least 1/3 of the mapped emerging technology threats in assessing risk at the national level</li> </ul>
8.B Increase understanding of the state of cybersecurity	Article 9 CSA and eIDAS Article 10	2025	<ul style="list-style-type: none"> <li>Use of cybersecurity index by MSs</li> </ul>	<ul style="list-style-type: none"> <li>All MSs give input to cybersecurity index</li> <li>2/3 of MSs are using the index to inform their national cybersecurity strategies</li> </ul>
8.C Deliver relevant and timely information	Article 9 CSA	2024	<ul style="list-style-type: none"> <li>Usage of knowledge management portals, i.e. index, the cybersecurity incident reporting and analysis system, etc.</li> <li>Value and usability of knowledge management portals</li> </ul>	<ul style="list-style-type: none"> <li>2/3 of targeted stakeholders use the portals regularly</li> <li>2/3 of stakeholders are satisfied with the portals</li> </ul>

 <b>OUTPUTS</b>	 <b>Expected results of output</b>	 <b>Validation</b>	 <b>Output indicator</b>	 <b>Frequency (data source)</b>	 <b>Latest results</b>	 <b>Target 2024</b>
8.1. Develop and maintain EU cybersecurity index	<ul style="list-style-type: none"> <li>Measuring maturity</li> <li>Stakeholders can better prepare for future challenges based on indication of maturity</li> </ul>	NISD CG, NLO, CSIRT's Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Uptake of the cybersecurity index	Biennial (survey)	n/a	<ul style="list-style-type: none"> <li>20 MS representatives</li> <li>60 % satisfaction rate</li> <li>Agreement by all validating bodies</li> </ul>
8.2. Collect and analyse information to report on the cyber threat landscapes	<ul style="list-style-type: none"> <li>Mapping threats</li> <li>Generate recommendations for stakeholders to take up</li> </ul>	NLO, Advisory Group and Cybersecurity Threat Landscape AHWG  CSIRT's Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357	±5 % compared to 2023
			Uptake of reports generated in activity 8	Annual (report)	n/a	±5% compared to 2023
8.3. Analyse and report on incidents as required by Article 5(6) of the CSA as well as other sectorial legislations (e.g. DORA, Article 10 eIDAS, etc.)	<ul style="list-style-type: none"> <li>Analysing incidents</li> <li>Generate recommendations for stakeholders to take up</li> </ul>	Work Stream 3 of the NISD CG, European Competent Authorities for Secure Electronic Communications and Article 19 eIDAS groups	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			EU incident reporting maturity	Annual (survey)	n/a	EU Average >50%
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	n/a	±5 % compared to 2023
			Uptake of reports generated in activity 8	Annual (report)	n/a	±5% compared to 2023
8.4. Foresight on emerging and future cybersecurity challenges and recommendations	<ul style="list-style-type: none"> <li>Identifying future challenges and opportunities</li> <li>Generate recommendations for stakeholders to take up</li> </ul>	Foresight AHWG, NLO and AG	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357	±5% compared to 2023
			The influence of foresight on the development of ENISA's work programme	Biennial (ENISA SPD)	n/a	>2 emerging areas identified
			Uptake of reports generated in activity 8	Annual (report)	n/a	±5 % compared to 2023

## Stakeholders and engagement levels



**Partners:** NISD CG Work stream 3, European Competent Authorities for Secure Electronic Communications, Article 19 eIDAS Group, Foresight AHWG, CTL AHWG, Index NLO subgroup

**Involve/ Engage:** NLO/AG, CSIRTs Network

RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 8.1	INDEX	2.75	181 982	0	0	0	0	2.75	181 982
Output 8.2	INDEX, SITAW, NIS	2	136 616	0.25	0	0.15		2.35	136 616
Output 8.3	INDEX, SITAW, NIS	1.2	178 791		0	0	0	1.2	178 791
Output 8.4	INDEX	1.1	207 257	0	0	0.1	7 000	1.2	214 257
Activity total	FTE: 7.5 Budget: 711 646								
Actual resources used in previous year (2022) <sup>(59)</sup>	FTE: 10.9 Budget: EUR 1 043 564 <sup>(60)</sup>								

<sup>(59)</sup> Activity 10 outputs and thus resources were undertaken within activity 8 in 2022.

<sup>(60)</sup> Carried over into 2023: EUR 81 543.

# ACTIVITY 9: Outreach and education



## Overview of activity



The activity seeks to raise the overall awareness of cybersecurity risks and practices. In cooperation with MSs, EU institutions, bodies, offices and agencies and the 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 EU. As part of this activity, the agency will organise regular outreach campaigns, provide guidance on best practices and support coordination across MSs on awareness and education. Moreover, the agency will facilitate the exchange of best practices and information on cybersecurity in education between MSs.

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

The activity will also seek to contribute to the EU's efforts to cooperate with non-EU countries and international organisations on cybersecurity.

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

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

## Link to strategic objectives (ENISA STRATEGY)










- SO1. Empowered and engaged communities across the ecosystem
- SO4. Cutting edge competences and capabilities in cybersecurity across the Union

## Indicator for strategic objectives










- The % gap between demand and supply of cybersecurity skilled professionals
- General level of cybersecurity awareness and cyber hygiene among citizens and entities

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
9.A Increase awareness of cybersecurity risks and improve cyber-secure behaviour	Article 10	2025	<ul style="list-style-type: none"> <li>Cybersecurity indicator 'Enterprises: Staff awareness'</li> <li>Cybersecurity indicator 'SME culture of cybersecurity'</li> <li>Number of cybersecurity incidents with human error as root cause</li> <li>Cybersecurity index indicators 'National culture of cybersecurity'</li> </ul>	<ul style="list-style-type: none"> <li>1–2 % increase of cybersecurity indicator 'SME culture of cybersecurity' year by year</li> <li>Number of cybersecurity incidents in critical sectors with human error as root cause decreases year by year in relative percentages</li> <li>1–2 % increase of cybersecurity index 'National culture of cybersecurity'</li> </ul>
9.B Increase the supply of skilled professionals to meet market demand	Articles 6 and 10  EU priority on skills shortage  Commission Communication on Cybersecurity Skills Academy	2025	<ul style="list-style-type: none"> <li>Increase in cybersecurity indicator 'Cybersecurity graduates in higher education'</li> <li>Number of professionals trained under cybersecurity skills academy</li> </ul>	<ul style="list-style-type: none"> <li>'Cybersecurity graduates in higher education'</li> <li>At least 200 000 professionals trained by 2025</li> </ul>
9.C Foster EU cybersecurity values and priorities	Article 42	2024	<ul style="list-style-type: none"> <li>Ability to support the EU external objectives</li> <li>Coherence of ENISA international engagement with the agency's strategy</li> </ul>	<ul style="list-style-type: none"> <li>ENISA is seen as a key contributor to foster EU cybersecurity values and priorities where engaged</li> <li>ENISA activities are judged to be aligned with its international strategy</li> </ul>







 Outputs	 Expected Results Of Output	 Validation	 Output Indicator	 Frequency (Data Source)	 Latest Results	 Target 2024
9.1 Develop activities to enhance behavioural change by essential entities <sup>(61)</sup>	<ul style="list-style-type: none"> <li>Targeted awareness campaigns to improve behaviour</li> <li>Take-up of best practices by stakeholders</li> </ul>	Awareness raising AHWG, NISD Work stream	Stakeholder satisfaction	Biennial (survey)	91.5%	>1 % increase (from previous year – decrease in duplication)
			Number of activities and participation in awareness-raising initiatives organised by ENISA on cybersecurity topics	Annual (report)		>5% increase
			Total social media impressions		27 278 491	
			Total social media engagement		19 301	
			Total video views		6 602 355	
			Total website visits		300 530	
			Total participation at events		40	
Number of downloads of materials and overall utilisation of Awareness Raising tools (i.e. Awareness Raising-in-a-box and SME tool)		Annual (ENISA website)	n/a	>4000 per semester		

<sup>(61)</sup> Defined by NIS2

							
9.2 Promote cybersecurity topics and good practices <sup>(62)</sup>	<ul style="list-style-type: none"> <li>Recognise threats and risks and how to act cyber secure</li> <li>Better informed stakeholder</li> </ul>	Awareness Raising AHWG, ECSM coordinators group	Stakeholder satisfaction	Biennial (survey)	91%	1 % increase (from previous year – decrease in duplication)	
			Number of activities and participation in awareness-raising initiatives organised by ENISA on cybersecurity topics	Annual (report)		>5 % increase	
			Total social media impressions	Annual (report)	27 278 491	>5% increase	
			Total social media engagement		19 301		
			Total video views		6 602 355		
			Total website visits		300 530		
			Total participation at events		40		
			Number of downloads of materials and overall utilisation of Awareness Raising tools (i.e. AR-in-a-Box and SME tool)	Annual (ENISA website)	n/a	>4000 per semester	
9.3 Implement ENISA international strategy and outreach	<ul style="list-style-type: none"> <li>EU values recognised by international stakeholders</li> <li>International cooperation support ENISA objectives</li> </ul>	MT, EEAS, COM and (MB as required )	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)	
			Staff satisfaction with international coordination	Annual (survey)	n/a	>80%	
			Number of international engagements	Annual (report)	n/a		
9.4 Support the implementation and uptake of EU cybersecurity skills framework	<ul style="list-style-type: none"> <li>Promoting cybersecurity skills courses</li> <li>Greater number of participants in cybersecurity courses</li> </ul>	AHWG on Cybersecurity Skills, ECCC WG on Skills	Stakeholder satisfaction	Biennial (survey)		1% increase (from previous year – decrease in duplication)	
			Number of cybersecurity programmes (courses) and participation rates	Annual (cyberhead platform)	<ul style="list-style-type: none"> <li>19% female</li> <li>81% male</li> </ul>	1-2% increase	
			Total number of students enrolled in the first year of the academic programmes				5 205
			Student gender distribution (% female: % male)				
			Total number of cybersecurity programmes				122
			Number of postgraduate programmes				5%
			Number of master's degree programmes				80%
			Number of bachelor's degree programmes				15%
			Number of entities included in ECSF registry (i.e. # of MS adopted ECSF, #of ECSF implementations/pledges)				Annual (register of activities)

<sup>(62)</sup> Including based on stakeholder strategy.



						
9.5 Implement the cybersecurity in education roadmap <sup>(63)</sup>	<ul style="list-style-type: none"> <li>Influence education to include cybersecurity</li> <li>Greater awareness and interest in cybersecurity as a career path</li> </ul>	AR AHWG	Stakeholder satisfaction	Biennial (survey)	91.5%	1 % increase (from previous year – decrease in duplication)

## Stakeholders and engagement levels



**Partners:** ECSM Coordination Group, national competent authorities through the NIS CG workstreams, AHWG on Awareness Raising and Education, Enterprise Security AHWG (SMEs), AHWG on Skills, EEAS, DG Neighbourhood and Enlargement Negotiations, DG Communications Networks, Content and Technology

**Involve/ Engage:** ENISA NLOs, DG Communications Networks, Content and Technology, NIS OES / entities within the scope of NIS2, ECCC, international partners

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 <sup>(64)</sup>	NIS	1.75	50 000	0.6	50 000	0	0	2.35	100 000
Output 9.2	INDEX, TREX	1	50 000	0.5	49 315	0	0	1.5	99 315
Output 9.3	SITAW, TREX	1	-	0.75	20 000	0	0	1.75	20 000
Output 9.4	INDEX, TREX, NIS	1.5	70 000	1	30 000	0	0	2.5	100 000
Output 9.5	INDEX	0.5	60 000	0.5	30 000	0	0	1	90 000
Activity total	FTE: 9.1 Budget: €409 315								
Actual resources used in previous year (2022)	FTE: 5.22 Budget: EUR 415 122 <sup>(65)</sup>								

<sup>(63)</sup> Roadmap developed by ENISA during the course of 2022.

<sup>(64)</sup> Carried over into 2023: EUR 125 341.

<sup>(65)</sup> ENISA during the course of 2022.

# ACTIVITY 10: Advise on research and innovation needs and priorities



## Overview of activity



The activity aims to provide advice to MSs and EUIBAs on research needs and priorities in the field of cybersecurity, thereby contributing to the EU's strategic R & I 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 R & I from the different quadrants of the community.

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

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

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

## Link to strategic objectives (ENISA STRATEGY)



- SO6. Foresight on emerging and future cybersecurity challenges








## Indicator for strategic objectives



- Overall EU investment in R&I activities addressing emerging cybersecurity challenges

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
10.A EU R & I funding programmes address emerging cybersecurity challenges identified by ENISA	Article 11, EU Research Agenda	2024	Assessment of ENISA's contribution to EU R & I funding programmes and work programmes	50 % <sup>(66)</sup>
10.B EU R & I funding programmes focus on the development of solutions made in the EU	Article 11, EU Research Agenda	2025	Assessment of EU-funded projects transitioning from research into deployment of new cybersecurity solutions	10
10.C EU cybersecurity R & I community generates knowledge on emerging cybersecurity challenges identified by ENISA	Article 11	2024	Number of research articles and papers generated by the community reviewing emerging cybersecurity challenges identified by ENISA	10

<sup>(66)</sup> Percentage of funding programmes that address cybersecurity challenges proposed by ENISA.

 OUTPUTS	 Expected results of output	 Validation	 Output indicator	 Frequency (data source)	 Latest results	 Target 2024
10.1 Collect and analyse information on new and emerging information and communications technologies in order to identify gaps, trends, opportunities and threats (R & I observatory)	Identifying current and emerging R & I needs and funding priorities	Academia, industry and national R & I entities (including National Competence Centres) and EUIBAs	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Evaluation of the trends, wild cards and weak signals on emerging cybersecurity challenges leading to R & I needs and priorities	Annual (annual work programme)	n/a	3
10.2 Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment	Advising EU funding programmes including the ECCC	Commission including DG Communications Networks, Content and Technology and the Joint Research Centre, ECCC and National Competence Centres	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Number of contributions to EU funding programmes	Annual (reports)	n/a	5

### Stakeholders and engagement levels



**Partners:** Commission Joint Research Centre, national and EU R & I entities, academia and industry, ECCC and national cybersecurity centres

RESOURCE FORECAST									
Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
Output 10.1	NIS	0.6	0	1.15	85 510	0.00	0	1.75	85 510
Output 10.2				1.8	35 490	0.20	5 000	2	40 490
Activity total		FTE: 3.75 Budget: 126000							
Actual resources used in previous year (2022)		n/a <sup>(67)</sup>							

<sup>(67)</sup> Activity 10 outputs were undertaken under activity 8 in 2022

### 3.2. CORPORATE ACTIVITIES

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

## ACTIVITY 11: Performance and sustainability



### Overview of activity










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

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

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

#### ANUAL

Activity Objectives	Link To Corporate Objectives	Activity Indicators	Frequency( Data Source)	Latest Result	Target
11.A Maintain corporate performance and coordinate strategic planning	Ensure efficient corporate services	Proportion of SPD KPIs meeting targets	Annual	13 metrics were unchanged, 21 underperformed and 58 outperformed	>80 of indicators outperformed
	Continuous innovation and service excellence	Results of Internal control framework assessment	Annual	Effective (Level 2)	Effective level 1/2
	Developing service propositions with additional external resourcing	High satisfaction with essential corporate services in the area of compliance and coordination	Annual	n/a	>60%
11.B Increase corporate sustainability	Ensure climate neutral ENISA by 2030	EU Eco-Management and Audit Scheme (EMAS) established	Annual	n/a	Adopted by end 2024
	Develop efficient framework for ENISA continuous governance to safeguard high level of IT	<ul style="list-style-type: none"> <li>Agency IT strategy aligned with corporate strategy</li> <li>Proportion of total IT budget allocated to information security proportional to the level of risks across various IT systems within Agency</li> </ul>	Annual	<ul style="list-style-type: none"> <li>n/a</li> <li>n/a</li> </ul>	<ul style="list-style-type: none"> <li>Revised IT strategy by 2024</li> <li>20% by 2024</li> </ul>

						
OUTPUTS	How output expected to contribute to activity objective for the year	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
11.1 Coordinate the implementation of the Agency's performance management framework, including Agency wide budget management and IT management processes, environmental management and regulatory compliance	<ul style="list-style-type: none"> <li>Unified day to day practices across the agency upon implementing SPD</li> </ul>	<ul style="list-style-type: none"> <li>MT &amp; relevant committees</li> </ul>	Efficiency and effectiveness of project management procedures and tools (survey)	Annual	N/a	>80%
	<ul style="list-style-type: none"> <li>Annual risk assessment and internal controls assessment performed and reported</li> </ul>	<ul style="list-style-type: none"> <li>External and internal audits</li> </ul>	Number of high risks identified in annual risk assessment		3	≤3
	<ul style="list-style-type: none"> <li>Legal and regulatory compliance are monitored; issues and areas of improvement identified</li> </ul>	<ul style="list-style-type: none"> <li>Statutory bodies</li> </ul>	Percentage of identified internal controls deficiencies addressed within timelines		N/a	100% for critical, 80% for major, 60% for moderate
	<ul style="list-style-type: none"> <li>Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy; reports from ITMC</li> </ul>		Number of complaints filed against ENISA/ number of identified legal or regulatory breaches		3	≤3
	<ul style="list-style-type: none"> <li>Streamlined budget management across the Agency; reports from BMC</li> </ul>		% of revised and up to date corporate rules (MBD, EDD, policies, processes)		N/a	60% corporate rules which have not been reviewed less than 3 years ago; 80% corporate rules which have not been reviewed less than 4 years ago
	<ul style="list-style-type: none"> <li>A plan to reduce CO2 emissions at ENISA's HQ</li> </ul>		MoU with Hellenic authorities for CO2 reduction in ENISA HQ in place		N/a	MoU process initiated by end 2024
			Efficiency and effectiveness of ITMC/ BMC processes (survey)		N/a	> 60%
11.2 Maintain and enhance ENISA's cybersecurity posture	<ul style="list-style-type: none"> <li>Compliance with new Regulation on a high common level of cybersecurity within EUIBAs</li> </ul>	<ul style="list-style-type: none"> <li>MT and relevant committees</li> </ul>	Percentage of identified high risk mitigation measures addressed within timelines	Annual	NA	90%
	<ul style="list-style-type: none"> <li>Timely identification and response to cybersecurity risks</li> <li>Continuous monitoring of IT systems cybersecurity and timely identification of issues and areas of improvement (first level and second level controls)</li> </ul>	<ul style="list-style-type: none"> <li>External and internal audits</li> <li>Statutory bodies</li> </ul>	Cybersecurity trainings for staff and managers	Annual	NA	At least two trainings per year
11.3 Provide support services in the EU Agencies network and in key areas of the Agency's expertise	<ul style="list-style-type: none"> <li>Cybersecurity advisory in implementation of the new Regulation on a high common level of cybersecurity within EUIBAs and in co-operation with CERT-EU</li> <li>Shared services in the area of data protection, legal services and accounting</li> </ul>	<ul style="list-style-type: none"> <li>MT, BMC</li> <li>EUAN (agencies receiving ENISA's support)</li> </ul>	Satisfaction within the EU Agency network with ENISA support services	Annual	NA	>80%
11.4 Ensure the implementation of single administration processes across the Agency	Streamlined document management practices	<ul style="list-style-type: none"> <li>MT, Staff committee</li> </ul>	Percentage of staff considering that the information they need to do their job is easily available/accessibly within ENISA	Annual	29%	55%
			Response timeliness to external parties (internal reporting)	Annual	NA	48h

## Stakeholders and engagement levels



**Partners:** EUAN, relevant EUIBAs and Commission, Staff Committee, MT

RESOURCE FORECAST							
Outputs	Supporting service packages	CORE		ESSENTIAL		ON-DEMAND	
		FTE	EUR	FTE	EUR	FTE	EUR
Output 11.1	All service packages	4.2	132 882	0		0	0
Output 11.2	All service packages	2	134 882	0	20 % IT investment – cybersecurity <sup>(68)</sup>	0	0
Output 11.3		0.6	0	0		0	0
Output 11.4	All service packages	4.2	0	0	203 125	0	0
Activity total	FTEs 11 (of which 0.6 reserve) Budget: EUR 470 888 <sup>(69)</sup>						
Actual resources used in previous year (2022) <sup>(70)</sup>	FTE: 16.5 Budget: EUR 829 614 <sup>(71)</sup>						

<sup>(68)</sup> Budget allocated from across the agency's operational activities for IT cybersecurity (as per corporate strategy KPI 20 % of IT spent allocated to cybersecurity). Although internal cybersecurity is centrally coordinated by activity 11, this amount is not included in the budget of activity 11 because it is counted within the budget of the different operational activities.

<sup>(69)</sup> In addition 54.604 SLA with the ECCC, see Annex XI for additional information.

<sup>(70)</sup> The current SPD activities 11 and 12 were undertaken within activity 11 in 2022.

<sup>(71)</sup> Carried over into 2023: EUR 174 087.

## ACTIVITY 12: Reputation and Trust



### Overview of activity



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

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

As part of this activity, ENISA will deliver essential and demand-driven communications services as described in the ENISA corporate strategy.

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

#### ANUAL

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

OUTPUTS	How output expected to contribute to activity objective for the year	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
12.1 Implement the multiannual communications and stakeholders' strategies	<ul style="list-style-type: none"> <li>Increased transparency and outreach</li> <li>Engaged communities</li> <li>Increased impact of ENISA activities</li> <li>Relevant and easily accessible information is provided to stakeholders</li> </ul>	Management Team and agency stakeholders	Number & types of activities at each engagement level (stakeholder strategy implementation)	Annual (Internal report)	N/a	
			Number of social media engagement	Annual (Media monitoring)	75 000	>80 000
			Stakeholder satisfaction with ENISA outreach	Biennial (survey)	N/a	>80%
			Number of total ENISA website visits	Annual (website analytics)	2.03 million	>2.5 million
12.2 Implement internal communications strategy	<ul style="list-style-type: none"> <li>Engaged staff</li> </ul>	Management Team and staff committee	Staff satisfaction with the quality and timing of ENISA internal communications	Annual (survey)	36%	>50%
12.3 Manage and provide the secretariat for the statutory bodies	<ul style="list-style-type: none"> <li>Support the operation and organisation of ENISA statutory bodies</li> <li>Support the effectiveness of the implementation of the work programme (validation of operational outputs)</li> <li>Providing administrative support for the day-to-day working of the bodies</li> <li>MB decisions and recommendations from NLO and AG</li> </ul>	Statutory bodies, Management Team and Committees	Number of feedback received per NLO consultation	Annual (Internal report)	NA	>2
			Number of feedback received per AG consultation	Annual (Internal report)	NA	>2
			Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA	Annual (Survey)	NA	>80%
			Satisfaction of statutory bodies with ENISA portals	Annual (Survey)	NA	>80%

## Stakeholders and engagement levels



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

**Involve / Engage:** All ENISA stakeholders

RESOURCE FORECAST							
Outputs	Supporting service packages	CORE		ESSENTIAL		ON-DEMAND	
		FTE	EUR	FTE	EUR	FTE	EUR
Output 12.1	All service packages	2.5	430 000	c	0	0	0
Output 12.2	All service packages	1	5 000	0	0	0	0
Output 12.3	All service packages	2	50 000	0	0	0	0
Total	FTE: 5.50 Budget: 485 000						
Actual resources used in previous year (2022)	n/a <sup>(72)</sup>						

<sup>(72)</sup> Activity 12 outputs were undertaken within activity 11 in 2022.



## ACTIVITY 13: Effective and efficient corporate services



### Overview of activity








This activity seeks to support ENISA aspirations as stipulated in Article 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'.

The initiatives which will be pursued as part of 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 as an agile and knowledge-based organisation where staff can evolve personally and professionally, keeping staff engaged, motivated and with a 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 an effective framework enabling teleworking outside the place of assignment, developing and maintaining excellent working conditions (premises, layout of office space) and implementing modern user-centric IT and teleconferencing tools delivering state-of-the-art corporate services and supporting ENISA's business owners and stakeholders in line with the agency's objectives.

ENISA will strive to maximise the efficiency of its resources by maintaining its focus on developing a flexible, highly skilled and fit-for-purpose workforce through strategic workforce planning in order to ensure the effective functioning of the agency and maintain a 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 an agile, knowledge-based and matrix organisational structure. 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 the secure operational environment at the highest level, strive excellence in its infrastructure services based on best practices and agile frameworks. It will also explore cloud-enabled services that are fit for purpose and provide services in accordance with recognised European and international standards and the ENISA IT strategy. Besides that, ENISA will strive to promote and foster sector solutions, explore opportunities for shared services with other EU agencies, leverage standard technologies where possible, and support flexible ways of working. As ENISA aspires to become a trusted partner, it will continue by providing customer-focused, multi-disciplinary teams that demonstrate a customer-centric, can-do and agile attitude.

Activity Objectives	Link To Corporate Objectives	Activity Indicators	Frequency( Data Source)	Latest Result	Target
13.a Enhance people centric services by implementing the Corporate and HR strategy	<ul style="list-style-type: none"> <li>Effective workforce planning and management</li> <li>Efficient talent acquisition, development and retention</li> <li>Caring and inclusive modern organisation</li> </ul>	<ul style="list-style-type: none"> <li>Implementation of SWP/SWR decisions</li> <li>Implementation of the Corporate and HR strategy</li> <li>High participation in staff satisfaction survey</li> </ul>	<ul style="list-style-type: none"> <li>Annual</li> <li>Annual</li> <li>Annual</li> </ul>	<ul style="list-style-type: none"> <li>Fully implemented</li> <li>N/a</li> <li>69 %</li> </ul>	<ul style="list-style-type: none"> <li>Fully implemented</li> <li>Actions implemented according to the timelines</li> <li>75 %</li> </ul>
13.b Ensure sustainable and efficient corporate solutions and promote continuous improvement	<ul style="list-style-type: none"> <li>Ensure efficient corporate services</li> <li>Introduce digital solutions that maximise synergies and collaboration in the agency</li> <li>Develop service propositions with additional external resourcing</li> <li>Promote and enhance ecologic sustainability across all agency operations</li> <li>Develop an efficient framework for ENISA continuous governance to safeguard a high level of IT and physical security</li> </ul>	<ul style="list-style-type: none"> <li>Understand best practices in sustainable IT solutions</li> <li>Limited disruption of continuity of corporate services</li> <li>Handling EUCI at the level of SECRET UE/EU SECRET</li> </ul>	<ul style="list-style-type: none"> <li>Annual</li> <li>Annual</li> <li>By Q2 2024</li> </ul>	<ul style="list-style-type: none"> <li>N/a</li> <li>N/a</li> <li>N/a</li> </ul>	<ul style="list-style-type: none"> <li>IT strategy updated accordingly</li> <li>BCP for corporate IT, facilities, financial and HR services ensured</li> <li>Has been accredited</li> </ul>

 OUTPUTS	 Expected results of output	 Validation	 Output indicator	 Frequency (data source)	 Latest results 2022	 Target 2024
13.1 Manage and provide horizontal, recurrent, quality support services in the area of resources for ENISA staff and partners	<ul style="list-style-type: none"> <li>Implement payroll and recurrent administrative services</li> <li>Implement annual recruitment plan</li> <li>Implement annual L&amp;D plan and staff performance</li> <li>Implement annual procurement plan via PPMT</li> <li>Implement insource mission service support</li> <li>Implementation of the ED decision on strategic workforce review [adopted in May 2023]</li> <li>Follow up on FIA centralisation and implementation of results of external analysis on simplification of ENISA financial procedures</li> <li>Analyse procurement services and tenders and propose simplifications</li> <li>Explore further synergies with PMO SLA (e.g. reimbursement of experts)</li> </ul>	<ul style="list-style-type: none"> <li>Management Team</li> <li>IT Management Committee</li> <li>Budget Management Committee</li> <li>Staff Committee</li> </ul>	Turnover rates	Annual	4%	> 3 %
			Establishment plan posts filled		89%	>95%
			Time spent from vacancy announcement to candidate selection		n/a	<300 days
			Percentage of the implementation of approved Recruitment plan		n/a	>90%
			Percentage of the implementation of approved Procurement Plan		n/a	>90%
			Percentage of procurement procedures launched via e-tool (PPMT)		n/a	>90%
			Percentage of budget implementation		100%	>95%
			Average time for initiating a transaction (FIA role)		n/a	<7 days
			Average time for verifying a transaction (FVA role)		n/a	<3 days
			Number of budget transfers		4	<4
Late payments		n/a	<8%			

						
<p>13.2 Implement Agency's Corporate strategy including HR strategy with emphasis on initiatives in talent development, growth and welfare, innovation and inclusiveness areas</p>	<ul style="list-style-type: none"> <li>Establish / review corporate costing models and mechanisms to forecast, anticipate and timely manage emerging needs</li> <li>Revision of HR related MB decisions on middle management staff, on SNEs, on the framework for learning and development, on the appraisal of TA staff and CA staff, on reclassification of TA staff and CA staff indicated in the corporate strategy</li> <li>Set up of key HR policies in the area of learning and development and review staff welfare and mission policies</li> <li>Introduce modern digital solutions in managing talent that give real time input to managers</li> <li>Modernize the selection process by introducing automated IT tool in the process</li> </ul>	<ul style="list-style-type: none"> <li>Management Board</li> <li>Management Team</li> <li>Staff Committee</li> <li>EUAN</li> <li>BMC</li> </ul>	<p>Number of policies/IR revised or adopted</p> <p>Number of processes reviewed/redesigned</p> <p>Percentage of staff satisfaction survey with talent development</p> <p>Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time</p> <p>Number of implemented competency driven training and development activities</p> <p>Number of multisource feedback evaluations implemented and followed up</p>	<p>Annual</p>	<p>n/a</p> <p>n/a</p> <p>43%</p> <p>n/a</p> <p>n/a</p> <p>n/a</p>	<p>&gt;1</p> <p>&gt;1</p> <p>&gt;50%</p> <p>&gt;95%</p> <p>&gt;1</p> <p>&gt;5</p>
<p>13.3 Manage and provide horizontal, recurrent, quality support services in the area of facilities, security and corporate IT for ENISA staff and partners</p>	<ul style="list-style-type: none"> <li>Implement annual IT project plan</li> <li>Implement annual FM plan, maintenance and upgrades, including physical security service provision</li> <li>Upgrade infrastructure to improve working conditions and create a conducive work environment to ensure sustained productivity and employee satisfaction</li> <li>Align the lifecycle of IT services and equipment (servers, used equipment) with objectives</li> <li>Ensure timely implementation of requirements to maintain EUCI at relevant level</li> <li>Review ENISA's geographically disperse IT solutions and systems and propose cost benefit solutions that would maximise ENISA's corporate resilience</li> <li>Follow up on the ServiceNow implementation and explore further synergies for integrating further services (HR, FM, EDO, etc)</li> <li>Follow up on AV implementation and upgrade of meeting rooms</li> </ul>	<ul style="list-style-type: none"> <li>Management Team</li> <li>IT Management Committee</li> <li>Budget Management Committee</li> <li>Staff Committee</li> </ul>	<p>Satisfaction survey for working environment</p> <p>Safety and security incidents reported at workplace in any of the 3 ENISA offices</p> <p>Average time for dealing with facilities management requests &gt;1</p>	<p>Annual</p>	<p>n/a</p> <p>n/a</p> <p>n/a</p>	<p>80 %</p> <p>&lt;3</p> <p>&lt;3 days</p>
<p>13.4 Enhance operational excellence and digitalisation through modern, safe and secure and streamlined ways of working and introducing self-service functionalities</p>	<ul style="list-style-type: none"> <li>Explore synergies between FM and Security service provision by integrating services via one service provider, hence reducing FWC numbers and provide all-inclusive services</li> <li>Implementation of an Identity and Access Management Solution to increase the Cybersecurity posture of the organisation</li> <li>Equipment renewal (laptops/mobiles) to ensure business continuity through updated technology, enhanced security measures and improved equipment performance</li> <li>Implement an effective backup solution (SAN) to enhance business continuity by safeguarding critical data, mitigating the risk of data loss and ensuring a swift operation recovery in the event of system failures, disasters or cyber-attacks</li> <li>Implement new A/V and conference equipment to bolster business continuity by facilitating seamless remote collaboration to ensure high-quality communication and collaboration, which is essential to maintain productivity and operational efficiency</li> <li>Implement of a cloud-based platforms and solutions automate IT delivery services, assure service availability, improve self-service functionalities and provide critical IT-related metrics enabling secure access and sharing of information or device from any location</li> <li>Upgrade physical security measures to ensure high standards for the other ENISA offices to get EUCI accreditation</li> <li>Further development of Athens data centre for high availability purposes to ensure the business continuation and minimisation of downtime risks</li> </ul>	<ul style="list-style-type: none"> <li>Management Team</li> <li>IT Management Committee</li> </ul>	<p>Resilience and quality of ENISA IT systems and services (automated or via surveys) [specific KPIs will be defined for each expected result of the output and will be monitored separately] – as generic indicators –</p> <ul style="list-style-type: none"> <li>Critical systems uptime/downtime</li> <li>Staff satisfaction with resolution</li> </ul>	<p>Annual</p>	<p>100 %</p> <p>84 %</p>	<p>99 %</p> <p>85 %</p>

## Stakeholders and engagement levels

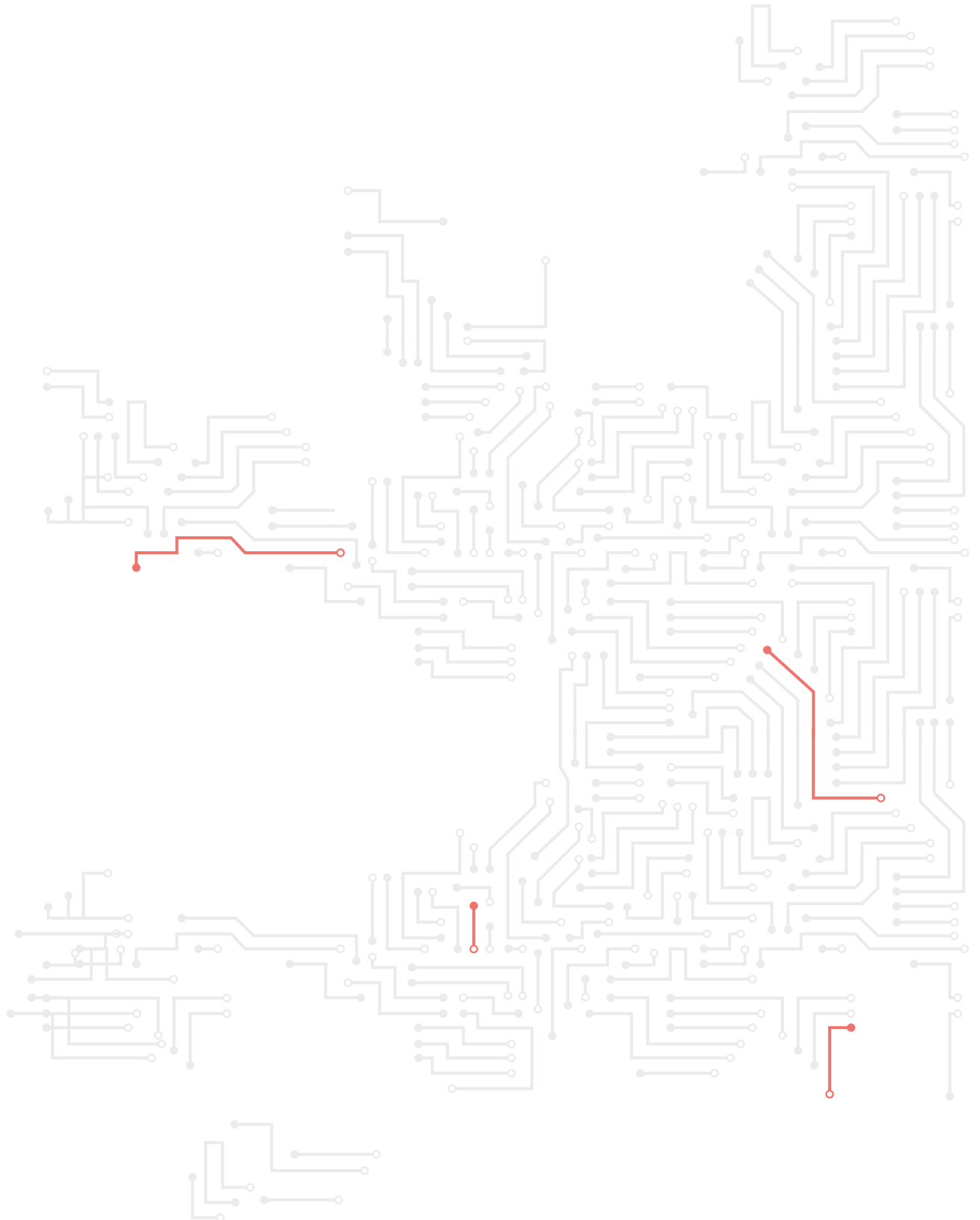


**Partners:** ENISA staff members and EUIBAs

**Involve / Engage:** Private sector and international organisations

RESOURCE FORECAST							
Outputs	Supporting service packages	CORE		ESSENTIAL		ON-DEMAND	
		FTE	EUR	FTE	EUR	FTE	EUR
Output 13.1				8.25	428 250		
Output 13.2				4.75	858 601		
Output 13.3				3.75	2 612 060		
Output 13.4				2.75	362 000		
Total	FTE: 19.50 Budget 4 260 911						
Actual resources used in previous year (2022)	FTE: 15 Budget: EUR 1 229 738 <sup>(73)</sup> (*) (*) Direct costs only: staff learning and development, staff welfare, books and newspapers, consultancy and travel expenditures linked to Activity 13						

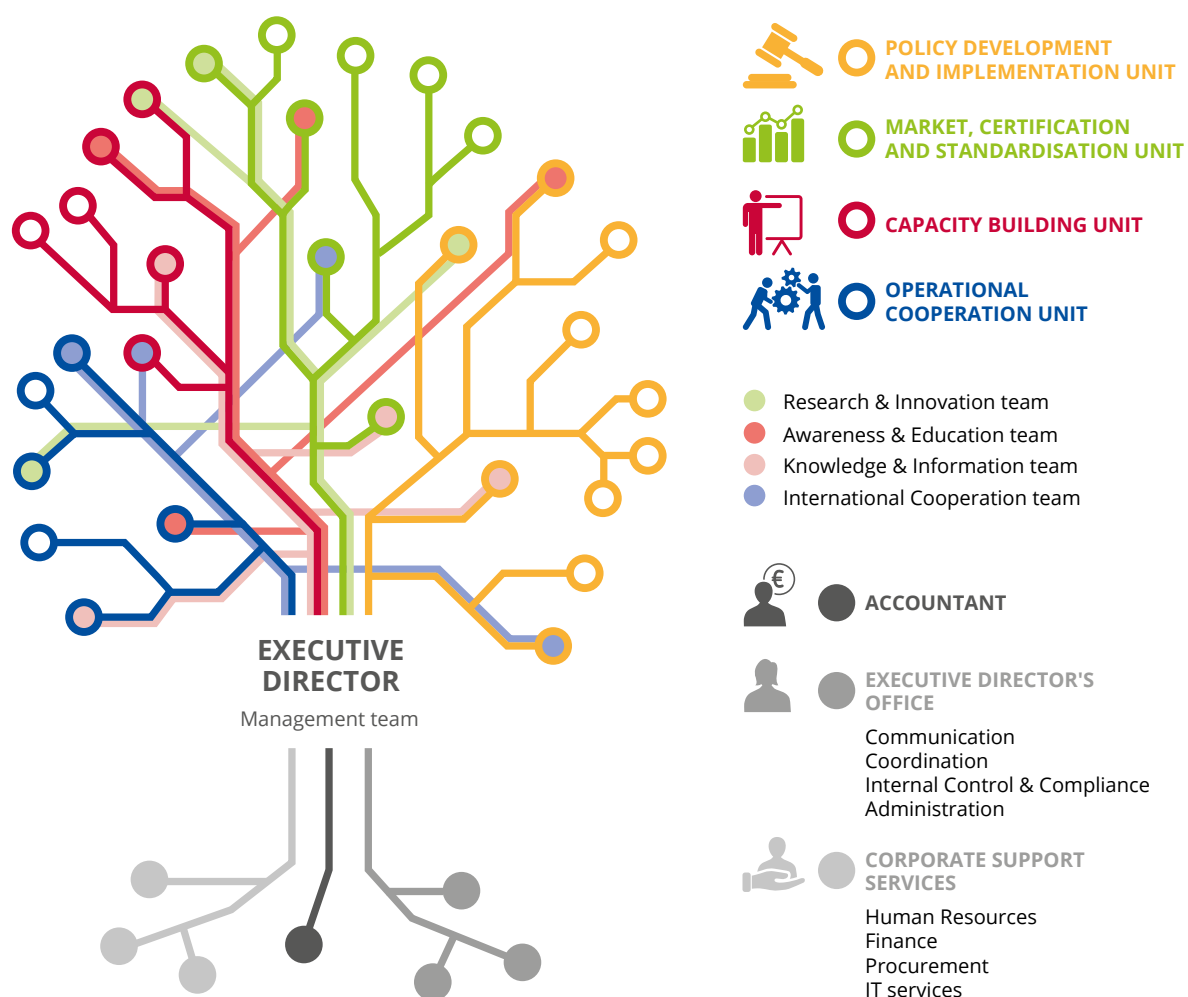
<sup>(73)</sup> Carried over into 2023: EUR 444 812.



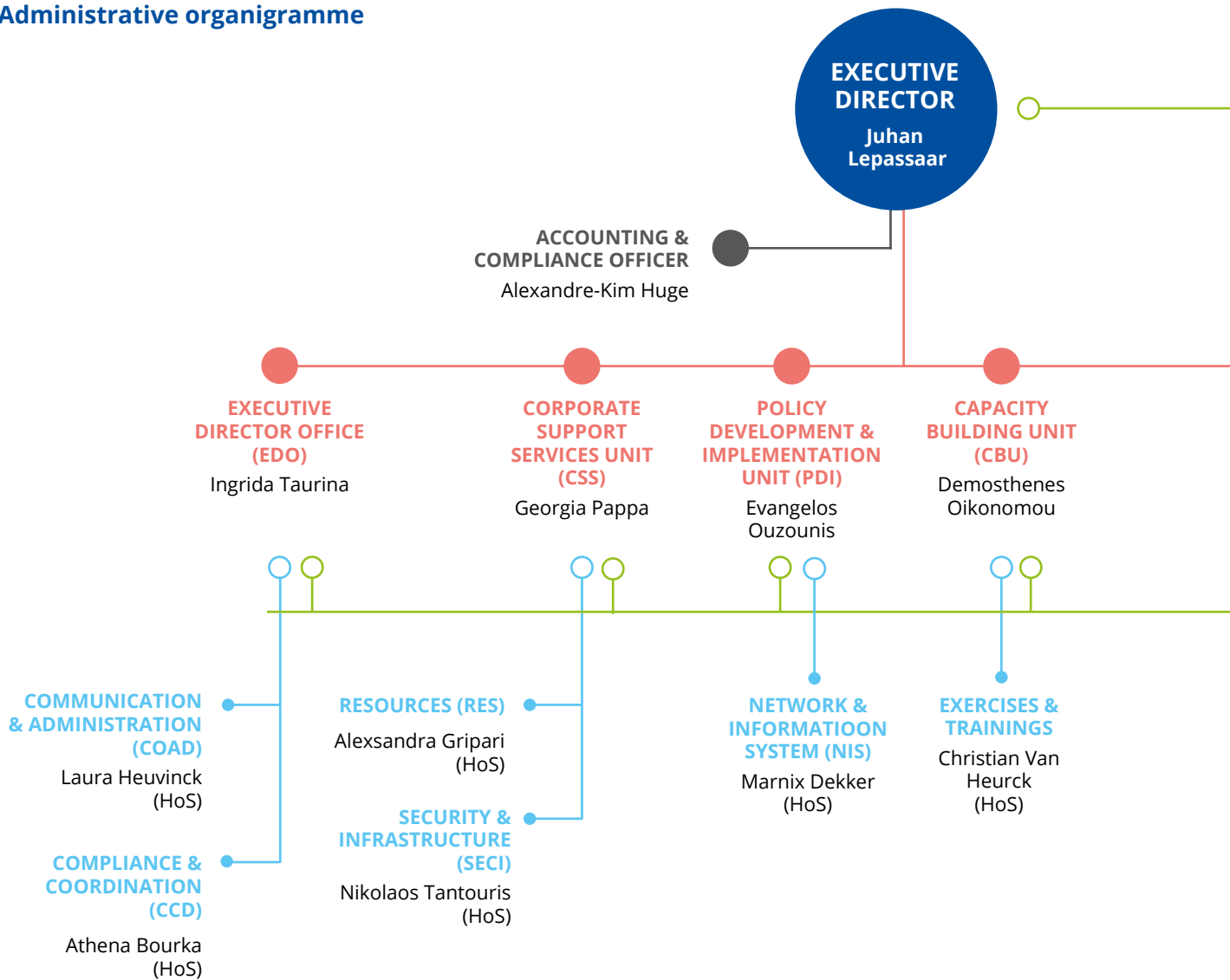
A

# ANNEX 1

## ORGANISATION CHART AS OF 1 DECEMBER 2022



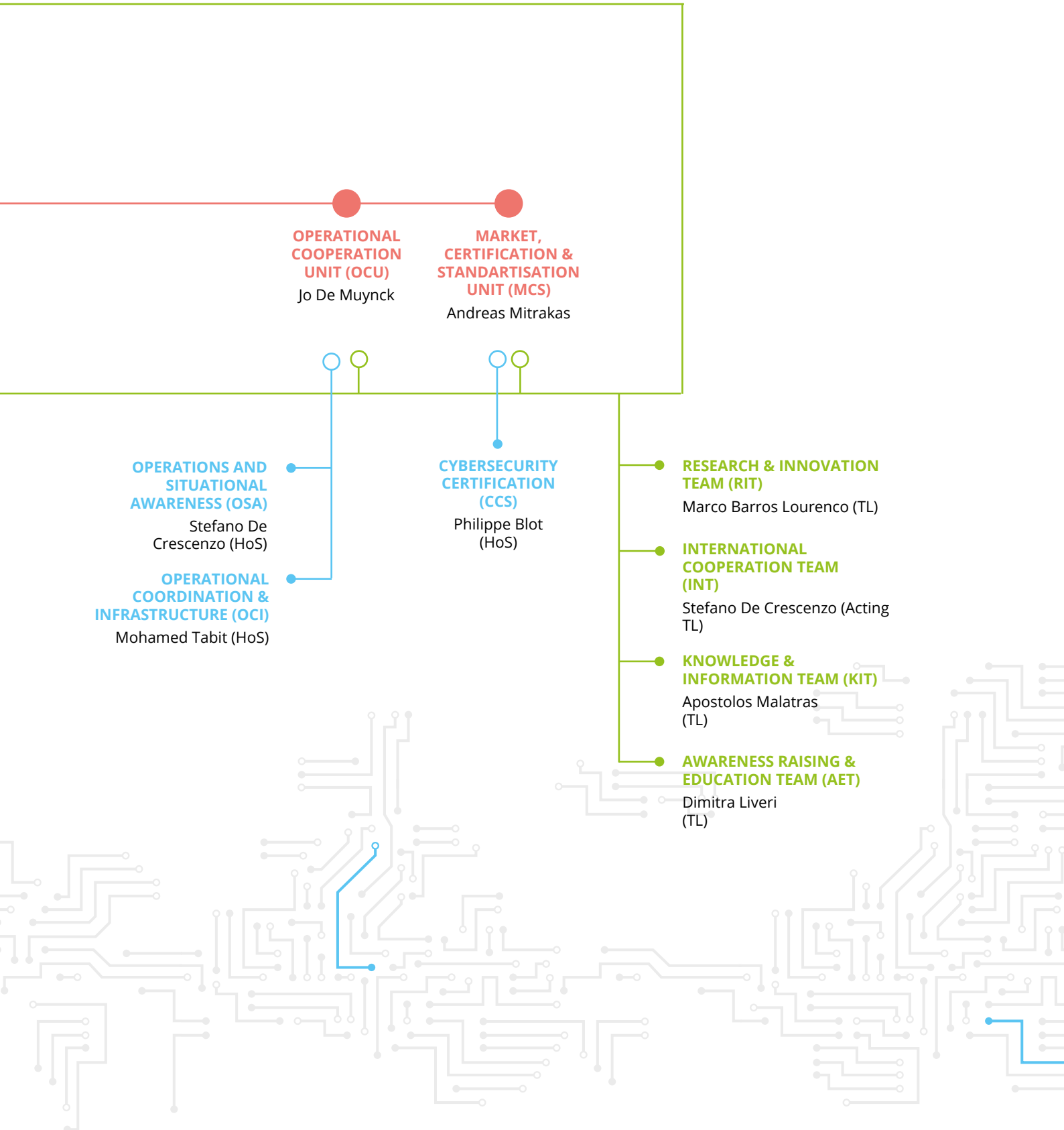
## Administrative organigramme



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







## ANNEX 2

# RESOURCE ALLOCATION PER ACTIVITY 2024–2026

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

The following assumptions are used in the simplified Activity Based Budgeting 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 2024–2026 single programming document (SPD) (carried out under Articles 5-12 of CSA) in terms of goods and services to be procured.
- Indirect budget is the cost estimate of salaries and allowances, buildings, information technology (IT), equipment and miscellaneous operating costs attributable to each activity. The indirect budget is allocated to activities based on different drivers. The main driver for costs allocation was the number of expected direct FTEs for each operational activity in 2024.
- In order to estimate the full costs of operational activities, the corporate activities (activities 11–13) shall be distributed accordingly to all operational activities based on respective drivers.

Table

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2024)	Activities as referred to in Section 3	Direct and Indirect budget allocation (in EUR)	FTE allocation
Providing assistance on policy development	Activity 1	1 038 153	4.96
Supporting implementation of Union policy and law	Activity 2	2 670 232	14.21
Building capacity	Activity 3	3 152 259	13.96
Enabling operational cooperation	Activity 4	3 280 613	10.96
Contributing to cooperative response at the EU and Member State (MS) level through effective situational awareness	Activity 5a	2 165 802	9.46
Contributing to cooperative response at the EU and MS level through <i>ex ante</i> and <i>ex post</i> services provision	Activity 5b	509 538	3.71
Development and maintenance of EU cybersecurity certification framework	Activity 6	1 904 535	9.71
Supporting European cybersecurity market and industry	Activity 7	1 256 347	7.21
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	1 804 214	7.96
Outreach and education	Activity 9	1 467 587	7.71
Research and innovation (R & I)	Activity 10	635 538	3.71
Performance and sustainability	Activity 11	1 874 064	11.21
Reputation and trust	Activity 12	1 046 543	4.96
Effective and efficient corporate services	Activity 13	3 031 048	18.21
<b>TOTAL</b>		<b>€25 836 475</b>	<b>128 <sup>(74)</sup></b>

<sup>(74)</sup> Includes three posts equally distributed across all activities (executive director (ED), accountant and advisor).

# ANNEX 3

## FINANCIAL RESOURCES

### 2024–2026

**Table 1. Revenue**

Revenue	2023	2024
EU contribution	24 475 757	24 953 071
Other revenue (EFTA)	707 738	883 404
Other revenue (SLAs, Annex XI)	p.m	174 604
<b>TOTAL</b>	<b>25 183 495</b>	<b>26 011 079</b>

Revenue	2023 adopted budget	VAR 2024 / 2023	Draft estimated budget 2024	Envisaged 2025	Envisaged 2026
1. Revenue from fees and charges					
2. EU contribution	24 475 757	1.95%	24 953 071	25 439 933	25 936 532
– of which assigned revenues deriving from previous years' surpluses **	320 868				
– of which Reserve conditional to approval of NIS2 Directive	707 738	24.82%	883 404	735 989	750 539
3. Third countries' contribution (including EEA/EFTA and candidate countries)	707 738	24.82%	883 404	735 989	750 539
– of which EEA/EFTA (excl. Switzerland)**					
– of which Candidate Countries		n/a			
4. Other contributions*					
5. Administrative operations					
– of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)					
6. Revenues from services rendered against payment***	P.M		174 604	174 604	174 604
7. Correction of budgetary imbalances					
<b>TOTAL REVENUES</b>	<b>25 183 495</b>	<b>3.29%</b>	<b>26 011 079</b>	<b>26 350 526</b>	<b>26 861 675</b>

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

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

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

**Table 2. Expenditure**

Expenditure (EUR)	2023		2024	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	12 719 412	12 719 412	14 739 106	14 739 106
Title 2	3 519 470	3 519 470	3 666 898	3 666 898
Title 3	8 944 613	8 944 613	7 430 471	7 430 471
<b>Total expenditure</b>	<b>25 183 495</b>	<b>25 183 495</b>	<b>25 836 475</b>	<b>25 836 475</b>

**Table 3. Expenditure details**

Expenditure (in EUR)	Commitment and Payment appropriations					
	Amended budget 2022 (**)	Adopted Budget 2023 Agency	Draft estimated Budget 2024 (*)	VAR 2024 / 2023	Envisaged in 2025	Envisaged in 2026
<b>Title 1. Staff Expenditure</b>	<b>11 917 868</b>	<b>12 719 412</b>	<b>14 739 106</b>	<b>16%</b>	<b>14 932 752</b>	<b>15 224 351</b>
11 Staff in active employment	9 862 695	11 019 993	13 058 316	18%	13 229 880	13 488 226
12 Recruitment expenditure	405 780	404 684	517 889	28%	524 693	534 939
13 Socio-medical services and training	1 101 619	923 735	754 501	-18%	764 413	779 341
14 Temporary assistance	547 774	371 000	408 400	4%	413 766	421 845
<b>Title 2. Building, equipment and miscellaneous expenditure</b>	<b>3 236 767</b>	<b>3 519 470</b>	<b>3 666 898</b>	<b>4%</b>	<b>3 715 075</b>	<b>3 787 621</b>
20 Building and associated costs	1 065 153	1 357 750	1 000 719	-26%	1 013 867	1 033 665
21 Movable property and associated costs (***)	64 285	0	0	n.a	0	0
22 Current corporate expenditure	480 593	472 650	516 125	9%	522 906	533 117
23 Corporate ICT	1 626 737	1 689 070	2 150 054	27%	2 178 302	2 220 839
<b>Title 3. Operational expenditure</b>	<b>9 052 990</b>	<b>8 944 613</b>	<b>7 430 471</b>	<b>-17%</b>	<b>7 528 094</b>	<b>7 675 099</b>
30 Activities related to meetings and missions	551 000	438 600	387 000	-12%	392 085	399 741
37 Core operational activities	8 501 990	8 506 013	7 043 471	-17%	7 139 010	7 275 358
<b>TOTAL EXPENDITURE</b>	<b>24 207 625</b>	<b>25 183 495</b>	<b>25 836 475</b>	<b>0%</b>	<b>26 175 921</b>	<b>26 687 071</b>

(\*) Does not amount (total of EUR 174 604) for possible revenue under SLAs with ECCC and EU-LISA, ref. Annex XI

(\*\*) Does not include the additional EUR 15 000 000 granted for Support Assistance Fund

(\*\*\*) As from 2023, "Movable property and associated costs" have been included in Chapter 21 and 22 for streamline purpose

## ADDITIONAL EU FUNDING: CONTRIBUTION AND SERVICE-LEVEL AGREEMENTS APPLICABLE TO ENISA

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

**Table 3. Budget outturn and cancellation of appropriations**

Budget outturn	2020	2021	2022
Revenue actually received (+)	21 801 460	23 058 211	39 227 392
Payments made (-)	-15 050 421	-17 989 374	-20 396 780
Carry-over of appropriations (-)	-6 200 614	-5 082 548	-18 836 095
Cancellation of appropriations carried over (+)	180 023	209 385	248 745
Adjustment for carry-over of assigned revenue appropriations carried over (+)	10 403	125 622	33 743
Exchange rate difference (+/-)	-1 291	-428	-17,88
<b>Total</b>	<b>739 560</b>	<b>320 868</b>	<b>276 988</b>

### Budget 2022 outturn amounts to EUR 276 988.

With a more than double budget increase from EUR 24.2 million to EUR 39.2 million during 2022, a commitment rate of 99.93 % (99.51 % in 2021) of appropriations of the year (C1 funds) at the end of the year has been reached, which shows the already proven capacity of the agency to fully implement its annual appropriations.

In 2022, commitment appropriations were cancelled for an amount of EUR 111 911 representing 0.49 % of the total budget.

The payment rate for the full budget of EUR 39.2 million was 52.02 %, while the payment rate for usual ENISA operations (without EUR 15 million Assistance Fund which was committed late December

2022) reached 84.11 % (in 2021 it was 77.40 %). The total amount including the Assistance Fund carried forward to 2023 is EUR 18 782 626.

No payment appropriations were cancelled during 2022.

The appropriations of 2021 carried over to 2022 were utilised at a rate of 95.07 % (automatic carry-overs) which indicates a satisfactory capability to estimate needs. From the EUR 5 048 805 carried forward, EUR 248 745 was cancelled (or 4.93 %). This cancellation represents 1.09 % of the total 2021 budget of EUR 22 721 149 (fund source C1).

## ANNEX 4

# HUMAN RESOURCES – QUANTITATIVE

The following is an overview of all categories of staff and their evolution

**Table 4. Staff population and its evolution – overview of all categories of staff**

**(a) Statutory staff and SNE**

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

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

Human resources	2021	2022	2023	2024	2025	2026
	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
CAs	n/a	n/a	n/a	10	10	10
SNEs	n/a	n/a	n/a	n/a	n/a	n/a
Total	n/a	n/a	n/a	10	10	10

<sup>(75)</sup> Article 38.2 of the ENISA Financial Rules allows the opportunity to 'offset the effects of part-time work'. ENISA will explore this option in 2024 and may use this option in the future to offset long-term absences and part-time work with short term CA contracts.

<sup>(76)</sup> Refers to TA, CA and SNE figures.

## Other human resources

### - Structural service providers

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

### - Interim workers

	Actually in place as of 31 December 2021	Actually in place as of 31 December 2022
Number	10	10



Table 5. Multiannual staff policy plan – years 2022–2026 <sup>(77)</sup>

Function group and grade	2022				2023		2024 <sup>(78)</sup>		2025		2026	
	Authorised budget		Actually filled as of 31 December 2022		Authorised		Envisaged		Envisaged		Envisaged	
	Perm. Posts	Temp. posts	Perm. Posts	Temp. posts	Perm. Posts	Temp. posts	Perm. Posts	Temp. posts	Perm. Posts	Temp. posts	Perm. Posts	Temp. posts
AD 16												
AD 15		1				1		1		1		1
AD 14				1								
AD 13		2		1		2		2		2		2
AD 12		4		4		4		4		4		4
AD 11		2		2		2		3		4		4
AD 10		4		1		4		4		3		3
AD 9		11		12		11		14		15		15
AD 8		22		8		25		15		24		24
AD 7		8		11		10		13		8		8
AD 6		9		15		4		7		2		2
AD 5												
AD TOTAL		63		55		63		63		63		63
AST 11												
AST 10												
AST 9										2		2
AST 8		2		2		2		3		4		4
AST 7		3		1		4		2		4		4
AST 6		8		5		7		7		6		6
AST 5		5		4		5		4		4		4
AST 4		1		4		1		2		0		0
AST 3				1				1				
AST 2				1								
AST 1												
AST TOTAL		19		18		19		19		19		19
AST/SC 6												
AST/SC 5												
AST/SC 4												
AST/SC 3												
AST/SC 2												
AST/SC 1												
AST/SC TOTAL												
TOTAL		82		73		82		82		82		82
Grand TOTAL		82		73		82		82		82		82

<sup>(77)</sup> The change in the number of establishment plan up to 10% requested can be modified as per Article 38 of the ENISA Financial Regulation. In 2024, ENISA will review its staffing strategy and will update a forecast for reclassification also in line with job mapping.

<sup>(78)</sup> To be updated after the 2024 EU budget has been adopted.

## External personnel

### CAs

CAs	FTE corresponding to the authorised budget for 2022	Executed FTE as of 31 December 2022	FTE corresponding to the authorised budget for 2023	FTE corresponding to the authorised budget for 2024	FTE corresponding to the authorised budget for 2025	FTE corresponding to the authorised budget for 2026
Function Group IV	30	19	30	30	30	30
Function Group III	2	7	2	2	2	2
Function Group II	0	0	0	0	0	0
Function Group I	0	1	0	0	0	0
<b>Total</b>	<b>32</b>	<b>27</b>	<b>32</b>	<b>32</b>	<b>32</b>	<b>32</b>

### SNEs

CAs	FTE corresponding to the authorised budget for 2022	Executed FTE as of 31 December 2022	FTE corresponding to the authorised budget for 2023	FTE corresponding to the authorised budget for 2024	FTE corresponding to the authorised budget for 2025	FTE corresponding to the authorised budget for 2026
<b>Total</b>	<b>12</b>	<b>10</b>	<b>14</b>	<b>14</b>	<b>14</b>	<b>14</b>

**Table 6. Recruitment forecasts for 2024 following retirement/mobility or new requested posts**

Job title in the agency	Type of contract (Official, TA or CA)		TA/Official		CA
			Function group/grade of internal (brackets) and external (single grade) recruitment foreseen for publication (*)		Recruitment function group (I, II, III and IV)
	Due to expected retirement/ mobility	New post requested due to additional tasks <sup>(79)</sup>	Internal	External	
Expert		8 TAs and 2 SNEs	n/a	n/a	n/a
Officer		4 TAs	n/a	n/a	n/a
Assistant		1 TA	n/a	n/a	n/a

<sup>(79)</sup> Posts stemming from the resource shortfall identified for the 2024 work programme (15 FTEs).

## ANNEX 5

# HUMAN RESOURCES – QUALITATIVE

## A. RECRUITMENT POLICY

### Implementing rules in place

		Yes	No	If no, which other implementing rules are in place?
<b>Engagement of CAs</b>	Decision C(2019)3016	x		
<b>Engagement of TAs</b>	Decision C(2015)1509	x		
<b>Middle management</b>	Decision C(2018)2542	x		
<b>Type of posts</b>	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?
<b>Reclassification of TAs</b>	Decision C(2015)9560	x		
<b>Reclassification of CAs</b>	Decision C(2015)9561	x		

**Table 7. Reclassification of TAs / promotion of officials**

Average seniority in the grade among reclassified staff								
Grades	2017	2018	2019	2020	2021	2022	Actual average over 5 years	Average over 5 years (according to decision C(2015)9563)
AD 5	—	—	—	—	—	—	—	2.8
AD 6	1	2	3	—	1	1	3.8	2.8
AD 7	—	—	—	1	—	2	3	2.8
AD 8	1	1	1	2	1	2	4,1	3
AD 9	—	1	—	—	—	—	10	4
AD 10	—	—	—	—	—	2	10.5	4
AD 11	—	—	—	—	—	—	—	4
AD 12	—	—	—	—	1	—	10	6.7
AD 13	—	—	—	—	—	—	—	6.7
AST 1	—	—	—	—	—	—	—	3
AST 2	—	—	—	—	—	—	—	3
AST 3	1	1	1	—	—	1	5.2	3
AST 4	1	1	1	1	—	—	4.33	3
AST 5	—	1	—	—	1	—	5.5	4
AST 6	—	—	—	1	1	—	3.5	4
AST 7	—	—	—	—	1	1	4	4
AST 8	—	—	—	—	—	—	—	4
AST 9	—	—	—	—	—	—	—	n/a
AST 10 (senior assistant)	—	—	—	—	—	—	—	5
There are no AST/SCs at ENISA: n/a								
AST/SC 1								4
AST/SC 2								5
AST/SC 3								5.9
AST/SC 4								6.7
AST/SC 5								8.3

Table 8. Reclassification of CA staff

Function group	Grade	Staff in activity at 31 December 2022	How many staff members were reclassified in year 2022	Average number of years in grade of reclassified staff members	Average number of years in grade of reclassified staff members according to Decision C(2015)9561
CA IV	17	1	-	-	Between 6 and 10 years
	16	4	-	-	Between 5 and 7 years
	15	6	1	4	Between 4 and 6 years
	14	7	1	5.8	Between 3 and 5 years
	13	1	-	-	Between 3 and 5 years
CA III	12	1	-	-	-
	11	1	-	-	Between 6 and 10 years
	10	4	1	3	Between 5 and 7 years
	9	1	1	3	Between 4 and 6 years
	8	0	-	-	Between 3 and 5 years
CA II	6	-	-	-	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
CA I	3	1	-	-	n/a
	2	-	-	-	Between 6 and 10 years
	1	-	-	-	Between 3 and 5 years

## C. GENDER REPRESENTATION

**Table 9: Data on 31 -12- 2022 statutory staff (only TAs and CAs on 31 -12- 2022)**

		Official		TAs		CA		Grand total	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	-	-	21	29 %	11	41 %	32	32 %
	Assistant level (AST and AST/SC)	-	-	12	16 %	4	15 %	16	16 %
	<b>Total</b>	-	-	33	45 %	15	56 %	48	48 %
Male	Administrator level	-	-	34	47 %	8	29 %	42	42 %
	Assistant level (AST and AST/SC)	-	-	6	8 %	4	15 %	10	10 %
	<b>Total</b>	-	-	40	55 %	12	44 %	52	52 %
<b>Grand total</b>		-	-	73	100 %	27	100 %	100	100 %

**Table 10. Data regarding the gender evolution over 5 years of the middle and senior management (31 December 2022)**

	2018		31.12.2022	
	Number	%	Number	%
Female managers	2	22 %	2 <sup>(80)</sup>	29 %
Male managers	7	78 %	5 <sup>(81)</sup>	71 %

The focus of the agency being cybersecurity hints at the reason for a certain gender imbalance. Nevertheless, an improvement has been noted during the past 5 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 coming years

<sup>(80)</sup> This category comprises the ED and head of unit (HoU) level (TLs not included).

<sup>(81)</sup> This category comprises the ED and HoU level (TLs not included).

## D. GEOGRAPHICAL BALANCE

**Table 11. Data on 31 December 2022 – statutory staff only**

Nationality	AD + CA FG IV		AST/SC- AST + CA FGI / CA FGII / CA FGIII		Total	
	Number	% of total staff members in AD and FG IV categories	Number	% of total staff members in AST SC/AST and FG I, II and III categories	Number	% of total staff
Belgium	5	7 %	1	4 %	6	6 %
Bulgaria	2	3 %	0	0 %	2	2 %
Czechia	1	1 %	0	0 %	1	1 %
Germany	2	3 %	0	0 %	2	2 %
Double * <sup>(82)</sup>	4	5 %	3	12 %	7	7 %
Estonia	1	1 %	0	0 %	1	1 %
Greece	27	36 %	14	54 %	41	41 %
Spain	4	5 %	0	0 %	4	4 %
France	4	5 %	1	4 %	5	5 %
Italy	6	8 %	0	0 %	6	6 %
Cyprus	2	3 %	2	8 %	4	4 %
Latvia	2	3 %	0	0 %	2	2 %
Lithuania	0	0 %	1	4 %	1	1 %
Netherlands	2	3 %	0	0 %	2	2 %
Poland	3	4 %	1	4 %	4	4 %
Portugal	2	3 %	1	4 %	3	3 %
Romania	6	8 %	1	4 %	7	7 %
Slovakia	0	0 %	1	4 %	1	1 %
Sweden	1	1 %	0	0 %	1	1 %
<b>Total</b>	<b>74</b>	<b>100 %</b>	<b>26</b>	<b>100 %</b>	<b>100</b>	<b>100 %</b>

**Table 12. Evolution over 5 years of the most represented nationality in the agency**

Most represented nationality	2017		31.12.2022	
	Number	%	Number	%
Greek	27 (out of 71)	38	41 (out of 100)	41.0

## E. Schooling

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

<sup>(82)</sup> Double nationalities also comprise staff members who also have non-EU nationalities (i.e. Italian/australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek, etc.).

# ANNEX 6

## ENVIRONMENT MANAGEMENT

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

In 2021, the MB of ENISA established – within the Agency's SPD for 2022–2025 – a goal for the agency to achieve climate neutrality (defined as zero CO<sub>2</sub>, methane and nitrous oxide emissions) across all its operations by 2030. As a first step, in 2022 the agency undertook an exercise to map its current climate footprint. Based on an audit of past ENISA emissions for which 2019 and 2021 were used as reference years, it was established that ENISA creates 584 485 greenhouse gas emissions (tonnes of CO<sub>2</sub> equivalent (tnCO<sub>2</sub>eq)) annually, with indirect emissions from purchased electricity (50.33 %) and air travel (36.80 %) being the main sources of impact on the climate.

Furthermore, the audit established that energy emissions per employee in Athens constitute 1 435 tnCO<sub>2</sub> per employee whereas energy emissions per employee in Heraklion constitute 10 times as much (14 217 tnCO<sub>2</sub>/emp). While ENISA staff undertook 770 journeys by air (ENISA staff missions) in 2019, the agency also organised 79 in-person meetings in 2019 (and 125 in-person or hybrid/online meetings in 2022). It operated almost entirely online throughout the period from March 2020 to May 2022.

On its path to achieve climate neutrality, a 41 % 'automatic' reduction of greenhouse gas emissions in comparison to the base year transitional emissions (2019, 2021) is expected due to external factors (reforms undertaken by the host country – Greece). The remaining 59 % or 413 tnCO<sub>2</sub>eq will be tackled by ENISA itself, a) through changing and evolving its business practices to lessen their impact on the climate (less in-person participation in meetings or events) and b) by offsetting emissions if activities cannot be transformed without undermining the

objectives of ENISA's operational mandate. This is pursued under the condition that offsetting is used only when other options have been exhausted.

In order to ensure that ENISA is on the correct path towards climate neutrality by 2030 and to promote and enhance ecological sustainability across all the agency's operations, the following key performance indicators (KPIs) have been adopted within its corporate strategy.

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



# ANNEX 7

## BUILDING POLICY

### CURRENT BUILDINGS

Building name and type	Location	Location surface area (in m <sup>2</sup> )			Rental contract			Host country (grant or support)	Building present value (EUR)
		Office space (m <sup>2</sup> )	non-office (m <sup>2</sup> )	Total (m <sup>2</sup> )	Rent (EUR per year)	Duration	Type		
<b>Heraklion office</b>	<b>Heraklion</b>	706		706		1 January 2021 to 28 February 2030	Lease	Rent is fully covered by Hellenic authorities	N/a
<b>Athens office</b>	<b>Chalandri</b>	4 498	2 617	7 115		1 January 2021 to 28 February 2030	Lease	Rent is fully covered by Hellenic authorities	N/a
<b>Brussels office</b>	<b>Brussels centre</b>	98		98	56 496	N/a	SLA with Office for Infrastructure and Logistics in Brussels		N/a
<b>Total</b>	<b>Location</b>	5 302	2 617	7 920					

### BRUSSELS OFFICE

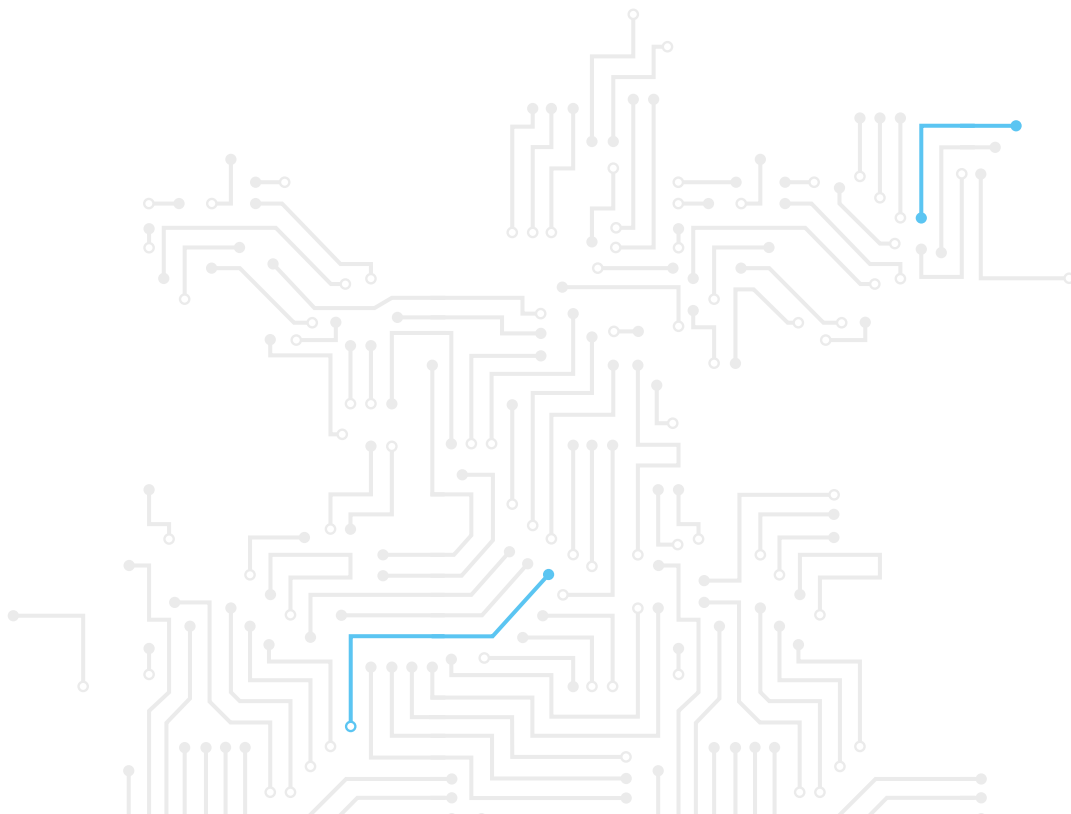
The Brussels office was completed in April 2022 and has been operational since then. The office is used on a daily basis by Brussels-based staff, which is of significant benefit for the Operational Cooperation Unit as they are able to communicate easily with the Computer Emergency Response Team for EUIBAs (CERT-EU) 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) on its Brussels premises. The second phase of implementation is likely to continue into Q4 2023. Indicative resources expected are as follows.

Resources (indicative)	2023	2024	2025	2026
Head count (FTEs)	12–13	12–13	12–13	13–14
Budget (one-off and maintenance costs)	130 000	130 000	130 000	130 000

# ANNEX 8

## PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education/day care
<p>In accordance with Article 23 of Regulation (EU) 2019/881, Protocol No 7 on the privileges and immunities of the European Union annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union applies to the agency and its staff.</p> <p>The Greek government and ENISA signed a Seat Agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 4 October 2019 and is applicable to ENISA and its staff.</p>	<p>In accordance with Article 35 of Regulation (EU) 2019/881, Protocol No 7 on the privileges and immunities of the European Union annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union applies to the agency and its staff.</p> <p>The Greek government and ENISA signed a Seat Agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 4 October 2019 and is applicable to ENISA and its staff.</p>	<p>A public school of European education, type 2, was founded in 2005 by the Greek government in Heraklion, Crete, for the children of the staff of ENISA.</p> <p>There is no European School operating in Athens.</p>



# ANNEX 9

## EVALUATIONS

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

ENISA's mandate requires that the agency carry out its tasks while avoiding the duplication of MS activities, therefore the result that 83.7 % of stakeholders find that ENISA deliverables do not duplicate or only somewhat duplicate MS activities is tantamount to ENISA's efforts to involve stakeholders in all stages of its work and ensure that the outcomes/results are fit for purpose. However, duplication in some areas is unavoidable due to the nature of the work and the need for MSs to have their own capacities, thus ENISA will take action to increase efforts to focus its work even more on high added-value / low duplication areas and has specifically introduced targets in the work programme to reduce duplication of MS activities.

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

# ANNEX 10

## STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

As adopted by the MB <sup>(83)</sup>, the agency's strategy for effective internal controls is based on international practices (Committee of Sponsoring Organizations of the Treadway Commission Framework's international standards) and on the relevant internal control framework (ICF) of the 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 (MT) sets the tone at the top with respect to the importance of the internal controls, including expected standards of conduct.

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

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

Information is necessary for the agency to carry out internal controls and to support the achievement of objectives. In this respect, it is necessary to consider both external and internal communication. External communication provides the Agency's stakeholders

and globally the EU citizens with information on ENISA's policy, objectives, actions and achievements. Internal communication provides ENISA staff with the information required to support the achievement of objectives and the awareness for day-to-day controls.

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

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

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

---

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

<sup>(84)</sup> <https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2021-5-on-anti-fraud-strategy>.

## ANNEX 11

# PLAN FOR GRANT, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS

	Date of signature	Total amount	Duration	Counter-part	Short description	FTEs
<b>Service level agreements</b>						
SLA with ECCC	20/12/22	54 604	1 year	ECCC	The scope of this Service Level Agreement covers support services offered by ENISA to ECCC: data protection officer, accounting officer	0.4 FTEs
SLA with eu-LISA M-CBU-23-C35	13/7/23	120 000	31/12/23	eu-LISA	The scope of this Service Level Agreement covers support services offered by ENISA to eu-LISA on the planning, execution and evaluation of upcoming annual exercises	2 FTEs
<b>Contribution agreements</b>						
Support Action fund	draft	est. 20 M	up to 31/12/25	DG CNECT	The purpose of this Agreement is to provide a financial contribution to implement the action "Incident Response Support and Preparedness for Key Sectors" which is composed of three activities: 1) EU-level cyber reserve with services from trusted private providers for incident response; 2) penetration tests in key sectors and 3) the Party's contribution to the Cyber Analysis and Situation Centre.	est. 13.5 FTEs

## ANNEX 12

# STRATEGY FOR COOPERATION WITH NON-EU COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

The international strategy confirms the agency's mandate in terms of its focus on the EU and EU actors, while also allowing increased flexibility to engage with international partners in line with the strategic objectives outlined in the ENISA strategy for a trusted and cyber secure Europe of July 2020 and in support of the EU's international priorities. The agency's international strategy <sup>(85)</sup> was adopted by the MB during the November 2021 meeting.

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

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

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

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

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

---

<sup>(85)</sup> <https://www.enisa.europa.eu/publications/corporate-documents/enisa-international-strategy>

# ANNEX 13

## ANNUAL COOPERATION PLAN 2024



The 2024 annual cooperation plan between ENISA and CERT-EU will be annexed to the 2024–2026 SPD as a separate document.



# NOTES



# NOTES



# NOTES





## ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: [enisa.europa.eu](https://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

#### Brussels Office

Rue de la Loi 107  
1049 Brussels, Belgium

[enisa.europa.eu](https://enisa.europa.eu)



Publications Office  
of the European Union



ISBN 978-92-9204-663-7