



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

# ENISA SINGLE PROGRAMMING DOCUMENT 2023–2025

Including multiannual planning,  
work programme 2023 and  
multiannual staff planning



JANUARY 2023

## CONTACT

For contacting ENISA please use the following details:

info@enisa.europa.eu

website: www.enisa.europa.eu

## LEGAL NOTICE

This publication presents the European Union Agency for Cybersecurity (ENISA) Single Programming Document 2022–2024 as approved by the Management Board in Decision No MB/2010/17. The Management Board may amend the Work Programme 2022–2024 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), 2022

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, 2022

<b>Print</b>	ISBN 978-92-9204-626-2	ISSN 2467-4397	doi: 10.2824/52222	TP-AH-23-001-EN-C
<b>PDF</b>	ISBN 978-92-9204-625-5	ISSN 2467-4176	doi: 10.2824/870602	TP-AH-23-001-EN-N



# ENISA SINGLE PROGRAMMING DOCUMENT 2023–2025

EUROPEAN UNION AGENCY  
FOR CYBERSECURITY



# TABLE OF CONTENTS

List of acronyms	5
Foreword	6
Mission statement	8
Strategy	9
<b>FORESIGHT</b>	<b>10</b>
<b>KNOWLEDGE</b>	<b>11</b>
<b>SECTION I</b>	
<b>GENERAL CONTEXT</b>	<b>13</b>
<b>LEGISLATIVE MEASURES DESIGNED TO STRENGTHEN THE RESPONSE TO THE THREAT LANDSCAPE</b>	<b>15</b>
<b>FURTHER DEVELOPMENTS</b>	<b>19</b>
<b>SECTION II</b>	
<b>MULTI-ANNUAL PROGRAMMING 2023–2025</b>	<b>21</b>
<b>2.1. MULTI-ANNUAL WORK PROGRAMME</b>	<b>21</b>
<b>2.2. HUMAN AND FINANCIAL RESOURCES – OUTLOOK FOR YEARS 2023–2025</b>	<b>28</b>
2.2.1. Overview of the past and current situation	28
2.2.2. Outlook for the years 2023–2025	29
<b>2.3. RESOURCE PROGRAMMING FOR THE YEARS 2023–2025</b>	<b>31</b>
2.3.1. Financial Resources	31
2.3.2. Human Resources	32
<b>2.4. STRATEGY FOR ACHIEVING GAINS IN EFFICIENCY</b>	<b>33</b>
<b>SECTION III</b>	
<b>WORK PROGRAMME 2023</b>	<b>37</b>
<b>3.1. OPERATIONAL ACTIVITIES</b>	<b>38</b>
<b>3.2. CORPORATE ACTIVITIES</b>	<b>71</b>
<b>ANNEX 1</b>	
<b>ORGANISATION CHART AS OF 1 JANUARY 2022</b>	<b>81</b>
<b>ANNEX 2</b>	
<b>RESOURCE ALLOCATION PER ACTIVITY 2023–2025</b>	<b>84</b>

<b>ANNEX 3</b> <b>FINANCIAL RESOURCES 2023–2025</b>	<b>86</b>
<b>ANNEX 4</b> <b>HUMAN RESOURCES – QUANTITATIVE</b>	<b>89</b>
<b>ANNEX 5</b> <b>HUMAN RESOURCES – QUALITATIVE</b>	<b>93</b>
<b>A. RECRUITMENT POLICY</b>	<b>93</b>
<b>B. APPRAISAL AND RECLASSIFICATION/PROMOTIONS</b>	<b>93</b>
<b>C. GENDER REPRESENTATION</b>	<b>96</b>
<b>D. GEOGRAPHICAL BALANCE</b>	<b>97</b>
<b>E. SCHOOLING</b>	<b>98</b>
<b>ANNEX 6</b> <b>ENVIRONMENT MANAGEMENT</b>	<b>99</b>
<b>ANNEX 7</b> <b>BUILDING POLICY</b>	<b>100</b>
<b>ANNEX 8</b> <b>PRIVILEGES AND IMMUNITIES</b>	<b>102</b>
<b>ANNEX 9</b> <b>EVALUATIONS</b>	<b>103</b>
<b>ANNEX 10</b> <b>STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS</b>	<b>104</b>
<b>ANNEX 11</b> <b>PLAN FOR GRANT, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS</b>	<b>106</b>
<b>ANNEX 12</b> <b>STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS</b>	<b>107</b>
<b>ANNEX 13</b> <b>ANNUAL COOPERATION PLAN 2023</b>	<b>108</b>

# LIST OF ACRONYMS

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



## FOREWORD

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

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

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

Secondly, building on the outcomes of strategic discussions within its Management Board throughout 2022, the Agency has developed service packages in key areas of its mandate. They integrate ENISA's various outputs across different activities, help the agency to prioritise its actions, build and make use of internal synergies, and ensure that adequate resources are reserved across the Agency in a transparent manner.

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



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

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

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

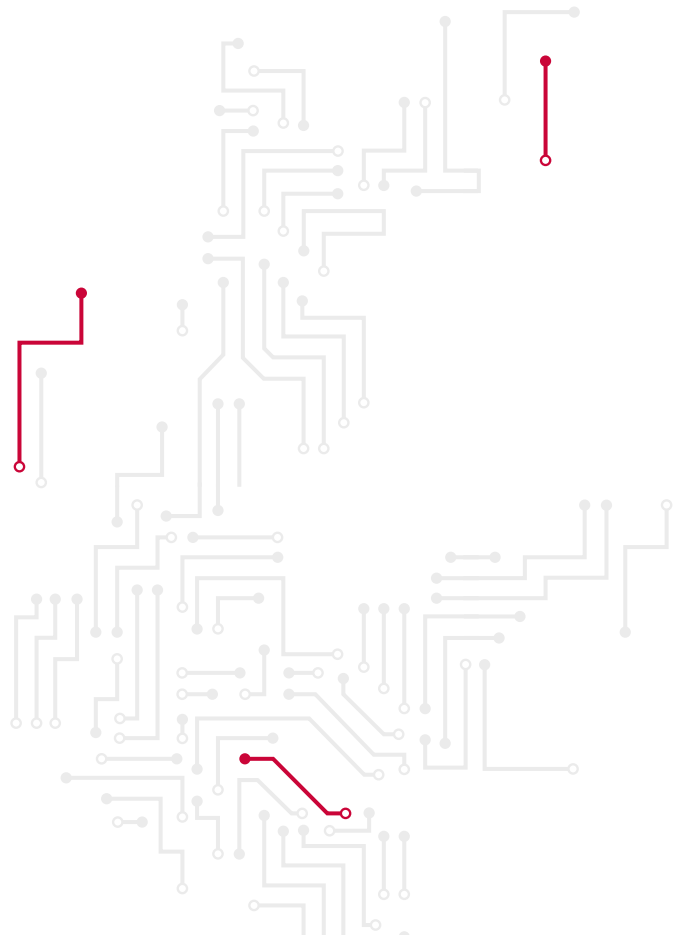
The EU has been mastering cybersecurity initiatives and structures not least through a unique general consensus across parties and across Member States as its prime driving force. This consensus should now also include the resourcing of the Agency. This would give the Union the ability it needs to steer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

**Juhan Lepassaar**  
Executive Director

# MISSION STATEMENT

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

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



# STRATEGY

## CYBERSECURITY POLICY

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

## OPERATIONAL COOPERATION

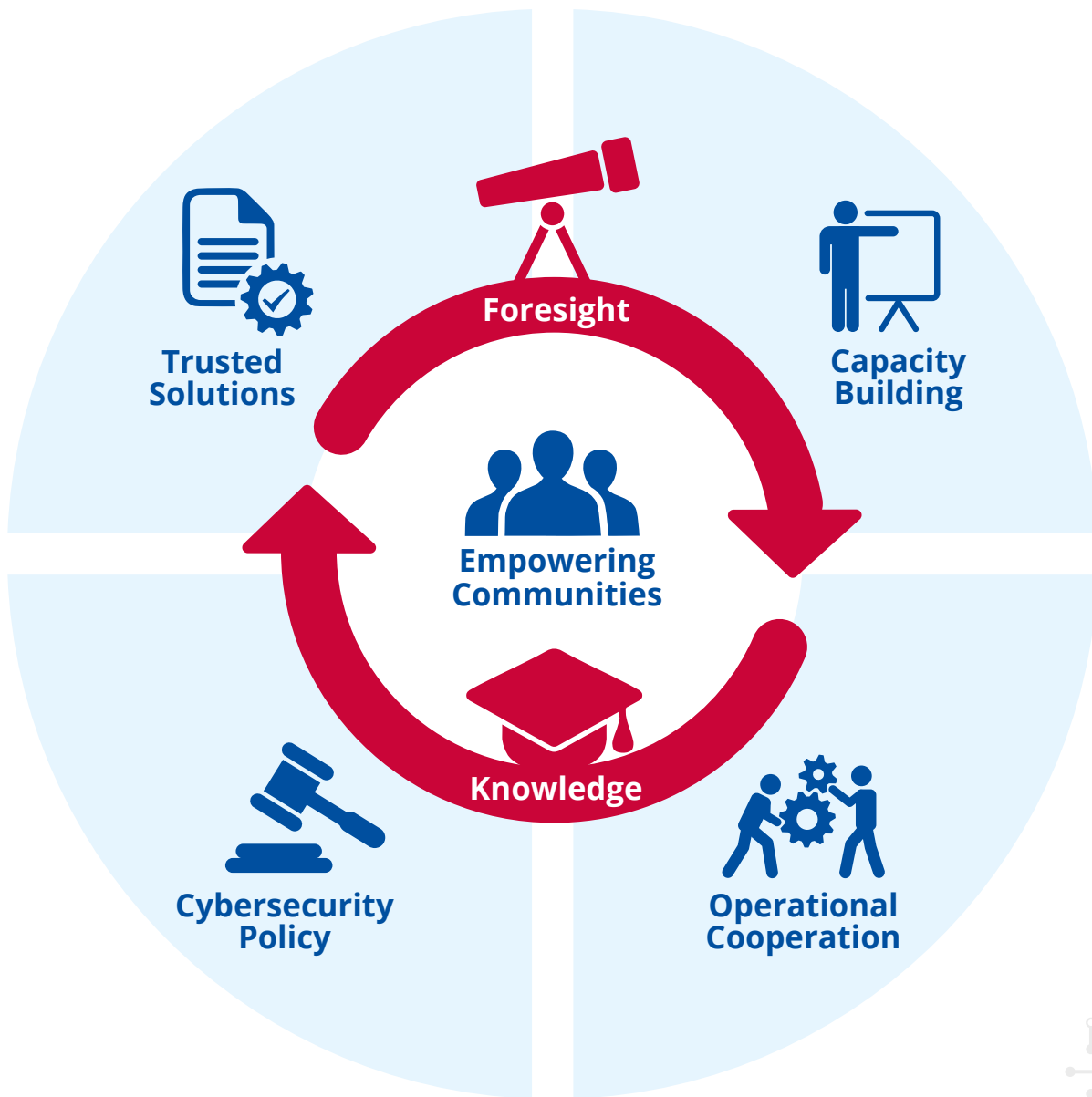
The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large-scale and cross-border) cyber-attacks and cyber crisis.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

## CAPACITY BUILDING

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

## TRUSTED SOLUTION

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



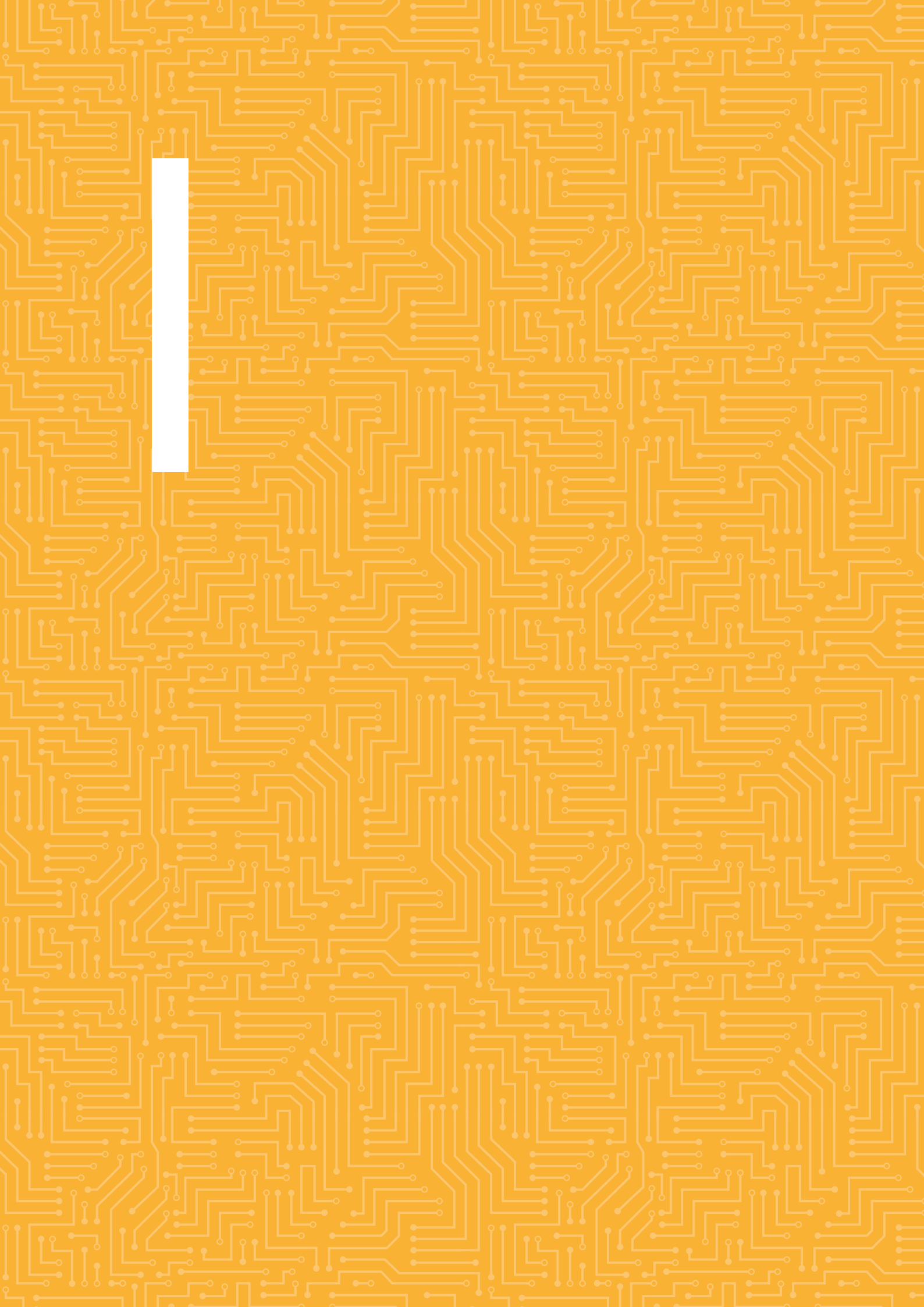
## FORESIGHT

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

## KNOWLEDGE

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





# SECTION I

## GENERAL CONTEXT

The Russian war of aggression against Ukraine dominates today's EU security agenda and threatens global stability and security. ENISA has stepped up its coordination and preparedness and contributed to the EU's shared situational awareness by providing regular situational reports on cyber activity. There has also been intensified coordination and exchange of information with cybersecurity networks, such as the Cyber Crises Liaison Organisation Network (CyCLONe) consisting of national cybersecurity crisis management authorities, and numerous sectorial communities supported by ENISA. In addition, constant efforts have ensured that channels of communication between the political, operational and technical levels, as well as enhanced cooperation with the Computer Security Incident Response Teams (CSIRT) Network were realised.

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

### ENISA cybersecurity support action

While the implementation of a new 'Emergency Response Fund for Cybersecurity' is under assessment and may require further deliberations, DG CONNECT allocated EUR 15 million to support Member States in the short term in view of the immediate and elevated threat of malicious cyber activities due to the ongoing Russian war of aggression against Ukraine. The EU needs to respond to these threats and be prepared to respond to cyberattacks.

This short-term support aims to complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, by providing ENISA with additional means to support preparedness (ex-ante), and response (ex-post) to large-scale cybersecurity incidents. As such, regular tasks in the work programmes under activities 3, 4 and 5 have been expanded to continue this support well into 2023.

### Service catalogue

In 2022 the Agency introduced the concept of a service catalogue to allow management to focus efforts and resources in a highly structured and more efficient manner for attaining specific objectives. The ENISA service catalogues are organised into individual service packages. A service package is a collection of

cybersecurity products and services that span across a number of activities and contribute to the objectives of a discrete service package. A service package is a means of centralising all services that are important to the stakeholders that use it.

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

- NIS directive (NIS);
- Training and exercises (TREX);
- Situational Awareness (SITAW);
- Certification (CERTI);
- Cybersecurity index (INDEX).

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

ENISA's annual Threat Landscape (ETL) for 2022 marks the 10th iteration of this flagship report and will be published in October 2022. ETL 2022 looked at threats across the EU and the world in the period starting July 2021 and finishing in July 2022.

The major highlights include an increase in threats against availability and the persistence of ransomware as one of the prime threats, despite ongoing efforts to tackle it. Threats against availability increased significantly, targeting the provisioning of services (telecommunications and energy in particular) and the major motivation behind relevant incidents that involve disruption of service.

When it comes to ransomware, a dedicated threat landscape was published in July 2022 noting the importance of this threat. Approximately 10 terabytes of data are stolen each month by ransomware threat actors and 58.2% of the data stolen includes employees' personal data. While at least 47 distinct threat actors who use ransomware were identified, for 94.2% of incidents we do not know whether the company paid the ransom or not. It is estimated however that 62.12% of companies either came to an agreement with the attackers or found another solution. In most cases the affected organisations are unaware of how threat actors managed to gain initial access.

The latter two findings highlight issues in incident reporting; when it comes to ransomware incidents only the tip of the iceberg is reported.

In 2022, a notable increase in the activities of state-sponsored and proxy threat actors was observed,

attributed to the volatile geopolitical environment and the war in Ukraine in particular. It is important to highlight the inclusion of an analysis of the vulnerability landscape and the impact and motivation per sector that were part of the ETL for the first time in 2022.

ENISA continues to constantly monitor the cybersecurity threat landscape using an open and transparent methodology that was made available to the public in June 2022. This initiative aims to promote transparency in ENISA's work, build confidence and support capacity building across MSs.

It is in the context of such challenges that ENISA is exploring ways to improve the reporting of incidents. The revised Network and Information Security Directive (NIS2) is expected to change the way cybersecurity incidents are notified. The new provisions will aim to support a better mapping and understanding of the relevant incidents.

## NIS Investments 2022

The 3rd ENISA NIS Investments study is scheduled for publication in November 2022 and offers additional insights into the cybersecurity budgets of Operators of Essential Services (OES) and Digital Service Providers (DSP) and how the NIS Directive has influenced this budget. The annual stock-taking of this data now allows for historical traceability and the identification of trends.

A typical OES or DSP in the EU earmarks 6.7% of its IT investments for information security, while the average value is 7.2%. When analysing this normalised data set with historically available data, a decrease of one percentage point is observed in comparison to the median IS vs IT spending in 2020. However, the historical analysis has to be done while keeping in mind the slight differences in the samples between the years of study and the differences in the macro environment, such as the impact of the COVID-19 pandemic in the cost-optimisation practices of OESs and DSPs.

The survey data also indicates that a typical OES or DSP in the EU spends EUR 50,000 on cyber threat intelligence, while the average spend amounts to EUR 399,000. The disparity between the median and average values indicates that most organisations do not earmark vast budgets for CTI, while some (larger) organisations — specifically within the banking and energy sectors — do invest significantly in CTI. Cybersecurity investment strategies of 69% of the OESs and DSPs in the EU were mostly influenced by



the threat landscape, closely followed (66%) by their obligations under the NIS Directive.

## LEGISLATIVE MEASURES DESIGNED TO STRENGTHEN THE RESPONSE TO THE THREAT LANDSCAPE

The adoption and implementation of policy frameworks is one key response area where the EU is making a difference. Indeed, the policies and initiatives being put in place in the coming years are determining how the EU faces the cybersecurity challenges of today and tomorrow. Within this picture, ENISA will determine and adapt its support in particular in the following areas.

### NIS2 Directive

In May 2022 political agreement was reached between the European Parliament and EU Member States on measures for a high common level of cybersecurity across the Union (NIS2 Directive) proposed by the Commission in December 2020.

The NIS2 proposal consolidates, reinforces and extends the existing approach under NIS1, consolidating cybersecurity provisions from other legal provisions (EECC/telecoms and eIDAS/trust) under NIS2, strengthening for example incident reporting provisions and extending the scope, including cloud and data centres under critical services, and adding additional sectors, such as space (important for securing satellite communications, a vital infrastructure in remote rural areas, but also as a fail over in times of a natural disaster or military conflict).

NIS2 underlines the special role of telecoms as a highly mature sector, a conduit for cyberattacks and a possible filter or shield, protecting less mature and harder to protect sectors such as healthcare. In addition the ambitions of NIS2 need to be supported with better incident reporting to create a better situational picture, with vulnerability disclosure policies and an EU vulnerability database, with supply chain security and other coordinated Union-wide cybersecurity risk assessments, by expanding the scope in terms of sectors covered, and by creating the right culture and environment for essential and important entities to share cybersecurity relevant information such as cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools.

The transposition of NIS2 into national laws and the implementation phase lie ahead. As such ENISA is developing its service and expertise for this with the introduction of a service catalogue based on existing NIS1 expertise that are reflected in this draft single programming document (SPD).

ENISA is already invested in activities linked to the development and implementation of the NIS Directive, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the outcome of the proposal in the coming years, using existing resources and building on these wherever necessary.

### Joint Cyber Unit

The EU cybersecurity eco-system does not yet have a common space to work together across different communities and fields which allow existing networks to tap their full potential. The 2020 EU Cybersecurity Strategy outlined the need for a Joint Cyber Unit (JCU). The strategy identified the main problems to which the JCU would contribute solutions, its objectives and the steps needed to achieve them. It builds on the work started with the Recommendation (4520 (2021)) for a coordinated response to incidents and crises – the so called Blueprint - in 2017.

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

### Cyber Resilience Act (CRA)

In her State of the Union 2021 address, President von der Leyen underlined that the EU should strive to become a leader in cybersecurity, announcing in that context a new European Cyber Resilience Act. The act would add in particular to the existing baseline cybersecurity framework of the NIS Directive (and upcoming NIS2 framework) and the Cybersecurity Act.

The Act establishes common European cybersecurity requirements for products with digital elements that are placed on the internal market by introducing essential requirements for such products as well as

imposing obligations on manufacturers, importers and distributors. Products with digital elements create opportunities for EU economies and societies. However, they also lead to new challenges – when everything is connected, a cybersecurity incident can affect an entire system, disrupting economic and social activities.

The CRA aims to address market needs and protect consumers from insecure products by introducing common cybersecurity rules for manufacturers, importers and distributors of tangible and intangible products with digital elements. The CRA proposal was published on the 15 September 2022. The CRA will apply to all products connected directly or indirectly to another device or network. Open-source software and products and services covered by other existing rules, such as medical devices, aviation and cars, are explicitly excluded.

ENISA has provided expert opinion and is working towards collecting evidence to support an impact assessment through its Cybersecurity Policy Observatory (CSPO) and will also provide support in later stages (post-impact assessment) by contributing to elements of the legislative proposal such as risk categorisation and security requirements.

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

ENISA is playing a central role in supporting the implementation of the European cybersecurity certification framework by preparing and maintaining the candidate schemes. In this task ENISA is supported by area experts and operates in collaboration with public authorities in the Member States. It is expected that the draft candidate cybersecurity certifications schemes proposed by ENISA will be adopted as Commission implementing Regulations. The adopted schemes will allow for the assessment of the conformity of digital products, services and processes in the Digital Single Market under those schemes, which can contribute to increasing the level of customer trust in digital solutions in the Union.

Currently, ENISA has prepared a candidate scheme for the EU Common Criteria European candidate cybersecurity certification scheme (EUCC) which has been transposed into an EU Implementing Act by the Commission for its final adoption. In 2022, the candidate scheme on Cloud Services (EUCCS) will be submitted to the ECCG for its opinion. Furthermore, an ad hoc working group has started work preparing a candidate certification scheme for 5G networks (EU5G), with a first phase to

characterise the possibility of reusing existing schemes, and to identify related gaps to be covered by a relevant EU scheme.

Finalising the candidate schemes for specialised product categories under the EU Common Criteria (EUCC) scheme and for cloud services is just the first step and it will likely bring about benefits in terms of recognition and trust across government services, business and citizens during the time period 2023-2025.

In relation to the digital identity framework, ENISA will support and continue the development of a certification strategy matching the expectations of Article 6a of the Regulation which requires Member States to issue a European Digital Identity Wallet under a notified eID scheme to common technical standards following compulsory assessment of compliance and voluntary certification within the European cybersecurity certification framework, as established by the Cybersecurity Act. This strategy shall make the best reuse of existing schemes under development and shall also identify potential new certification means for schemes that would contribute to the certification of a wallet.

ENISA will also support the development of means of certification that would allow compliance with certain requirements of Article 18 of the NIS2 directive to be demonstrated, as the regulatory provisions of Member States may require entities to use particular ICT products, services and processes, either developed by an essential or important entity or procured from third parties that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881.

Where applicable, certification means for CRA related products, such as Protection Profiles, any additional certification tool or scheme. Such certification elements supporting the CRA, as well as other certification elements supporting other legislations should be consolidated into the first public version of the Union Rolling Work Programme, that the EC foresees being published in Q4 2022.

## **Research & Innovation**

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

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

ENISA, with the support from the community, will continue mapping ongoing activities to identify and prioritise areas where more research, development and implementation is needed to improve Europe's knowledge, resilience and response to current and emerging cyber threats. These research and innovation needs and funding priorities will constitute ENISA's advice and contribution to the EU's strategic research and innovation agenda.

### The European Digital Identity Framework

Digital identity and trust services are crucial for the EU digital market, because they allow citizens and businesses to carry out transactions online in a safe and trusted way. In 2020 the Commission reviewed the Electronic Identification and Trust Services (eIDAS) Regulation and identified factors hindering the adoption of mechanisms for electronic identification. In June 2021 the Commission made a proposal for a revised eIDAS Regulation establishing a European Digital Identity framework and a European Digital Wallet, to be available for all EU citizens, on a voluntary basis and that will be usable for online transactions with government entities, but also with businesses.

In the 2023-2025 period, ENISA will support Member States and the Commission with the development of the European Digital Identity Framework and the European Digital Identity Wallets, as set out in proposal for a revised eIDAS regulation in addition to promoting the exchange of good practises and capacity building for relevant stakeholders. The revised eIDAS regulation also expands the list of qualified trust services with distributed ledgers and electronic archiving and the management of remote devices for the creation of electronic signatures and seals.

The NIS2 proposal for a revised NIS Directive foresees that the security obligations laid down in this Directive should be considered complementary to the requirements imposed on trust service

providers under Regulation (EU) No 910/2014 (eIDAS Regulation). When this proposal is adopted, ENISA will support Member States and the Commission with this transition, to ensure that the trust service providers and the national authorities can benefit from the ecosystem of the NIS Directive.

### Artificial Intelligence (AI)

With the EU's AI agenda advancing rapidly following the European Commission's proposal on AI<sup>1</sup> and the Coordinated Plan on Artificial Intelligence 2021<sup>2</sup>, the EU is addressing the major technological, ethical, legal and socio-economic challenges to put AI at the service of European citizens and the economy, for instance by considering linking high-risk AI systems to mandatory trustworthiness requirements. One of these challenges is understanding the interplay between cybersecurity and AI and how this can affect availability, safety or the resilience of future AI services and applications.

Building on ENISA's efforts towards securing AI and machine learning, the Agency can continue its open dialogue with EU institutions in support of legislative initiatives reaching into 2023-2025. For this, ENISA will systematically monitor existing initiatives from Member States in this area and continue supporting the Commission and Member States by providing guidelines to good security practices.

### Digital Operational Resilience Act (DORA)

In June 2022, the Council presidency and the European Parliament reached a political agreement on the regulation of 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 proposed legislation will require firms to ensure that they can withstand all types of ICT-related disruptions and threats. ENISA is actively supporting the mapping of cyber legislative initiatives in the finance sector and works closely with the European Commission and relevant EU Bodies on the cybersecurity aspects of DORA including crisis management, incident reporting and information sharing.

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

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

## Network Code on Cybersecurity

The Network Code on Cybersecurity aims to set sector specific rules for the cybersecurity of cross-border electricity flows across EU member states. It includes rules on cyber risk assessment, common minimum requirements, cybersecurity certification of products and services, monitoring, reporting and crisis management. It is part of the Commission's request to European Network of Transmission System Operators for Electricity (ENTSO-E) pursuant to Regulation (EU) 2019/943 and ENISA has been actively involved in defining approaches to risk assessment, common minimum cybersecurity requirements and appropriate technical and organisational measures. The code contains many references to and foresees new leading and supporting tasks for ENISA amongst others, facilitation of an Early Warning System, supporting Agency for the Cooperation of Energy Regulators (ACER) in monitoring the implementation of the code and supporting (ENTSO) and the European Distribution System Operators (DSO) entity with organising sector specific exercises.

## Once-only technical system (OOTS)

Pursuant to Regulation (EU) 2018/1724<sup>3</sup>, the Commission adopted implementing Regulation C(2022)5628 which sets out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the 'once-only' principle. ENISA supports the efforts of the Commission and Member States on cybersecurity aspects of the deployment of the system, including risk management and the identification of appropriate technical and organisational measures to mitigate identified threats

## Chips Act

On 8 February 2022, the European Commission proposed a comprehensive set of measures for strengthening the EU's semiconductor ecosystem, the European Chips Act<sup>4</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 (KDT Joint Undertaking, and a Recommendation to Member States promoting actions for monitoring and mitigating disruptions in the semiconductor supply chain. Supply chain cybersecurity is an important cross-cutting issue for stakeholders.

## Cybersecurity and information security for EU institutions, bodies and agencies

In March 2022, the European Commission proposed a new regulation<sup>5</sup> with rules to increase cybersecurity in all EU institutions, by making it easier to share information on cyber threats and improving the efficiency of action to prevent and respond to cyber threats. This is expected to reduce the risk of incidents that cause material or reputational damage to EUIBAs. The proposal calls for increased cooperation with relevant bodies and stakeholders in the EU, via CERT-EU and ENISA. In addition, it is proposed that ENISA will receive on a monthly basis a summary report from CERT-EU on significant cyber threats, significant vulnerabilities and significant incidents.

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

---

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

4 COM(2022) 45. Communication from the Commission: A Chips Act for Europe. 08/02/2022  
COM(2022) 46. Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act). 08/02/2022.

COM(2022) 782. Commission Recommendation on a common Union toolbox to address semiconductor shortages and an EU mechanism for monitoring the semiconductor ecosystem. 08/02/2022.

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

6 Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union | European Commission (europa.eu).

## FURTHER DEVELOPMENTS

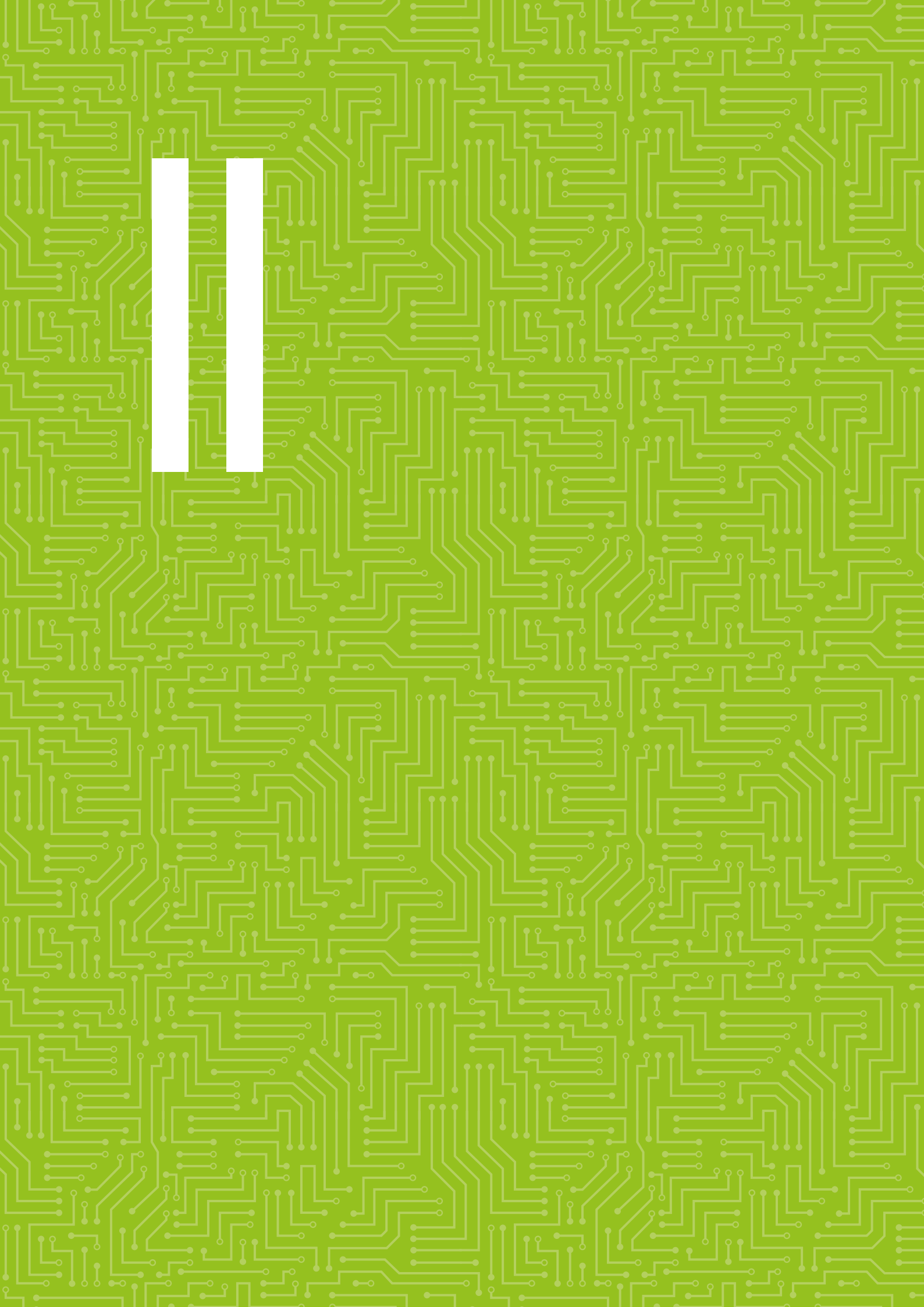
### Memorandum of Understanding with the European Data Protection Supervisor (EDPS)

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

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

### Trusted network of vendors and suppliers

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



## SECTION II

# MULTI-ANNUAL PROGRAMMING 2023–2025

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

### 2.1. MULTI-ANNUAL WORK PROGRAMME

The following table maps the strategic objectives stemming from ENISA's strategy<sup>7</sup> against the respective articles of the CSA. It furthermore integrates the activities of the Work Programme showing how the progress in the achievement of the objectives is monitored. These objectives shall be reviewed if applicable through the ENISA Management Board as from 1 July 2024.

---

<sup>7</sup> The ENISA strategy entered into force on the 31 July 2020 and the Management Board shall launch a review procedure, if relevant, as from 1st July 2024.

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	
<b>SO1</b> <b>Empowered and engaged communities across the cybersecurity ecosystem</b>	Activities 1 to 10	Art. 5 to Art. 12	<p>Empowered ecosystem encompassing authorities in Member States, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure</p> <p>An EU-wide state-of-the-art body of knowledge on cybersecurity concepts and practices, that builds cooperation amongst key actors in cybersecurity, promotes lessons learned, EU expertise and creates new synergies</p>	
<b>SO2</b> <b>Cybersecurity as an integral part of EU policies</b>	Activities 1 & 2	Art. 5	<p>Cybersecurity aspects are considered and embedded across EU and national policies</p>	
<b>SO3</b> <b>Effective cooperation amongst operational actors within the Union in case of massive<sup>9</sup> cyber incidents</b>	Activities 4 & 5	Art. 7	<ul style="list-style-type: none"> <li>• All communities (EU Institutions and MSs) use a streamlined and coherent set of SOPs for cyber crises management</li> <li>• Efficient, tools and methodologies for effective cyber crisis management</li> </ul>	
			<ul style="list-style-type: none"> <li>• Member States and institutions cooperating effectively during largescale 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>	

8 Surveys will be designed and developed in order to solicit a measurable response from participants to determine the added value of ENISA's contributions.

9 Large-scale and cross-border.



	Key performance indicator	Metrics
	Community-building across the cybersecurity ecosystem	<ol style="list-style-type: none"> <li>1. Number and types of activities at each engagement level</li> <li>2. Stakeholder satisfaction with ENISA's role as facilitator of community-building and collaboration across the cybersecurity ecosystem (survey)</li> </ol>
	ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante)	<ol style="list-style-type: none"> <li>1. Number of relevant contributions to EU and national policies and legislative initiatives</li> <li>2. Number of references to ENISA reports, analyses and/or studies in EU</li> <li>3. Satisfaction with the added-value of ENISA's contributions (survey)</li> <li>4. Number of EU policy files under development and supported by ENISA</li> </ol>
	Contribution to implementation of policy and monitoring of implementation at EU and national level (ex-post)	<ol style="list-style-type: none"> <li>1. Number of EU policies and regulations implemented at national level supported by ENISA</li> <li>2. Number of ENISA reports, analyses and/or studies referred to in EU and NIS cooperation group documents (survey)</li> <li>3. Satisfaction with the added-value of ENISA's support (survey)<sup>8</sup></li> <li>4. Number of critical sectors with high levels of cybersecurity maturity (NIS sector 360)</li> </ol>
	Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation	<ol style="list-style-type: none"> <li>1. Number of users both new and recurring and usage per platform/tool/ SOPs provided by ENISA</li> <li>2. Uptake of the platform/ tool/SOPs during massive cyber incidents</li> <li>3. Stakeholder satisfaction on the relevance and added value of the platforms/tools/SOPs including EU vulnerability database</li> </ol>
	ENISA's ability and preparedness to support response to massive cyber incidents	<ol style="list-style-type: none"> <li>1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate</li> <li>2. Number of relevant incident responses ENISA contributed to as per CSA Art7</li> <li>3. Take up of ENISA support services</li> <li>4. Number of trusted vendors</li> <li>5. Stakeholders' satisfaction with ENISA's ability to provide operational support</li> </ol>

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	
<b>SO4</b> <b>Cutting-edge competences and capabilities in cybersecurity across the Union</b>	Activities 3 & 9	Art. 6 & Art. 7(5)	<ul style="list-style-type: none"> <li>Enhanced capabilities across the community</li> <li>Increased cooperation between communities</li> </ul>	
		Art. 10 & Art. 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>	
<b>SO5</b> <b>High level of trust in secure digital solutions</b>	Activities 6 & 7	Art. 8	<p>Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework are adopted</p> <p>Smooth transition to the EU cybersecurity certification framework</p> <p>Certified ICT products, services and processes are preferred by consumers and, where relevant, operators of essential services or digital service providers</p>	
			<ul style="list-style-type: none"> <li>Contribution towards understanding market dynamics</li> <li>A more competitive European cybersecurity industry, SMEs and start-ups</li> </ul>	
<b>SO6</b> <b>Foresight on emerging and future cybersecurity challenges</b>	Activity 10 & 8	Art. 11 & Art. 9	<ul style="list-style-type: none"> <li>Research and development of cybersecurity technology reflecting the needs and priorities of the Union.</li> <li>Funding the development of cybersecurity technologies that meet the Union's ambition to become more resilient, autonomous and competitive.</li> </ul>	
<b>SO7</b> <b>Efficient and effective cybersecurity information and knowledge management for Europe</b>	Activity 8	Art. 9	<ul style="list-style-type: none"> <li>Decisions about cybersecurity are future proof and take account of trends, developments and knowledge across the ecosystem</li> <li>Stakeholders receive relevant and timely information for policy and decision-making</li> </ul>	

	Key performance indicator	Metrics
	Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	<ol style="list-style-type: none"> <li>1. Increase/decrease of maturity indicators</li> <li>2. Outreach, uptake and application of lessons learnt from capacity-building activities.</li> <li>3. The number of exercises executed annually.</li> <li>4. Stakeholder assessment on usefulness, added value and relevance of ENISA; and cooperation amongst communities in capacity building activities</li> <li>5. ISAC maturity</li> </ol>
	<p>Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU</p> <p>Level of outreach</p>	<ol style="list-style-type: none"> <li>1. Number of cybersecurity incidents reported having human error as a root cause</li> <li>2. Number of activities and participation in awareness raising actions organised by ENISA on cybersecurity topics</li> <li>3. Number of cybersecurity programmes (courses) and participation rates</li> <li>4. Geographical and community coverage of outreach in the EU</li> <li>5. Level of awareness, on cybersecurity across the EU/ general public (e.g. EU barometer)</li> </ol>
	<p>Uptake of the European cybersecurity certification framework and schemes as an enabler for more secure digital solutions</p> <p>Effective preparation of candidate certification schemes prepared by ENISA</p>	<ol style="list-style-type: none"> <li>1. Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions</li> <li>2. Stakeholders' level of trust in digital solutions of certification schemes (Citizens, public sector, businesses) and number of certificates issued on the basis of EU certification schemes</li> <li>3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework</li> <li>4. Number of candidate certification schemes prepared by ENISA</li> <li>5. Number of people or organisations engaged in the preparation of certification schemes</li> <li>6. Satisfaction with ENISA's support in the preparation of candidate schemes (survey)</li> </ol>
	Effectiveness of ENISAs supporting role for participants in the European cybersecurity market	<ol style="list-style-type: none"> <li>1. Number of market analyses, guidelines and good practices issued by ENISA</li> <li>2. Uptake of lessons learnt or recommendations from ENISA reports</li> <li>3. Stakeholder satisfaction with the added value and quality of ENISA's work</li> </ol>
	Contributing to Europe's Strategic Research and Innovation Agenda in the field of cybersecurity.	<ol style="list-style-type: none"> <li>1. Number of requests from EU-IBAs (including the ECCC) and MSs to contribute, provide advice or participate in activities.</li> <li>2. Number of references to ENISA advice and recommendations in the EU Strategic Research and Innovation Agenda including Annual and Multiannual Work programmes.</li> <li>3. Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's advice on cybersecurity research needs and funding priorities (Survey)</li> </ol>
	ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge	<ol style="list-style-type: none"> <li>1. Number of users and frequency of use of dedicated portal (observatory)</li> <li>2. Number of recommendations, analyses and challenges identified and analysed</li> <li>3. Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities (including threat landscapes)</li> <li>4. The influence of foresight on the development of ENISA's work programme</li> <li>5. Uptake of reports generated in activity 8</li> <li>6. Uptake of the cybersecurity index</li> </ol>



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

**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 relevant EU rules and obligations in its services and working environment ensuring fairness and inclusiveness.

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

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

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

The corporate objective of **sound resource and risk management** is derived from requirements in Art 4(1) of the CSA that sets an objective for the Agency to 'be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the

Corporate objective	Actions to achieve objective	Article of the CSA	Expected results
<b>Sound resource and risk management</b>	Activity 11	Art 4(1)	<ul style="list-style-type: none"> <li>• Maximise quality and value provided to stakeholders and citizens</li> <li>• Building lasting credibility and trust</li> </ul>
<b>Build an agile organisation focused on people</b>	Activity 12	Art 3(4)	ENISA as an employer of choice and enabling growth and excellence in a secure environment

information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks'. In addition, the inspiration for this corporate objective stems from the values of **Excellence** and **Transparency** derived from ENISA's strategy and the principle of **Efficiency** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to uphold the highest quality of standards, strive for continuous improvement and enhance the organisation's performance.

The corporate objective of **building an agile organisation focused on people** is derived from requirements in Art 3(4) of the CSA which obliges the Agency to 'develop its own resources, including /.../ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation'. In addition, the inspiration for this corporate objective stems from the values of **Responsibility** and **Respect** derived from ENISA's strategy and the principle of **Competences** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to respect fundamental European rights and values in its working environment, assume responsibility for the social and environmental dimensions of its procedures and to develop its staff competences, expertise and talent.

	Key performance indicator	Metrics
	<ol style="list-style-type: none"> <li>1. Organisational performance</li> <li>2. Trust in the ENISA brand</li> </ol>	<ol style="list-style-type: none"> <li>1. Proportion of KPIs reaching targets</li> <li>2. Individual contribution to achieving the objectives of the agency via clear link to KPIs (CDR report)</li> <li>3. Exceptions in Risk Register</li> <li>4. Number of complaints filed against ENISA incl number of inquiries or complaints for the EU Ombudsman</li> <li>5. Number of complaints addressed in a timely manner and according to relevant procedures</li> <li>6. Number of high risks identified in annual risk assessment exercise</li> <li>7. Implementation of risk treatment plans</li> <li>8. Number and types of activities at each level of engagement</li> <li>8. Observations from external audit bodies and the European Court of Auditors (ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed</li> <li>9. Level of trust in ENISA (survey)</li> </ol>
	<p>Staff commitment, motivation and satisfaction</p>	<ol style="list-style-type: none"> <li>1. Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities for internal mobility, work-space, -environment and -tools)</li> <li>2. Quantity and quality of ENISA training and career development activities organised for staff</li> <li>3. Reasons for staff departure (exit interviews)</li> <li>4. Turnover rates</li> <li>5. Establishment plan posts filled</li> <li>6. Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services and tools)</li> <li>7. Percentage of procurement procedures launched via e-tool (PPMT)</li> <li>8. Percentage of payments made within 30 days</li> <li>9. Late Payments</li> </ol>

## 2.2. HUMAN AND FINANCIAL RESOURCES – OUTLOOK FOR YEARS 2023–2025

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

A number of factors not considered or foreseen in 2021-2022 when the Commission established the MFF 2021-2027 programmes have had a cumulative effect on ENISA's requests for resources during this period. Acknowledging ENISA's exceptional operational mandate, the Commission and the Budgetary Authority have continued to support ENISA's annual budget and requests for posts, including allocating additional posts to the Agency through the NIS2 directive, transferring additional posts for seconded national experts to strengthen the domain of operational cooperation and through a one-off transfer of up to 15 million EUR in 2022 for supporting the Agency's ability to provide Member States with ex-ante and ex-post services in response to the heightened threat level caused by the Russian war in Ukraine.

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

In terms of its human resources, the number of Establishment Plan posts has grown from 59 to 82 posts during the period 2019–2022, that is by 39% as a result of the new tasks that were foreseen under the new Cybersecurity Act which came into force in 2019. An additional five posts (three TAs and two CAs) have been authorised under 2022 for new

tasks under the NIS2 Directive. The number of all authorised posts including TAs, CAs and SNEs grew following a similar trend, that is by 33%, during the period 2019-2022.

**Table 1a. Evolution of authorised posts and fulfilment**

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

As an Agency, ENISA has historically struggled to meet its needs for human resources and to take steps to ensure timely and rapid fulfilment of its Establishment Plan. The gap between available posts and plan fulfilment is evidenced in the table above. Historically, this has hampered the Agency in making use of its potential capabilities in the most efficient manner, resulting in a smaller real capacity of the Agency in terms of its human resources.

In order to change this, the Agency embarked on some human resources management novelties such as a large-scale call for expressions of interest for temporary agents (TAs) and contract agents (CAs) in 2020, with the aim of creating sufficiently diverse and broad reserve shortlists of candidates with more transversal competences and skills that could be used to recruit staff and thus fill the gaps in the current establishment plan, as well as serve as a pool of candidates for the establishment plan on a multiannual basis. In 2021 the Agency also embarked in an extensive reorganisation of the management of its human resources, creating a Strategic Workforce Planning framework<sup>11</sup> which

<sup>10</sup> 3 TA posts and 2 CA posts from NIS2 directive; projection on 31.12.2022 depends on successful conclusions of ongoing selection process Q3-Q4 2022.

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

**Table 1b. Monitoring the workforce under operational and support units.**

	Operational units		Supporting offices and services	
	Established staff (TAs & CAs)	Average	Established staff (TAs & CAs)	Average
Allocated posts as of 01.01.2021	48	12	38	19
Allocation as of 01.10. 2021	67	16.75	40	20
Allocated posts as of 01.08.2022	71	17.75	35.5	17.75
Current staff in house at 01.08.2022	60	15	32.5	16.25

prompts the organisation to analyse its human resource needs ahead on a multiannual basis for the Single Programming Document, and to plan and review the allocation and development of human resources between different activities as well as to prepare new recruitment calls well in advance of the enactment of the applicable annual Establishment Plan. Under this framework, the Agency has reviewed and restructured its human resources both in direct operational areas and in administrative and corporate areas.

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

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

The original impact that the conclusions of the 2021 and 2022 Strategic Workforce Review were supposed to bring are summarised in the table 1b.

Though these exercises aimed at fulfilling and supporting the resourcing of operational activities, the Agency's tight budgetary resources left limited

space for manoeuvring and the delivering of existing services in corporate and administrative units as due to budget limitations the possibilities of externalising service provision could not have been implemented.

### 2.2.2. Outlook for the years 2023–2025

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

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

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

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

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

Currently ENISA is still waiting for the final adoption of the NIS2 directive where ENISA is tasked with additional action areas. While these action areas are covered by ENISA's general tasks in accordance with its mandate, they would be supported by five supplementary fulltime equivalents (FTEs) (three TAs and two CAs) with a corresponding budget of around EUR 610,000 a year. This is an integral part of the NIS2 and is currently managed as a reserve that the Agency can draw on following the completion of the adoption process. It is expected that NIS2 directive will be adopted in Q4 2022. The indicated posts have been included in the general workforce planning as part of the approved human resources under the EU general budget 2023.

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

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

The human resource requirements forecasted in the current draft of the SPD are well above those foreseen by the current establishment plan. While ENISA remains committed to the continuous improvement of its administrative and operational efficiency, it will continue to closely monitor, assess and optimise its structures, services, processes, activities and resource allocation. ENISA faces a constant increase in its workload and while it will still seek for further gains in efficiency across the organisation, these gains will only compensate for minor workload increases and temporary absences of staff. However, the MFF 2021-2027 foresees no increase in the agency's establishment plan and thus imposes further constraints for its human resources. Unless further resources are allocated, ENISA would need to prioritise and limit the scope of its services within its existing tasks as well as within new tasks in order to fulfil its operational mandate.



## 2.3. RESOURCE PROGRAMMING FOR THE YEARS 2023–2025

### 2.3.1. Financial Resources

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

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

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

The introduction of the BMC and activity based budgeting have allowed enhanced monitoring of financial planning, leading to a more efficient execution of the budget. Concretely, a higher budgetary execution rate and fewer budgetary transfers were expected as a result of this, as evidenced in 2021. The budgetary execution rate in 2021 increased to 99.51% of the budget vs 97.35% in 2020 and there were five internal transfers by ED decision versus seven in 2020 and ten in 2019.

Based on the lessons learned from 2021 the Agency has extended this efficiency to title 1 and title 2 by merging the budget lines of these titles in the proposed 2023 budget structure. By reducing the number of budget lines from 30 to 11 for title 1 and 2, the Agency will be able to reduce the number of ED decisions required to transfer funds between budget lines thus reducing administrative burden and enhance the quality of the monitoring and reporting of the budget. The budget lines consolidated were those budget lines with less 500,000 EUR within the same type or category of expenditure in title 1 and 2. This would also allow the agency to apply a more agile and flexible way of managing its funds and services. The consolidated budget lines are reflected in the statement of estimates submitted and adopted alongside the draft SPD 2023-2025.

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

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

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

The general allocation of funds across titles is expected to remain stable over the period 2023-2025. Expenditure in 2023 is expected to amount to EUR 25.2 million, of which EUR 12.7 million in Title 1 covers all staff-related costs (50%), EUR 3.5 million in Title 2 covers main items such as building related expenditure and ICT expenses (14%) and EUR 9.0 million in Title 3 covers all core operating expenditure (36%). Total expenditure includes the reserve budget of EUR 610,000 expected to be allocated to cover additional staff (3 TAs and 2 CAs) to manage part of the activities linked to the NIS2 directive to be adopted in Q4 2022.

**Table 2**

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

Source:

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

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

### 2.3.2. Human Resources

In its budget proposal for the Single Programming Document (SPD) 2023-2025, the Agency asks for an extra four SNE posts (introduced gradually 2+2 over the two years to 2024). The four additional SNE posts requested would be justified both by the Agency's current activity areas, particularly the operational needs stemming from Article 7 of the CSA as well as by those extra activities and requirements, as foreseen especially in the initial phases laid out in the Commission's Recommendation on the Joint Cyber Unit (JCU) of 23 June 2021.

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

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

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

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

The reallocation of posts within ENISA will be done by following the established strategic workforce planning framework. Annual strategic workforce reviews will be conducted during the period from 2023 to 2025 in order to develop and maintain current staff competencies to fulfil the Agency's operational needs and achieve the balance of internal resource allocation between operational and corporate support units. As indicated in Table 1b under Section 2.1, the current allocation of posts between operational and corporate support units is balanced. ENISA will thus continue its best efforts to ensure that current in-house staff to be reported on 31 December 2022 will also be balanced, keeping the same trend throughout the coming period from 2023 to 2025. For this, ENISA aims to put an emphasis on the development of staff competences, including by gradually rolling out multisource feedback tools which enable staff members to actively address their development areas, expertise and skills in line with the needs of the Agency.

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

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

#### 2.4. STRATEGY FOR ACHIEVING GAINS IN EFFICIENCY

ENISA remains committed to the continuous improvement of its operational and administrative efficiency. It aims to ensure that it acts in the right way and exhausts gains in efficiency before reinforcing areas of work with extra resources. As part of its upcoming corporate strategy, the Agency aims to further improve ENISA's organisational efficiency and flexibility to meet operational needs. To this end, as part of its HR strategy, the Agency aims to address and include an efficiency strategy component, with specific initiatives and a cross-unit perspective. Such initiatives should be seen as a holistic package and cover different pillars such as activity and resources or service categorisation, capitalisation on shared services, strategic workforce planning, business and service optimisation among a few.

### Strategic Workforce Planning

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

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

**Table 3**

	2022 <sup>12</sup>	2023 <sup>13</sup>	2024 <sup>14</sup>	2025 <sup>15</sup>
Number of posts in the Establishment Plan	82	82	82	82
Per cent of expected fulfilment of the establishment plan on 31 December 94% 95% or higher 95% or higher 95% or higher	94%	95% or higher	95% or higher	95% or higher
Total number of authorised posts (TAs, CAs, SNEs) and expected (2024 & 2025) 126 128 130 132	126	128	130	132
Per cent of expected fulfilment of the total authorised posts (TAs, CAs, SNEs) on 31 December 94% 95% 95% 95%	94%	95%	95%	95%

<sup>12</sup> Forecast data will be finalised in November 2022 and 3 TA posts and 2 CA posts from NIS2 directive; projection on 31.12.2022 depends on successful conclusions of ongoing selection process Q3-Q4 2022.

<sup>13</sup> 3 TA posts and 2 CA posts from NIS2 directive.

<sup>14</sup> 3 TA posts and 2 CA posts from NIS2 directive.

<sup>15</sup> 3 TA posts and 2 CA posts from NIS2 directive.

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

### Business process review and service optimisation

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

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

- exploring and piloting changes in service levels and modalities, to improve added-value and cost-efficiency, such as shifting from owned to leased solutions, from manual entries to centrally managed solutions;
- identifying activities and services that may be downsized and discontinued if needed;
- continuously streamlining and automating administrative workflows to improve staff productivity, by removing redundant steps and capitalising on new technologies such as making use of DIGIT services and tools,

- reviewing ICT infrastructure and related technologies to reduce duplication of components and optimise maintenance and capital replacements such as for storage or move towards cloud-based solutions.

### Capitalising on shared services

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

- sharing services with other agencies and/or the Commission, including e.g. interagency and inter-institutional procurements, common services with CEDEFOP and the European Cybersecurity Competence Centre (ECCC) and the use of the Commission's ICT solutions such as those for human and financial resources management;
- contributing to further promoting shared services among agencies through different networks, particularly in the areas of procurement, HR, ICT and risk and performance management, data protection, information security, accounting etc;
- contributing to the improvement and piloting of IT services with DG HR, DIGIT and Frontex in the area of HR and financial management.

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

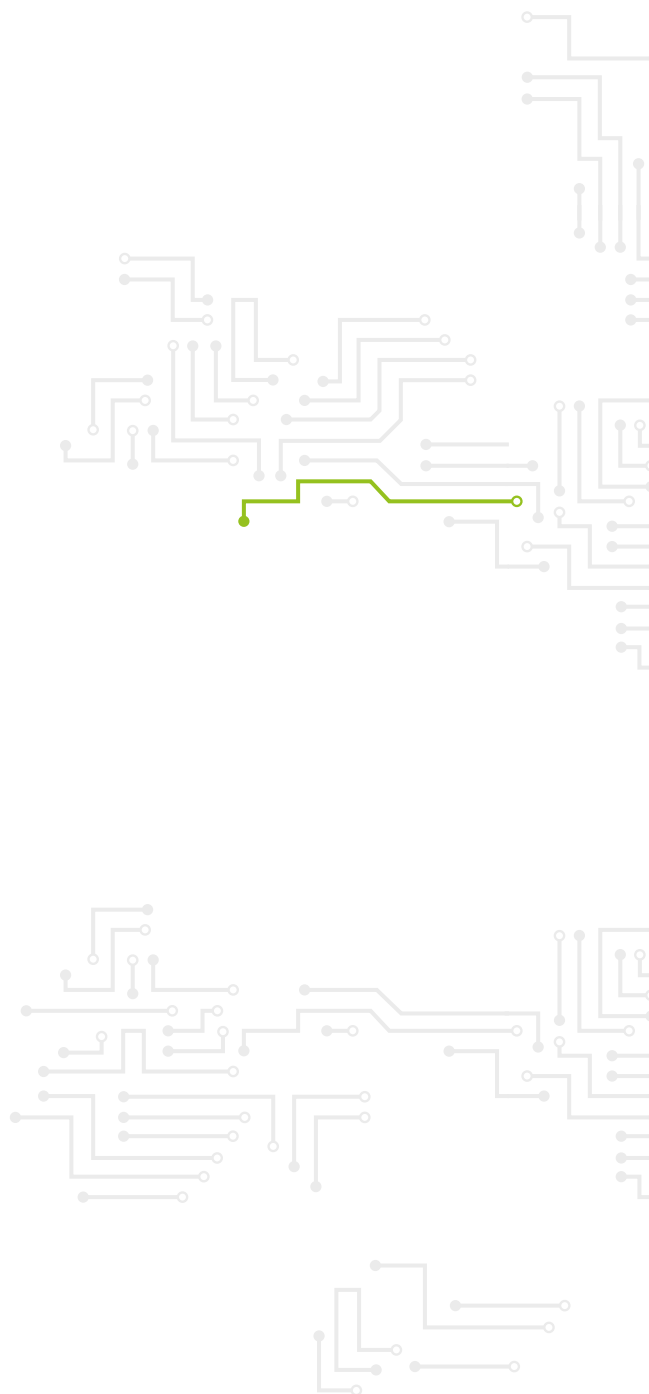
The Agency continues to implement its work programme by systematic use of its statutory bodies (NLO Network, ENISA Advisory Group), as well as other statutory groups. ENISA is involved in the Stakeholder Cybersecurity Certification Group (SCCG as set out in the CSA Art. 22, NISD Cooperation Group and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

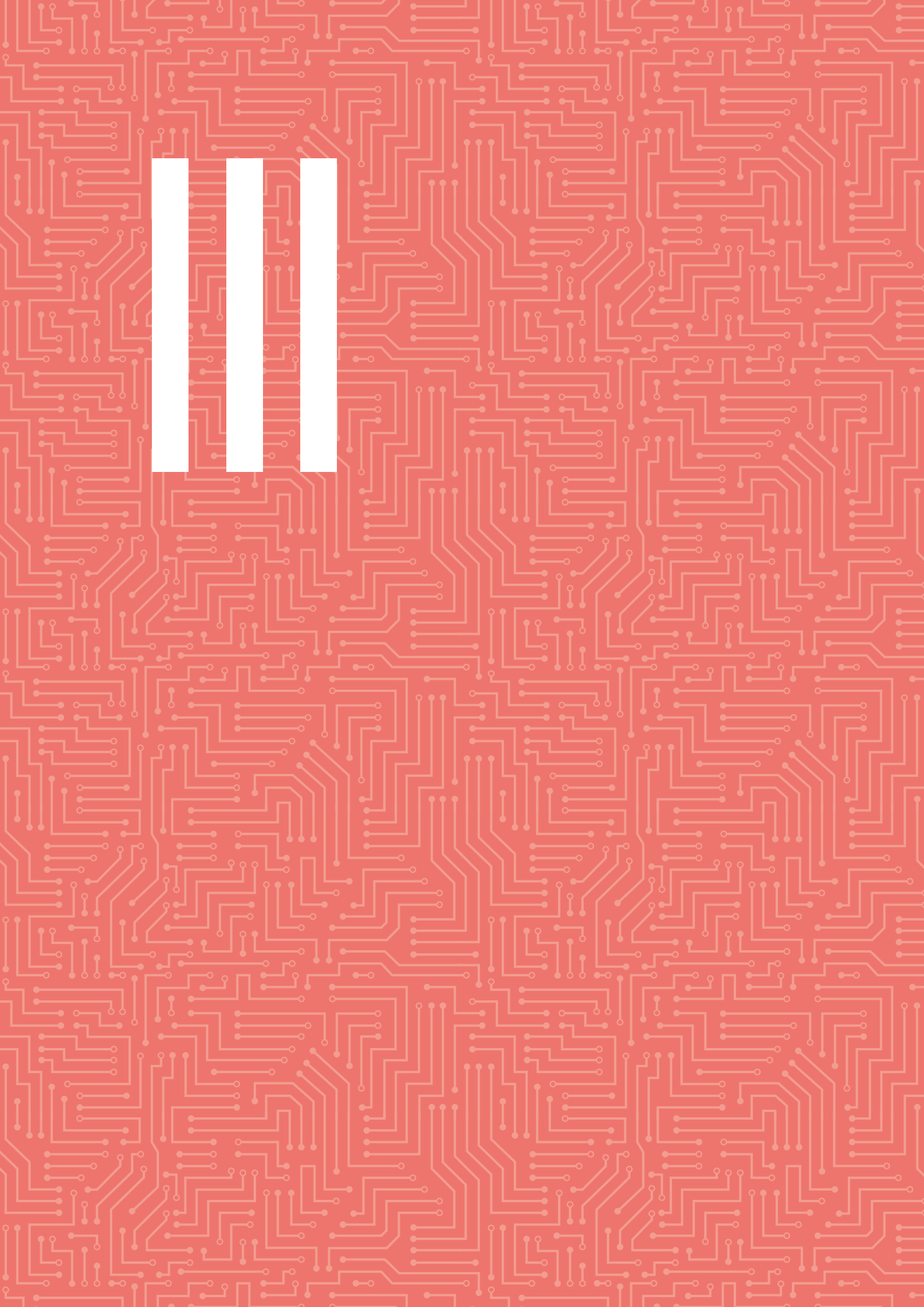
Since 2021, the framework for structured cooperation with CERT-EU has been formalised with the drafting of an annual cooperation plan to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation (Art 7 of the CSA). The Agency's local office in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

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

Most of ENISA's administrative tasks are supported by EU Tools such as accruals-based accounting (ABAC), Sysper for human resource management and for missions and document approvals and registry. In 2022, preparatory work to migrate to the Advanced Record System (ARES) was initiated and ENISA is engaged in preparatory work to use both the Missions Integrated Processing System (MIPS) and procurement management processes (PPMT) in the course of 2023.

In 2022 the Agency embarked on supporting the EU Agencies network in relation to the implementation of cybersecurity requirements proposed in the draft regulation on common binding rules on cybersecurity for EUIBAs, namely through a concept of shared services on the management of cybersecurity risk (virtual CISO concept)





# SECTION III

## WORK PROGRAMME 2023

This is the main body of the Work Programme describing, in terms of its operational and corporate activities, what the Agency aims to deliver in the year 2023 towards achieving its strategy and the expected results. Ten operational activities and two corporate activities in total have been identified to support the implementation of ENISA's mandate in 2023.

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

### STAKEHOLDERS AND ENGAGEMENT LEVEL

The management of stakeholders is instrumental to the proper functioning and implementation of ENISA's work programme. On 29 March 2022 the Management Team adopted ENISA's Stakeholders Strategy. This Strategy lays down the main principles and approach to the engagement of stakeholders at the Agency-wide level. The implementation of the Stakeholders Strategy is linked with the implementation of the Single Programming Document (SPD) through its activities.

Each activity includes a list of stakeholders and the expected or planned level of engagement for each stakeholder. The level of engagement refers to the degree of their interest and influence in the activity for stakeholders who are classified as either partners or involve/engage. Stakeholders classified as 'Partners' refers to those with high influence and

high interest, usually business owners and others with significant decision-making authority. They are typically easy to identify and to engage with actively. Stakeholders classified as involve/engage have high influence but lower interest. These are typically stakeholders with significant decision-making authority but lacking in availability or the interest to be actively engaged.

### KPIS AND METRICS

In 2020 the Agency developed and introduced a new set of key performance indicators and related metrics for measuring the performance of the activities. These metrics are inscribed in the Single Programming Document for each activity and are made up of both quantitative and qualitative metrics. Quantitative metrics are those that measure a specific number through a certain formulae. Qualitative metrics are those that are more of a subjective opinion based on information received; however even these are quantified in order to be interpreted and measured.

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

### 3.1. OPERATIONAL ACTIVITIES

## ACTIVITY 1: Providing assistance in policy development



### Overview of activity



This activity delivers assistance and advice to the EU and Member States in developing cybersecurity policy and sector-specific policy and legislative initiatives on matters related to cybersecurity and on the basis of the 2020 EU Cybersecurity Strategy. Aspects such as privacy and personal data protection are taken into consideration (including encryption).

The activity seeks to bolster policy initiatives on novel or emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. ENISA will support the EC and MSs on new policy initiatives<sup>16</sup> through evidence-based inputs into the process of policy development. ENISA, in coordination with the EC and Member States will also conduct policy scouting to support them in identifying potential areas for policy development based on technological, societal and economic trends as well as in developing monitoring capabilities and tools to regularly and consistently be able to provide advice on the effectiveness of existing Union policy and law in accordance with the EU's institutional competencies in the area.

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

The added value of this activity is to support decision-makers in a timely manner on developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework (see also Activity 8). Given the cross-cutting nature of cybersecurity across the policy landscape, the activity will provide an up-to-date risk-based analysis of cybersecurity not only in the areas of critical infrastructure and sectors, but also by providing advice across the field in an integrated and holistic manner. The legal basis for this activity is Article 5 of the CSA.

### Objectives



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

<sup>16</sup> Policy initiatives such as the forthcoming Cyber Resilience Act and initiatives on Artificial Intelligence (AI), 5G, quantum computing, blockchain, big data, data spaces, digital resilience and response to current and future crises



## Results



Cybersecurity aspects are considered and embedded across EU and national policies

## Link to strategic objective (ENISA strategy)



Cybersecurity as an integral part of EU policies

Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 1.1. Assist and advise the EC and Member States in reviewing the effectiveness of current cybersecurity policy frameworks
- 1.2 Assist and advise the EC and MS on new policy developments, as well as carrying out preparatory work
- 1.3 Support policy monitoring of existing and emerging policy areas and maintain a catalogue of all relevant cybersecurity legislations and policies at the EU level

## Validation



- NIS Cooperation Group (NIS CG) and other formally established Groups (outputs 1.1, 1.2 and 1.3)
- ENISA ad hoc working groups<sup>17</sup> (outputs 1.1, 1.2, and 1.3)
- National Liaison Officers Network, ENISA Advisory Group and other formally established expert groups (when necessary)

## Stakeholders and levels of engagement<sup>18</sup>



### Partners

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

### Involve / Engage

ENISA National Liaison Officers, operators of essential services, digital service providers and industry associations or representatives.

<sup>17</sup> in accordance with Art 20(4) of CSA

<sup>18</sup> Stakeholders and levels of engagement stem from the implementation of the ENISA stakeholder strategy

## Key performance indicators



ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (ex ante)	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
1.1. Number of relevant contributions to EU and national policies and legislative initiatives	Number	Annual	Manual collection from staff members	193	215
1.2. Number of references to ENISA reports, analyses and/or studies in EU policy documents	Number	Biennial	Survey <sup>19</sup>	N/A	Baseline to be established in 2023
1.3. Satisfaction with added value of ENISA's contributions		Biennial	Survey	N/A	Baseline to be established in 2023
1.4. Number of EU policy files under development and supported by ENISA	Number	Annual	Report	N/A	Baseline to be established in 2023

## Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total		
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR	
1.1	INDEX, SITAW, NIS, CERTI	1.45	246,712	0.00	11,387	0.10	0	1.55	258,099	
1.2	NIS, CERTI	1.30	28,086	0.60	27,150	0.10	0	2.00	55,237	
1.3	NIS, CERTI	0.95	9,404	0.25	7,523	0.00	0	1.20	16,926	
<b>Activity total</b>				<b>FTE</b>		<b>4.75</b>		<b>Budget</b>		<b>330,262</b>

<sup>19</sup> Biennial surveys for each activity will be conducted in Q1 2023 for reference year 2022. Results will be recorded in annual activity report 2022 and single programming document 2024-2026.

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



### Overview of activity



This activity provides support to Member States and EU Institutions in the implementation of European cybersecurity policy and the legal framework and technical advice on specific cybersecurity aspects of the implementation of the NIS2<sup>20</sup> and other legislations. The activity seeks to avoid fragmentation and supports a coherent implementation of the Digital Single Market across Member States, following a consistent approach between cybersecurity, privacy and data protection.

Under this activity ENISA provides support to the NIS Cooperation Group, its work streams, and the implementation of its biannual Work Programme including, for example, the implementation of the 5G toolbox, but also new tasks under the NIS2 such as the EU register for operators of digital infrastructure.

It further includes horizontal outputs, which address sector-agnostic cross-cutting issues<sup>21</sup>, and sectorial outputs, which are sector-specific and are addressed via targeted service packages for the critical (NIS) sectors. In addition, this work contributes, with relevant sectorial intelligence, to other SPD activities such as exercises and training (Activity 3), situational awareness (Activity 5), knowledge and information (Activity 8), and awareness raising (Activity 9).

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

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

### Objectives



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

<sup>20</sup> The NIS2 covers a) critical operators such as telecoms and trust service providers, which were not covered by the NIS1 but by other legislation (EECC and eIDAS), b) sectors which were already covered by the NIS1 such as energy, finance, health and c) new sectors, such as space and public administration.

<sup>21</sup> Such cross-cutting issues include namely security measures, technical aspect of cybersecurity, supply chain risk management, and vulnerability disclosure policies.

## Results



- Consistent implementation of Union policy and law in the area of cybersecurity
- EU cybersecurity policy implementation reflects sectorial specificities and needs
- Wider adoption and implementation of good practices

## Link to strategic objective (ENISA strategy)



- Cybersecurity as an integral part of EU policies
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 2.1. Support the activities of the NIS Cooperation Group including its work programme
- 2.2. Support Member States and the EC in the implementation of horizontal aspects of the NIS directive
- 2.3. Support Member States and the EC with the security and resilience of the NIS sectors via targeted service package identified in the ENISA NIS strategy
- 2.4. Provide advice, issue technical guidelines and facilitate the exchange of good practices to support Member States and the EC on the implementation of cybersecurity aspects of transversal EU policies<sup>22</sup>

## Validation



- NIS Cooperation Group and/or established work streams (Outputs 2.1, 2.2, 2.3)
- Telecoms working group (ECASEC) and trust services working group (Outputs 2.3, 2.4)
- eID Cooperation network, ENISA Ad Hoc Working Group on data protection engineering (Output 2.4)
- ENISA National Liaison Officers' Network (as necessary)

## Stakeholders and levels of engagement



### Partners

National cybersecurity agencies and national authorities for cybersecurity in the EU Member States (NIS CG plenary and work streams), National Regulatory Authorities (ECASEC), National Supervisory bodies (ECATS), Conformity Assessment Bodies (CABs), and informal groups of authorities (e.g. FESA, informal working group of financial authorities), EC, EU Institutions or bodies (e.g. Body of European Regulators for Electronic Communications (BEREC), European Data Protection Supervisor (EDPS), European Data Protection Board (EDPB), European Railway Agency (ERA), European Maritime Safety Agency (EMSA), other sectorial EU Agencies (e.g. ACER, EASA, ESA, ECB, EBA) and institutional industry bodies (e.g. ICANN, RIPE-NCC, ENTSO-E, ENTSO-G, EU.DSO entity)

### Involve / Engage

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

<sup>22</sup> Including DORA, Electricity Code, privacy and eIDAS.

## Key performance indicators



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

## Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
2.1	SITAW, NIS, TREX	6.2	336,846	0	-	0.25	-	6.45	336,846
2.2	SITAW, NIS, CERTI, TREX	4.45	422,402	0	-	0.3	-	4.75	422,402
2.3	SITAW, NIS, CERTI	-	-	3	214,155	0.3	-	3.3	214,155
<b>Activity total</b>				<b>FTE:</b>		<b>14.5</b>		<b>Budget: 973,404</b>	

## ACTIVITY 3: Building capacity



### Overview of activity



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

Actions to support this activity include the organisation of large-scale exercises, sectorial exercises, training and others.<sup>23</sup>

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

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

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

### Objectives



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

### Results



- Enhanced capabilities across the community
- Increased cooperation between communities

### Link to strategic objective (ENISA strategy)



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

<sup>23</sup> CSIRT training and Capture the Flag (CTF) and Attach Defence (AD) competitions.

## Outputs



- 2.1. Assist MSs to develop, implement and assess National Cybersecurity Strategies
- 3.2. Organise large-scale biennial exercises and sectorial exercises<sup>24</sup>
- 3.3. Organise training and other activities to support and develop maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS cooperation group (NIS CG) and work streams, information sharing and analysis centres (ISACs) and other communities
- 3.4. Develop coordinated and interoperable risk-management frameworks<sup>25</sup>
- 3.5. Support the reinforcement of Security Operational Centres (SOCs) as well as their collaboration, assisting initiatives of the Commission and Member States in this area in line with the objectives of the EU Cybersecurity Strategy in the building and improving of SOCs<sup>26</sup>
- 3.6. Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)<sup>27</sup>

## Validation



- NLO Network (as necessary)
- CSIRTs Network (output 3.3)
- CyCLONe members (as necessary)
- NIS Cooperation Group (output 3.2 and 3.3)
- EU ISACs (output 3.3)
- Ad-hoc WG on SOCs (output 3.5)

## Stakeholders and levels of engagement



### Involve / Engage

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

## Key performance indicators



Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
<b>3.1. Increase/decrease in indicators of maturity</b>					
Maturity of national cybersecurity strategies					
Number of Member States that rate the overall maturity of their cybersecurity strategy					
High maturity	Number	Annual	Survey	3	5
Medium maturity	Number	Annual	Survey	4	5
Low maturity	Number	Annual	Survey	3	2

<sup>24</sup> (Including Cyber Europe, Blueprint operational level exercise (BlueOLEx), Cyber Exercise to test SOPs (CyberSOPEx etc) and through cyber ranges. NIS cooperation group exercise postponed due to resource constraints.

<sup>25</sup> Output is suppressed in 2023 work programme due to insufficient resources.

<sup>26</sup> Would be priority output for the consideration of consuming any surplus budget in 2023.

<sup>27</sup> In the context of this output ENISA is also preparing a few Service Levels Agreements with key EU Agencies with advanced requirements for capacity building activities (e.g. eu LISA).

Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
Number of Member States planning to use ENISA's framework to measure the maturity of their national cybersecurity capabilities					
Already using	Number	Annual	Survey	3	5
Not set but planning to use	Number	Annual	Survey	4	5
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	3	3
The frequency with which Member States update their strategies to adapt to technological advancements and new threats					
Every 2–3 years	Number	Annual	Survey	2	3
Every 4–5 years	Number	Annual	Survey	6	8
More than 6 years or don't know	Number	Annual	Survey	2	2
Total maturity of ISACs (self-assessment)	%	Annual	Report	63%	65%
<b>3.2. Outreach, uptake and application of lessons learned from capability-building activities</b>					
CySOPEX 2021 (number of improvements proposed by participants)	Number	Per exercise	Report	5	3 <sup>28</sup>
<b>3.4 The number of exercises executed annually</b>	Number	Annual	Report	5 <sup>29</sup>	5
<b>3.5 Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey)</b>					
Usefulness low	%	Biennial of capacity building activities	Survey	9%	Maximum 5%
Usefulness medium	%	Average of capacity building activities	Survey	71%	25% to 50%
Usefulness high	%	Average of capacity building activities	Survey	20%	Minimum 45%

28 Average number of improvements across all exercises.

29 Relates to 2022 exercises executed as of October 2022.



Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
Relevance low	%	Average of capacity building activities	Survey	4%	Maximum 5%
Relevance medium	%	Average of capacity building activities	Survey	53%	25% to 50%
Relevance high	%	Average of capacity building activities	Survey	43%	Minimum 45%

### 3.5 ISACs maturity

Number of Exercises organised by EU ISACs	% <sup>30</sup>	Biennial	Report	N/A	Minimum 30%
Number of Training sessions organised by EU ISACs	%	Biennial	Report	N/A	Minimum 30%

### Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
3.1	TREX, INDEX	2.00	108,919	0.00	0	0.00	0	2.00	108,919
3.2	TREX, NIS	4.25	584,153	0.00	0	0.00	0	4.25	584,153
3.3	TREX	4.00	635,580	0.00	0	0.00	0	4.00	635,580
3.4 <sup>31</sup>									-
3.5	TREX	0.50	28,544	0.00	0	0.00	0	0.50	28,544
3.6	TREX	3.00	352,043	0.00	0	0.00	0	3.00	352,043
<b>Activity total</b>				<b>FTE:</b>		<b>13.75</b>		<b>Budget: 1,709,239</b>	

30 The % out of a total of 10 EU ISACs (as per NIS and NIS2).

31 Output to be suppressed in 2023 given resource constraints.

## ACTIVITY 4: Enabling operational cooperation



---

### Overview of activity



The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities in particular through its local office in Brussels, Belgium. Actions include establishing synergies with and between the various national cybersecurity communities (including the civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors notably CERT-EU with a view to exchanging know-how, best practices, providing advice and issuing guidance.

In addition, inline with NIS2 requirements ENISA will continue to support Member States in the CSIRTs Network in respect of operational cooperation. Moreover with the formal establishment of the EU CyCLONe (Cyber Crisis Liason Organization Network) in NISD2, ENISA will support the coordination of cyber crises by advising and assisting both networks.

Under this activity ENISA is supporting operational communities through helping to develop and maintain secure and highly available networks and IT platforms and communication channels to ensure, in particular, the maintenance, deployment and uptake of the MeliCERTes platform<sup>32</sup>. Furthermore, in view of the implementation of the NIS2 Directive, this activity supports coordinated vulnerability disclosure by designated CSIRTs in the CSIRTs Network and the implementation of a European vulnerability database.

In view of the EC Recommendation 4520 (2021) and Council Conclusions of the 20 October 2021 (ST 13048 2021) on 'exploring the potential of the Joint Cyber Unit initiative – complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises', ENISA will engage in exploring the potential of the JCU, along the lines and the roles defined according to ongoing discussions amongst MSs and relevant EU institutions, bodies and agencies. In addition, this activity implements the ENISA Cybersecurity Support Action<sup>33</sup>.

This activity underpins the Situational Awareness service package and contributes to INDEX and NIS service packages. The legal basis for this activity is Article 7 of the CSA.

---

### Objectives



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

---

<sup>32</sup> This is especially relevant for the year 2023 and onwards because the support contract procured by the Commission finishes by the end of 2022.

<sup>33</sup> the Agency will prepare where possible for the future Emergency Response Fund, providing that ENISA will be asked to support it and without pre-empting the outcome of the legislative process.

## Results



- All communities (EU institutions and MSs) use a streamlined and coherent set of SOPs for management of cyber crises
- Efficient tools (secure and with high availability) and methodologies for effective management of cyber crises

## Link to strategic objective (ENISA strategy)



- Effective cooperation amongst operational actors within the Union in case of massive cyber incidents
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 4.1. Support the functioning and operations of the operational networks and communities and cooperation with relevant stakeholders including blueprint actors<sup>34</sup>.
- 4.2. Support coordinated vulnerability disclosure efforts by designing and deploying the EU Vulnerability Database.
- 4.3. Deploy, maintain and promote platforms for operational cooperation and tools including preparations for a secure virtual platform for CyCLONe

## Validation



- 4.1. NLO Network (as necessary)
- 4.2. CSIRTs Network and EU CyCLONe
- 4.3. Blueprint actors

## Stakeholders and levels of engagement

### Partners

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

### Involve / Engage

NISD Cooperation Group, OESs and DSPs, ISACs



<sup>34</sup> CSIRTs Network, CyCLONe, SOCs network, potentially JCU.

## Key performance indicators



Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
4.1 Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA					
CSIRT Network					
Active users – increase from 2020	%	Annual	Platform	115%	110%
Number of exchanges/interactions – increase from 2020	%	Annual	Platform	291%	100%
EU CyCLONe					
Active users – increase from 2020	%	Annual	Platform	143%	100%
Number of exchanges/interactions – increase from 2020	%	Annual	Platform	1,011%	150%*
4.2 Uptake of platforms/tools/SOPs during massive cyber incidents <sup>35</sup>		Ad hoc		N/A	
4.3 Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs including EU vulnerability database	N/A	Biennial	Survey	N/A	Baseline to be established in 2023

## Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
4.1	NIS, SITAW	4.30	44,567	3.70	412,895	0.35	0	8.35	457,462
4.2	NIS, SITAW	1.00	72,978	1.00	69,743	0.20	0	2.20	142,720
4.3	SITAW, NIS	3.00	636,908	3.00	885,440	0.00	0	6.00	1,522,348
<b>Activity total</b>				<b>FTE:</b>	<b>16.55</b>	<b>Budget:</b>	<b>2,122,530</b>		

35 CSIRTs Network, CyCLONe, SOCs network, potentially JCU.

## ACTIVITY 5: Contribute to cooperative response at Union and Member States level



### Overview of activity



This activity contributes to the development of cooperative preparedness and responses at the level of the Union and Member States to large-scale cross-border incidents or crises related to cybersecurity. ENISA is delivering this activity by aggregating and analysing reports to establish a common situational awareness, ensuring information flow between the CSIRTs network, CyCLONe, the Cyber Crisis Task Force and other technical, operational and political decision-makers at Union level and including cooperation with other services of EUIBAs such as CERT-EU and EC3 and the use of an information exchange with security vendors and non-EU cybersecurity entities. The activity includes the development of regular in-depth EU Cybersecurity Technical Situation Reports in accordance with CSA art 7(6).

In addition, the activity foresees, at the request of Member states, the facilitation of the handling of incidents or crises (including analyses and the exchange of technical information). The activity supports Union institutions, bodies, offices and agencies in the public communication of incidents and crises. The activity specific cyber threats, assisting in the assessment of incidents, facilitating the 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 supports operational cooperation, including mutual assistance and situational awareness in the framework of the proposed potential JCU. In addition, this activity implements the ENISA Cybersecurity Support Action<sup>36</sup>.

Moreover the activity pursues the further fostering and optimising of structured cooperation with CERT-EU (please see Annex XIII Annual Cooperation Plan 2023).

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

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

### Objectives



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

<sup>36</sup> The Agency will prepare where possible for the future Emergency Response Fund, provided ENISA will be asked to support it and without pre-empting the outcome of the legislative process.

## Results



- Member States and institutions cooperating effectively during large-scale cross-border incidents or crises
- Stakeholders and public aware of current developments in cybersecurity

## Link to strategic objective (ENISA strategy)



- Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 5.1. Generate and consolidate information (including for the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information at strategic, operational and technical levels<sup>37</sup>
- 5.2. Support technical (including through MeliCERTes) and operational cooperation, incident response coordination and EU wide crisis communication during large-scale cross-border incidents or crises
- 5.3. Maintain, develop and promote the trusted network of vendors or suppliers for information exchange and situational awareness

## Validation



- Blueprint actors

## Stakeholders and levels of engagement



### Partners

EU Member States (including CSIRTs Network members and CyCLONe), EU Institutions, bodies and agencies, other technical and operational blueprint actors, partnership programme for 5.3 (with trusted vendors, suppliers and partners)

### Involve / Engage

Other types of CSIRTs and PSIRTs

<sup>37</sup> Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.

## Key performance indicators



ENISA ability and preparedness to support response to massive cyber incidents	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
5.1 Number of relevant incident responses to which ENISA contributed in accordance with the CSA Art. 7	Number	Annual	Report	775 <sup>38</sup>	TBD
5.2 Number of incidents analysed or curated	Number	Annual	OSINT report	775	
5.3 Number of high visibility incidents analysed	Number	Annual	Flash report	38	
5.4 Number of large-scale cross-border incidents with high impact analysed	Number	Annual	Joint Rapid Report <sup>39</sup>	13	
5.5 Number of incidents to which ENISA contributed in response	Number	Annual	Cyber Assistance Mechanism	1	
5.6 Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents in which ENISA contributes efforts to mitigate	N/A	Biennial	Survey	N/A	Baseline to be established in 2023
5.7 Take up of ENISA support services	Number	Annual	Report	N/A	Baseline to be established in 2023
5.8 Number of trusted vendors	Number	Annual	Report	N/A	Baseline to be established in 2023
5.9 Stakeholder satisfaction with ENISA's ability to provide operational support	N/A	Biennial	Survey	N/A	Baseline to be established in 2023

<sup>38</sup> As of October 2022 for the year 2022.

<sup>39</sup> Structured cooperation with CERT-EU.

## 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	
5.1	SITAW, INDEX	7.40	764,432	0.00	0	0.00	0	7.40	764,432	
5.2	SITAW			1.4	97,701	0.00	0	1.40	97,701	
5.3	SITAW	0.25	51,379	0.95	0	0.00	0	1.20	51,379	
<b>Activity total</b>				<b>FTE:</b>		<b>10</b>		<b>Budget:</b>		<b>913,512</b>



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



### Overview of activity



This activity encompasses actions that seek to establish and support the EU cybersecurity certification framework by preparing and reviewing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the Union's Rolling Work Programme. Actions also include maintaining and evaluating adopted cybersecurity certification schemes and participating in peer reviews. In addition in this activity, ENISA assists the Commission in providing the secretariat of the European Cybersecurity Certification Group (ECCG), co-chairing and providing the secretariat to the Stakeholder Cybersecurity Certification Group (SCCG). ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Article 50 of the CSA.

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

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

### Objectives



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

### Results



- Certified ICT products, services and processes are preferred by consumers and businesses

### Link to strategic objective (ENISA strategy)



- High level of trust in secure digital solutions
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 6.1.** Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes
- 6.2.** Implementing and maintaining established schemes including the evaluation of adopted schemes, participation in peer reviews etc.
- 6.3.** Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks
- 6.4.** Developing and maintaining the necessary provisions and tools and services concerning the Union's cybersecurity certification framework (including a certification website, supporting the Commission in relation to the core service platform of CEF (Connecting Europe Facility) for collaboration and publication, and promoting the implementation of the cybersecurity certification framework etc.

## Validation



- Ad hoc working groups on certification (output 6.1 and 6.2.)
- ECCG (6.1.6.2, 6.3 and 6.4)
- European Commission (outputs 6.1, 6.2, 6.3, 6.4)
- SCCG (output 6.3. and 6.4.)

## Stakeholders and levels of engagement



### Partners

EU Member States (including National Cybersecurity Certification Authorities, ECCG), European Commission, EU institutions, bodies and agencies, Selected stakeholders as represented in the SCCG

### Involve / Engage

Private sector stakeholders with an interest in cybersecurity certification, conformity assessment bodies, national accreditation bodies consumer organisations

## Key performance indicators



1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions 2. Effective preparation of candidate certification schemes prepared by ENISA	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
6.2 Stakeholders' level of trust in the digital solutions of certification schemes (citizens, public sector and businesses).		Biennial	Survey	N/A	Baseline to be established in 2023
6.3 Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework		Biennial	Survey	N/A	Baseline to be established in 2023

1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions 2. Effective preparation of candidate certification schemes prepared by ENISA	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
6.4 Number of candidate certification schemes prepared by ENISA <sup>40</sup>	Number	Annual	Report	N/A	Minimum 75% of schemes formally requested to be under ongoing development
6.5 Number of people or organisations engaged in the preparation of certification schemes <sup>41</sup>	Number	Annual	Report	N/A	Minimum: 10 organisations; 10 individual experts; 50% of EU MSs joining an AHWG; 30% of organisations to be an SME; 5% to be from a third country
6.6 Satisfaction with ENISA's support for the preparation of candidate schemes		Biennial	Survey	N/A	Baseline to be established in 2023

### Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
6.1	CERTI, NIS	4.65	565,936	0.70	945	0.00	0	5.35	566,881
6.2	CERTI	1.35	90,720	0.00	-	0.00	0	1.35	90,720
6.3	CERTI	1.05		0.00		0.00	0	1.05	-
6.4	CERTI	1.10	75,859	0.15	71,118	0.00	0	1.25	146,977
<b>Activity total</b>				<b>FTE: 9</b>		<b>Budget: 804,578</b>			

40 Number of schemes formally requested by the Commission or given the go ahead on the basis of the Union Rolling Work Programme, and the number of cybersecurity certification schemes under development by ENISA.

41 Numerical value from ENISA records on a per scheme basis to produce number of: organisations, individual experts, EU Member States, percentage of SMEs, percentage of third country organisations involved that support the promulgation of a cybersecurity certification scheme.

## ACTIVITY 7: Supporting European cybersecurity market and industry



---

### Overview of activity



This activity seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence on outside sources and increase the capacity of the Union and to reinforce supply chains to the benefit of the internal market. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation. Actions to support this activity include producing analyses and guidelines as well as good practices on cybersecurity requirements, facilitating the establishment and take up of European and international standards across applicable areas such as risk management as well as performing regular analyses 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. It also involves creating platforms for collaboration among the cybersecurity market players, in order to improve the visibility of trustworthy and secure ICT solutions in the internal digital market.

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

This activity contributes to the CERTI and NIS service packages.

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

---

### Objectives



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

## Results



- Contributing towards an understanding of cybersecurity market dynamics
- A more competitive European cybersecurity industry, SMEs and start-ups

## Link to strategic objective (ENISA strategy)



- High level of trust in secure digital solutions
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 7.1.** Market analysis of the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes
- 7.2.** Monitoring developments in related areas of standardisation, analysis of gaps in standardisation and the establishment and take-up of European and international cybersecurity standards for risk management in relation to certification
- 7.3.** Guidelines and good practices on cybersecurity for ICT products, services and processes and recommendations to the EC and the ECCC
- 7.4.** Monitoring and documenting the dependencies and vulnerabilities of ICT products and services

## Validation



- SCCG (outputs 7.2 & 7.3)
- ENISA Advisory Group (output 7.1)
- NLO (as necessary)
- ECCG (output 7.4)
- Ad hoc working groups cybersecurity market analysis (output 7.1)

## Stakeholders and levels of engagement



### Partners

EU Member States (including entities with an interest in cybersecurity market monitoring e.g. NCCA, National Standardisation Organisations), European Commission, EU institutions, bodies and agencies, European Standardisation Organisations (CEN, CENELEC, ETSI), Private sector or ad hoc standards setting organisations

### Involve / Engage

Private sector stakeholders with an interest in cybersecurity market and/or standardisation, International Organisation for Standardisation / International Electrotechnical Committee, consumer organisations

## Key performance indicators



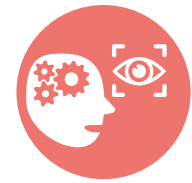
Effectiveness of ENISA's supporting role for participants in the European cybersecurity market	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
7.1. Number of market analyses, guidelines and good practices issued by ENISA					
Cybersecurity market analysis framework	Number	Annual	Reports	2	1
7.2. Uptake of lessons learned or recommendations from ENISA reports (average of responses)	%	Annual	Survey	49%	60%
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work	%	Biennial	Survey	N/A	Baseline to be established in 2023

## Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
7.1	CERTI, INDEX, CERTI	2.90	116,161	0.35	0	0.00	0	3.25	116,161
7.2	CERTI, NIS	1.60	112,132	0.20	0	0.00	0	1.80	112,132
7.3	CERTI	0.50	73,017	0.00	0	0.00	0	0.50	73,017
7.4	CERTI	0.50	54,716	0.00	0	0.00	0	0.50	54,716
<b>Activity total</b>				<b>FTE: 6</b>		<b>Budget: 356,027</b>			

## ACTIVITY 8: Knowledge of emerging cybersecurity challenges and opportunities



### Overview of activity



This activity delivers on ENISA's strategic objectives SO7 (efficient and effective management of cybersecurity knowledge for Europe) and supports SO6 (foresight on emerging and future cybersecurity challenges). In particular, work under this activity shall provide strategic long-term analyses, guidance and advice on emerging and future technologies, based on the results of regular cybersecurity foresight exercises. Typical examples may include artificial intelligence, quantum computing, space technology, etc

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

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

These activities leverage the expertise on relevant legal, regulatory, economic and social 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 various target audiences in accordance with their needs and contribute to the improvement of the state of cybersecurity across the Union.

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

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

### Objectives



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

## Results



- Decisions about cybersecurity are future proof and take account of the trends, developments and knowledge across the ecosystem
- MSs have the tools for assessing and understanding their cybersecurity maturity

## Link to strategic objective (ENISA strategy)



- Foresight on emerging and future cybersecurity challenges
- Efficient and effective management of cybersecurity information and knowledge for Europe
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 8.1.** Develop and maintain the EU cybersecurity index
- 8.2.** Collect and analyse information to report on the cyber threat landscapes
- 8.3.** Analyse and report incidents as required by Art 5(6) of the CSA as well as other sectorial legislation (e.g. DORA, eIDAS Art. 10, etc.)
- 8.4.** Develop and maintain a portal (information hub), respectively identify appropriate tools for a one-stop-shop to organise and make available to the public information on cybersecurity, and the establishment of a procedural framework to support knowledge management activities maximising synergies with the European Cybersecurity Atlas
- 8.5.** Foresight on emerging and future cybersecurity challenges and recommendations.
- 8.6.** Building and exchanging knowledge on ransomware threat (incl. capacity building and awareness raising and education)<sup>42</sup>

## Validation



- NLO Network (for Output 8.4 and 8.5, and as necessary for other outputs)
- ENISA Advisory Group (as necessary)
- ENISA ad hoc working groups (for Outputs 8.1, 8.2, 8.4 and 8.6 as necessary)
- CSIRT Network (output 8.1 and 8.2)
- Formally established bodies and expert groups as necessary (output 8.3)
- NIS Directive Cooperation Group (output 8.1)

## Stakeholders and levels of engagement



### Partners

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

### Involve / Engage

Industry, research and academic institutions and bodies

<sup>42</sup> Output suppressed during the 2023 work programme due to insufficient resources.



## Key performance indicators



ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including foresight on emerging and future challenges	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
8.1 Number of users and frequency of use of a dedicated portal (observatory)	N/A <sup>43</sup>				
8.2. Number of recommendations, analyses and challenges identified and analysed (reports)	Number	Annual	ENISA reports and studies	288	300
8.3 Number of recommendations, analyses and challenges identified and analysed (reports)	Number	Biennial	Survey	N/A	
8.4 The influence of foresight on the development of ENISA's work programme	Number	Annual	SPD	N/A	Applicable as of 2023
8.5 Uptake of reports generated in activity 8	Number	Annual	Media monitoring report	N/A	Applicable as of 2023
8.6 Uptake of the cybersecurity index	Number	Annual	Index platform	N/A	Applicable as of 2023

## Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
8.1	INDEX	2.50	181,982	0.00		0.00		2.50	181,982
8.2	INDEX, SITAW, NIS	2.00	156,616	0.35		0.25	15,000	2.60	171,616
8.3	INDEX, SITAW, NIS	1.00	58,791	0.20		0.00	-	1.20	58,791
8.4	INDEX, TREX	1.00	152,235	0.00		0.00	-	1.00	152,235
8.5	INDEX	1.10	207,257			0.10	40,000	1.20	247,257
8.6 <sup>44</sup>									
<b>Activity total</b>				<b>FTE:</b>		<b>8.50</b>		<b>Budget: 811,881</b>	

43 InfoHub is in the process of being developed.

44 Output suppressed in 2023 due to insufficient resources.

# ACTIVITY 9: Outreach and education



## Overview of activity



This activity seeks to raise the overall awareness of cybersecurity risks and practices. In cooperation with Member States, Union 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 Union. Under this activity the Agency will be organising regular outreach campaigns, providing guidance on best practices and supporting 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 Union's efforts to cooperate with third countries and international organisations on cybersecurity.

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

## Objectives



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

## Results



- Greater understanding of cybersecurity risks and practices
- Stronger European cybersecurity through higher global resilience

## Link to strategic objective (ENISA strategy)



- High level of trust in secure digital solutions
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 9.1 Develop activities to enhance behavioural change by essential service providers in critical sectors (as defined by the NISD)
- 9.2 Promote cybersecurity topics, education and good practices on the basis of the strategy of ENISA's stakeholders
- 9.3 Implement ENISA's international strategy and outreach
- 9.4 Organise European cybersecurity month (ECSM) and related activities
- 9.5 Report on needs and gaps in cybersecurity skills, and support skills development, maintenance and implementation (including the Digital Education Action Plan and a report on higher-education programmes)
- 9.6 Implement the Cybersecurity in Education roadmap<sup>45</sup>

## Validation



- Management Board (as necessary)
- SCCG (for certification related issues under output 9.2)
- NLO Network (as necessary)
- ENISA Advisory Group (outputs 9.1 and 9.2)
- AHWG on cybersecurity skills (output 9.5)

## Stakeholders and levels of engagement



### Partners

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

### Involve / Engage

ENISA National Liaison Officers (NLOs), DG CONNECT, NIS Operators of Essential services, European Cybersecurity Competence Centre, International partners (CISA, NIST etc)

<sup>45</sup> Roadmap developed by ENISA during the course of 2022.

## Key performance indicators



Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
<b>Level of outreach</b>					
9.1 Number of cybersecurity incidents reported having human error as a root cause	Number	Annual	Report	N/A	Baseline to be established in 2023
9.2 Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics					
Social media impressions	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	20,756,630	20,000,000
Social media engagement	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	117,720	150,000
Video views	Average number	Annual	Social media (Facebook, LinkedIn, Twitter)	2,021,129	3,000,000
Website visits	Average number	Annual	ENISA website	123,504	150,000
Participation in events	Average number	Annual	Media monitoring	5	10
References	Average number	Annual	Website announcements	40	50
9.3 Number of cybersecurity programmes (courses) and participation rates (a)					
Total number of students enrolled in the first year of academic programmes (2020)	Number	Annual	Report <sup>46</sup>	4,843	6,000
Number of male students	%	Annual	Report	80%	70%
Number of female students	%	Annual	Report	20%	30%
Total number of cybersecurity programmes (2020)	Number	Annual	Report	119	130

46 <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>.

Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU Level of outreach	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
Number of postgraduate programmes	%	Annual	Report	6%	5%
Number of masters programmes	%	Annual	Report	77%	80%
Number of bachelors programmes	%	Annual	Report	17%	15%
9.4 Geographical and community coverage of outreach in the EU	Number	Annual			Baseline to be established in 2023
9.5 Level of awareness of cybersecurity across the EU / general public (e.g. EU barometer)		Biennial		N/A	Baseline to be established in 2023

### Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total	
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR
9.1 <sup>47</sup>	NIS	1.00	66,482	0.50	43,688	0.00	0.00	1.50	110,170
9.2	INDEX, CERTI	0.75	42,701	0.75	31,314	0.00	0.00	1.50	74,014
9.3	SITAW, TREX	0.75	-	0.75	26,544	0.00	0.00	1.50	26,544
9.4	TREX	0.10	-	0.90	95,147	0.00	0.00	1.00	95,147
9.5*	INDEX, TREX	0.40	47,441	0.60	59,775	0.00	0.00	1.00	107,216
9.6	INDEX	0.20	38,059	0.80	38,059	0.00	0.00	1.00	76,117
<b>Activity total</b>				<b>FTE:</b>	<b>7.50</b>	<b>Budget:</b>		<b>489,209</b>	

47 Outputs 9.1 and 9.5 would be priority outputs for the consuming of any surplus budget in 2023.

# ACTIVITY 10:

## Advise on research and innovation needs and priorities



### Overview of activity



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

To prepare this strategic advice, ENISA will take full account of past and ongoing research, activities in development and technology assessment, 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, industries, start-ups and digital innovation hubs to consolidate information and identify gaps, challenges and opportunities in research and innovation from the different quadrants of the community.

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

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

### Objectives



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

### Results



- Research and development of cybersecurity technology reflecting the needs and priorities of the Union
- Funding the development of cybersecurity technologies that meet the Union's ambition to become more resilient, autonomous and competitive

### Link to strategic objective (ENISA strategy)



- Foresight on emerging and future cybersecurity challenges
- Empowered and engaged communities across the cybersecurity ecosystem

## Outputs



- 10.1** Consolidated cybersecurity research and innovation roadmap across the EU
- 10.2** Collect and analyse information on new and emerging information and communications technologies in order to identify gaps, trends, opportunities and threats (research & innovation observatory)
- 10.3** Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment

## Validation



- The European Cybersecurity Competence Centre and Network of National Coordination Centres and Competence Centre Governing Board (output 10.2 & 10.3)
- NLO as necessary

## Stakeholders and levels of engagement



### Partners

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

### Involve / Engage

Market actors – in particular the NIS sectors' stakeholders (e.g. OES), academia and research communities, cybersecurity industry as well as solution and service providers

## Key performance indicators



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

## Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)		Total		
		FTE	EUR	FTE	EUR	FTE	EUR	FTE	EUR	
10.1				1	41,428	0.00	0	1	41,428	
10.2	NIS	0.10	0	0.90	123,453	0.00	0	1	123,453	
10.3				1.8	25,490	0.20	5,000	2	30,490	
<b>Activity total</b>				<b>FTE:</b>		<b>4</b>		<b>Budget:</b>		<b>195,371</b>



### 3.2. CORPORATE ACTIVITIES

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

## ACTIVITY 11: Performance and risk management



### Overview of activity



This activity seeks to achieve the requirements set out in Art 4(1) of the CSA that sets an objective for the Agency to: 'be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks'. This objective requires an efficient performance and risk management framework, and the development of single administrative practices. It also includes building an internal capacity for contribution, e.g. via shared services, to the EU Agencies network and in key areas of the Agency's expertise (e.g. cybersecurity risk management).

Under this activity ENISA will continue to enhance the key objectives of the renewed organisation, as described in the MB decision No MB/2020/5, including the need to address the gaps in the Agency's quality assessment framework, enhance proper and functioning internal controls and compliance checks. In terms of resource management the budget management committee ensures the Agency adheres to sound financial management.

The legal basis for this activity is Art 4(1) and Art 32 of the CSA, the latter of which focuses strongly on sound financial management principles with a view to maximising value to stakeholders.

### Objectives



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

### Results



- Maximise quality and value provided to stakeholders and citizens
- Building lasting credibility and trust

### Link to strategic objective (ENISA strategy)



- Sound resource and risk management

## Outputs



- 11.1** Maintain the framework for performance management including through single administrative practices across the Agency
- 11.2** Develop and implement annual communications strategy
- 11.3** Develop and implement risk management plans including cybersecurity risk assessment for IT systems, including focus on quality management framework and business processes as well as relevant policies
- 11.4** Maintain and monitor the implementation of Agency wide processes for IT management and develop processes for budgetary management
- 11.5** Manage and provide secretariats for statutory bodies (EB, MB, NLO and AG)
- 11.6** Obtain and maintain the EU Eco-Management and Audit Scheme (EMAS) certificate through continuous overview of the impact of CO2 on all operations of the Agency in line with the applicable legal framework and publish a statement on the environment

## Validation



- Management Team
- Chairs of statutory bodies (Output 10.5)
- Budget Management Committee
- IT Management Committee
- Intellectual Property Rights Management Committee
- Staff Committee
- ENISA Ethics Committee

## Stakeholders and levels of engagement



### Partners

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

### Involve / Engage

All ENISA stakeholders

## Key performance indicators



Organisational performance culture Trust in ENISA brand	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
11.1. Proportion of key performance indicators reaching targets	%	Annual	Report	N/A <sup>48</sup>	65%
11.2. Individual staff contribution to achieving the objectives of the agency via clear link to KPIs in staff career development report (CDR report) (all units aggregated)	%	Annual	Objectives 2021	60%	85%
11.3. Exceptions in the risk register	Number	Annual	Internal control	16	11
Deviation from financial regulations	Number	Annual	Internal control	14	10
Deviation from staff regulations	Number	Annual	Internal control	2	1
11.4. Number of complaints filed against ENISA, including number of inquiries or complaints submitted to the European Ombudsman	Number	Annual	Report	19	12
11.5 Number of complaints addressed in a timely manner and according to relevant procedures	Number	Annual	Internal control files	N/A	Baseline to be established in 2023
11.6 Number of high risks identified in annual risk assessment exercise	Number	Annual	Internal control files	N/A	Baseline to be established in 2023
11.7 Implementation of risk treatment plans	Number	Annual	Report	N/A	Baseline to be established in 2023
11.8 Number and types of activities at each level of engagement <sup>49</sup>	Number	Annual	Report	N/A	Baseline to be established in 2023
11.9. Observations from external audit bodies (e.g. European Court of Auditors ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed)	Number	Annual	Report	4	2
11.10 Level of trust in ENISA		Biennial	Survey	N/A	Baseline to be established in 2023

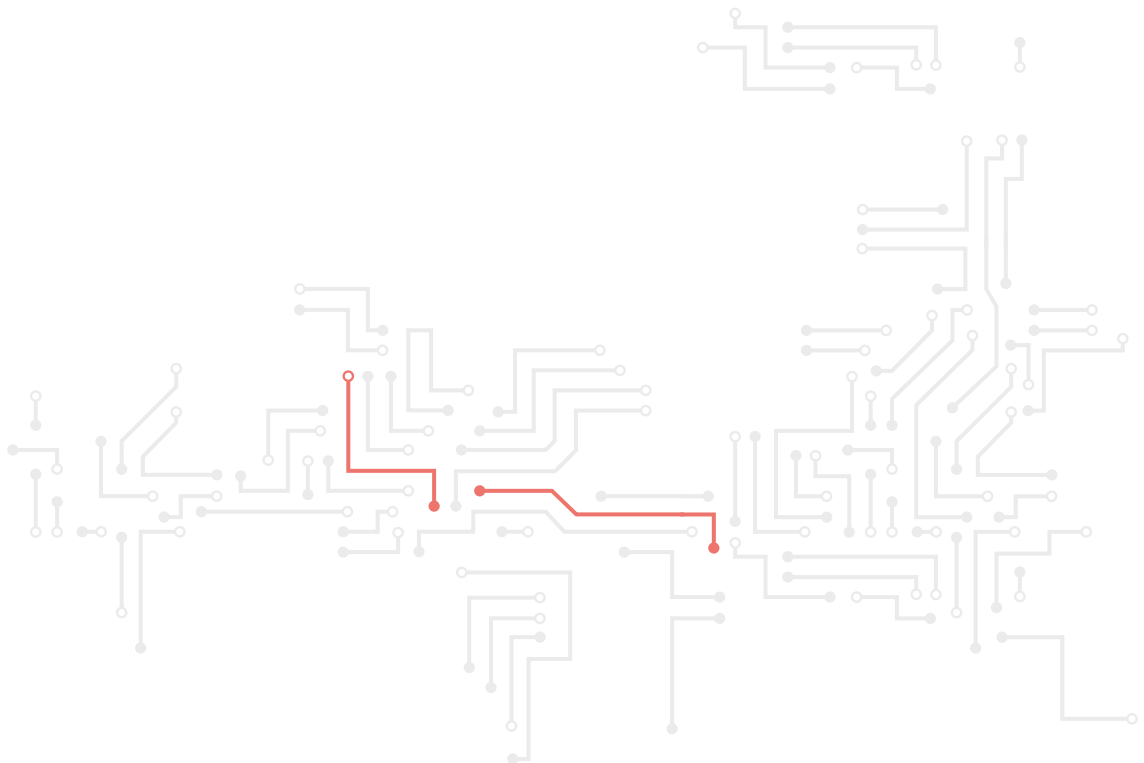
48 Baselines were available as of the 2021 annual activity report therefore proportion of metrics reaching targets will be assessed in the 2022 annual activity report.

49 Relates to the stakeholder strategy and its implementation, refers to activities such as conferences, workshops etc.

## Resource forecast



Outputs	Service package related to category A	A (reserved for tasks to maintain statutory service)		B (reserved for other regular statutory tasks)		C (reserved for ad hoc statutory tasks)	
		FTE	EUR	FTE	EUR	FTE	EUR
11.1	All service packages	1		5.5	160,850		
11.2	All service packages	2		2	304,000		
11.3	All service packages	0.5		3	197,000		
11.4				1.5	0		
11.5				2	126,500		
11.6				0.5	61,500		
<b>Activity total</b>		<b>FTEs:</b>		<b>18</b>	<b>Budget:</b>		<b>849,000</b>



## ACTIVITY 12: Staff development and working environment



### Overview of activity



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

The actions which will be pursued under this activity will focus on making sure that the Agency's HR resources fit the needs and objectives of ENISA, by attracting, retaining and developing talent and building ENISA's reputation as an agile and knowledge-based organisation where staff can evolve personally and professionally, where staff are kept engaged, motivated and have a sense of belonging. Emphasis will be placed on the development of competency and ways to make ENISA an 'employer of choice' in order to support ENISA's objectives. This 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 to maintain high quality services in the administrative and operational areas. ENISA will further improve the support given to it in strategic planning and resource management, leading to a constant optimisation of resources under short- and long-range time-frames. This will enable ENISA to enhance its capabilities in future-readiness and continue its path towards an agile, knowledge-based and matrix way of working. The Agency will continue to look into flexible (50/50) working arrangements to better balance work requirements in a pragmatic manner.

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

### Objectives



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

## Results



- ENISA as an employer of choice, enabling growth and excellence in a secure environment

## Link to strategic objective (ENISA strategy)



- Build an agile organisation focused on people

## Outputs



- 12.1** Manage and provide recurring quality support services in the area of resources, security<sup>50</sup> and infrastructure for ENISA staff, employees, corporate partners and visitors
- 12.2** Develop and implement the Agency's corporate strategy (including HR strategy) with an emphasis on talent development and growth, innovation and inclusiveness;
- 12.3** Enhance operational excellence and digitalisation through modern, secure and streamlined ways of working and self-service functionalities
- 12.4** Provide a secure, safe, modern and welcoming place to work (and telework) including staff welfare
- 12.5** Establish standards for the provision of services and processes for optimising services

## Validation



- Management Board (Output 12.2)
- Management Team
- IT Management Committee
- Budget Management Committee
- Staff Committee

## Stakeholders and levels of engagement



### Partners

ENISA staff members and EU institutions, bodies and agencies

### Involve / Engage

Private sector and international organisations

<sup>50</sup> Including full accreditation of the Agency to handle and manage EUCI by end of 2023 confirmed by DG Human Resources and Security.

## Key performance indicators



Staff commitment, motivation and satisfaction	Unit of measurement	Frequency	Data source	Results 2021	Target 2023
12.1 . Staff satisfaction survey (including the attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools)	%	Annual	Staff satisfaction survey	72%	75%
12.2-. Quality of ENISA training and career development activities organised for staff	%	Annual	Staff satisfaction survey	49%	55%
12.3. Reasons for staff departure (exit interviews) <sup>51</sup>	Scale 1–10	As required	HR files	7.1	7.5
12.4 Turnover rates	%	Annual	HR files	3%	3%
12.5 Establishment plan posts filled	%	Annual	HR files	91%	95%
12. 6. Resilience and quality of ENISA IT systems and services	%	Annual	IT reports and staff satisfaction survey	78%	80%
12.7 Percentage of procurement procedures launched via e-tool (PPMT)	%	Annual	Procurement files		> 80 %
12.8 Percentage of payments made within 30 days	%	Annual	Finance files		> 90%
12.9 Late Payments	%	Annual	Finance files		<10%

<sup>51</sup> Standardised set of ten questions with a scale of 1 to 10 that provide an opportunity for ENISA to seek feedback about a staff member's experience. The higher the number the better the experience.

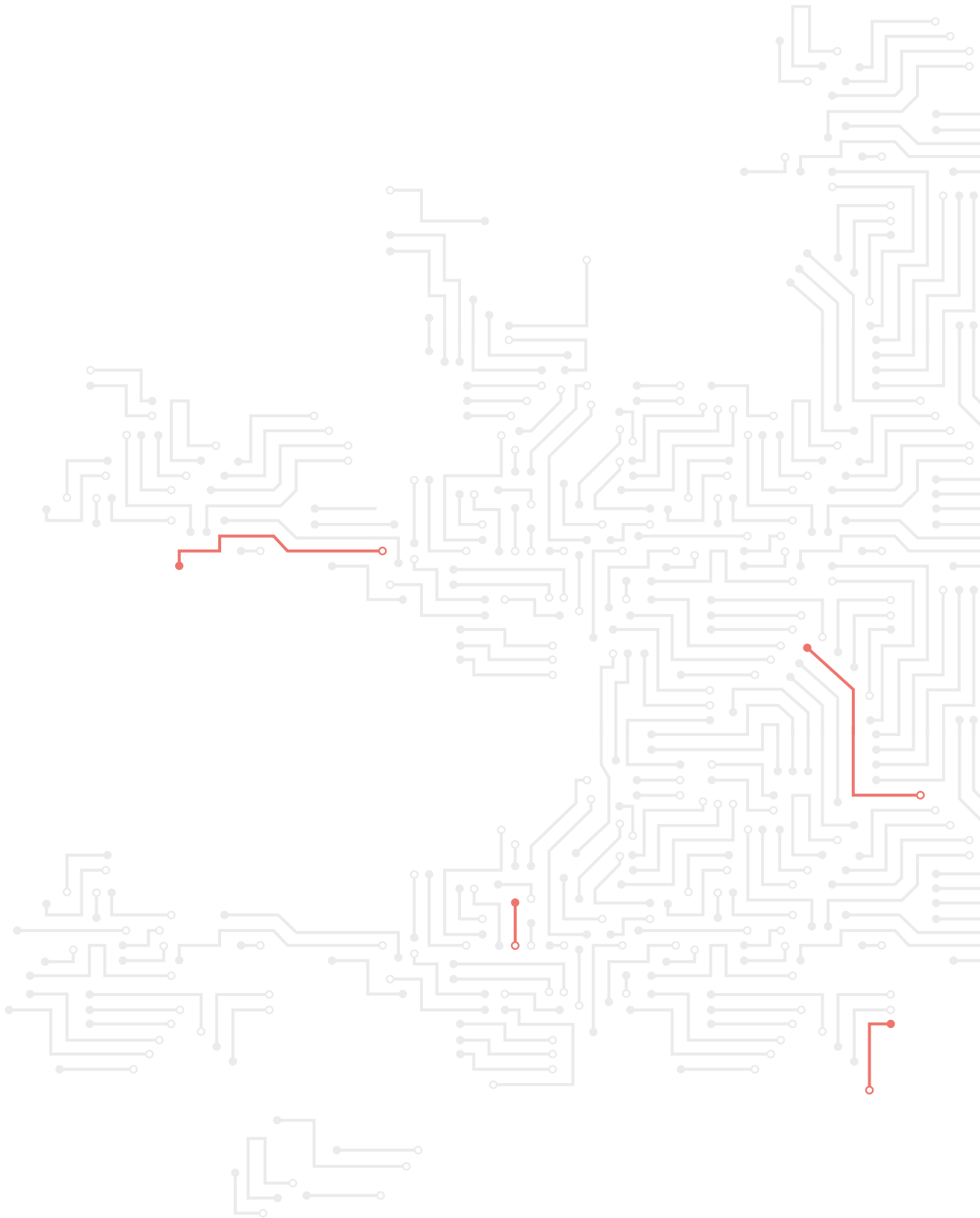
## Resource forecast




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)	
		FTE	EUR	FTE	EUR	FTE	EUR
12.1				9	2,138,000		
12.2				3	383,000		
12.3				1.5	964,000		
12.4				1.5	832,000		
12.5				2	100,000		
<b>Activity total</b>		<b>FTEs:</b>		<b>17</b>	<b>Budget:</b>	<b>4,417,000<sup>52</sup></b>	

52 Indicated budget excludes staff (TA, CA, SNE) salaries and allowances.





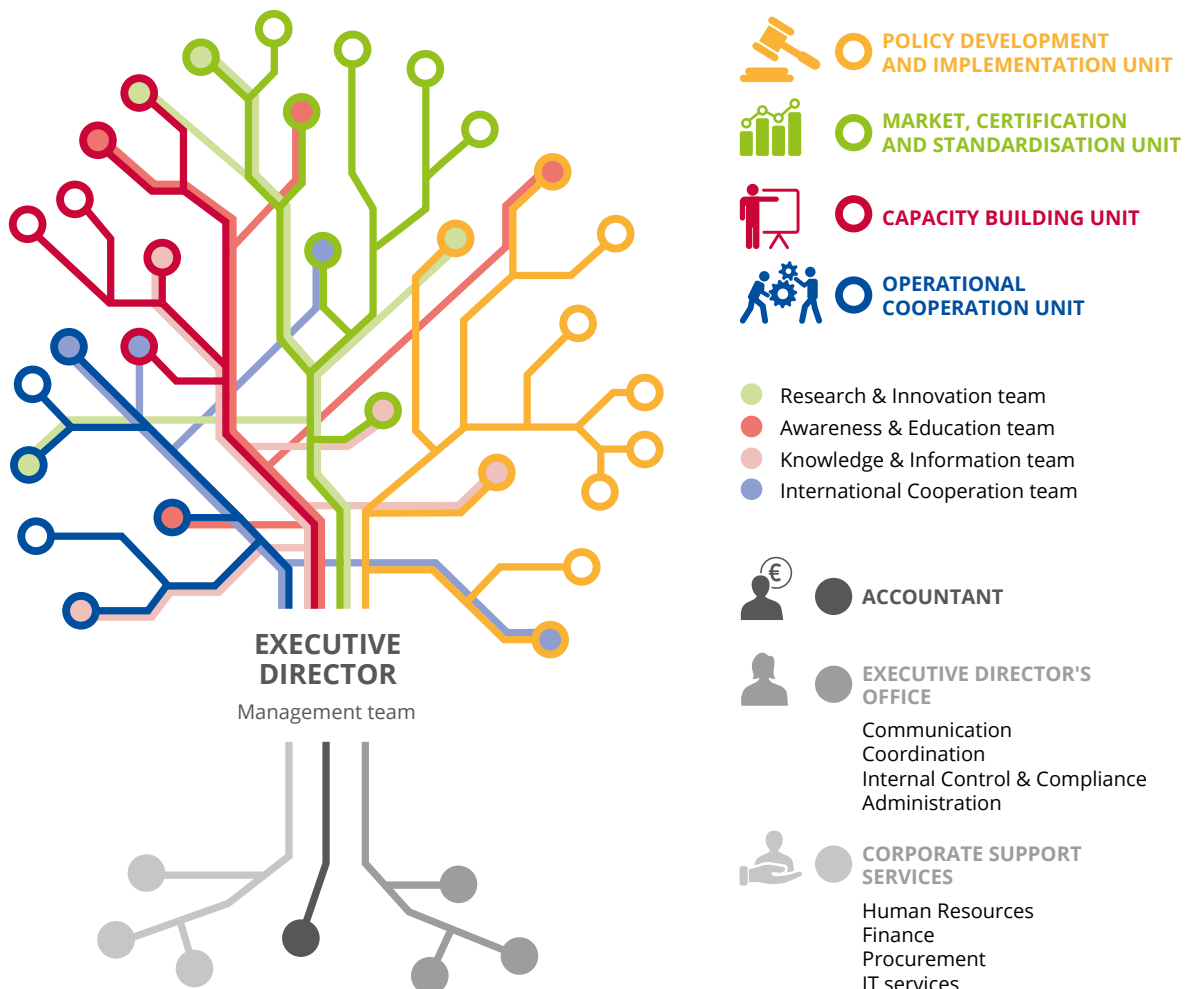
A large, bold, white capital letter 'A' is centered in the upper half of the image. The background is a solid light blue color, overlaid with a dense, repeating pattern of white circuit board traces and nodes, resembling a printed circuit board (PCB) layout. The traces are thin and form a complex, interconnected network of lines and small circles.

A

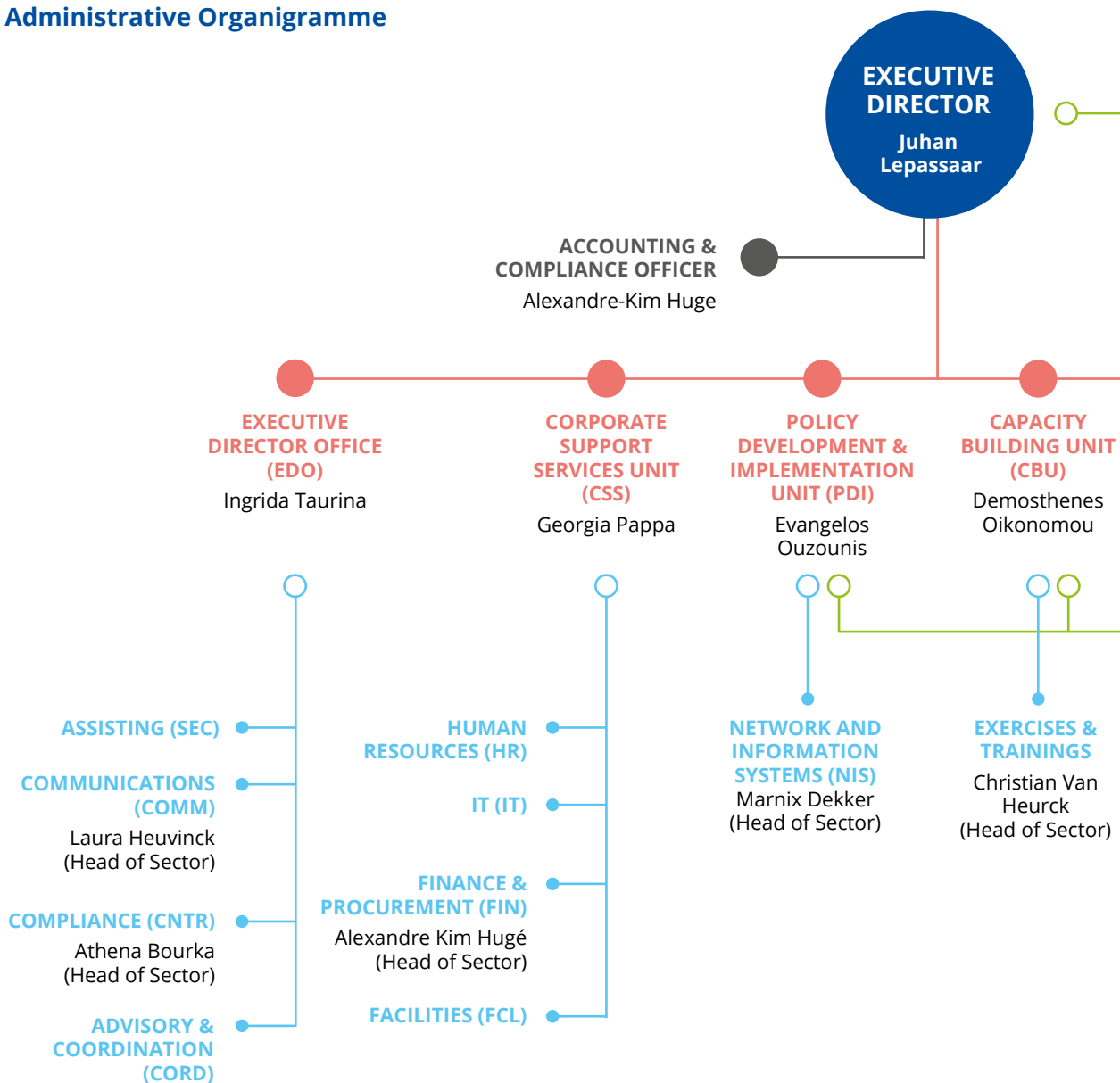
# ANNEX 1

## ORGANISATION CHART

### AS OF 1 JANUARY 2022



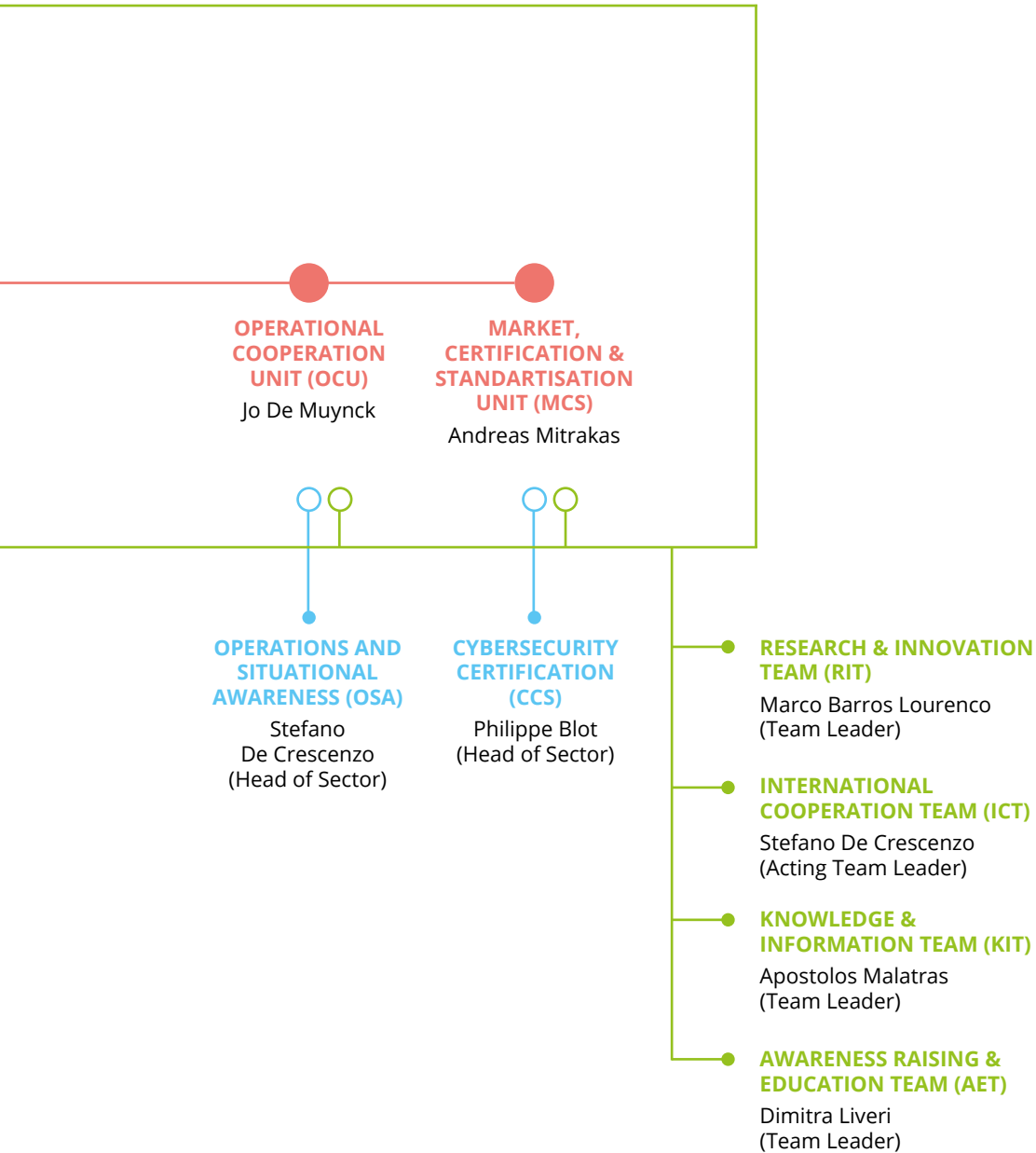
## Administrative Organigramme



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

### Status in-house staff (AD;AST;CA;SNEs) on 31. 12. 2022

ED*	EDO	CSS	PDI	CBU	OCU
AD 2	AD 7	AD 2	AD 15	AD 8	AD 10
<b>Total 2</b>	AST 7	AST 6	AST 0	AST 2	AST 1
	CA 2	CA 7	CA 5	CA 7	CA 3
* ED and accountant	SNE 1	SNE 0	SNE 0	SNE 1	SNE 6
	<b>Total 17</b>	<b>Total 15</b>	<b>Total 17</b>	<b>Total 18</b>	<b>Total 20</b>



<b>MCS</b>	
AD	14
AST	2
CA	3
SNE	2
<b>Total</b>	<b>21</b>

<b>SUMMARY</b>	
<b>AD</b>	<b>55</b>
<b>AST</b>	<b>18</b>
<b>CA</b>	<b>27</b>
<b>SNE</b>	<b>10</b>
<b>Total</b>	<b>110</b>

# ANNEX 2

## RESOURCE ALLOCATION PER ACTIVITY 2023–2025

The indicative allocation of the total financial and human resources for 2023 following the activities as described in part 3.1 of Section III and the corporate activities as described in part 3.2 of Section III are presented in the table below. The allocation was done by following the direct budget and FTEs as indicated for each activity with indirect budgets being assigned in accordance with causal relationships.

The following assumptions are used in the simplified ABB methodology

- The budget allocation of each activity includes the direct and indirect budget attributed to each activity.
- Direct budget is the cost estimate of each of the 10 operational activities as indicated under Section 3.1 of the SPD 2023-2025 (carried out under Articles 5-12) in terms of goods and services to be procured.
- Indirect budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs, attributable to each activity. The indirect budget is allocated to activities based on various drivers. The main driver for the allocation of costs was the number of foreseen direct FTEs for each operational activity in 2023.
- In order to estimate the full costs of operational activities, both corporate activities (Act 11-12) shall be distributed accordingly to all operational activities based on the respective drivers.



Table 4.

Allocation of human and financial resources (2023)	Activities as referred to in Section 3	Direct and indirect budget allocation (EUR)	FTE allocation
Providing assistance on policy development	Activity 1	907,618.48	4.75
Supporting implementation of Union policy and law	Activity 2	2,353,536.42	13.00
Building capacity	Activity 3	3,380,533.35	13.75
Enabling operational cooperation	Activity 4	4,128,083.63	16.50
Contributing to cooperative response at the level of the Union and Member States	Activity 5	2,128,998.78	10.00
Development and maintenance of EU cybersecurity certification framework	Activity 6	1,898,516.44	9.00
Supporting European cybersecurity market and industry	Activity 7	1,085,319.11	6.00
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	1,845,044.44	8.50
Outreach and education	Activity 9	1,400,23.94	7.50
Research and innovation	Activity 10	681,566.05	4.00
Performance and risk management	Activity 11	2,844,126.72	18.00
Staff development and working environment	Activity 12	2,529,327.63	17.00
<b>TOTAL</b>		<b>25,183,495.00</b>	<b>128.00</b>



# ANNEX 3

## FINANCIAL RESOURCES

### 2023–2025

**Table 5. Revenue**

Revenues	2022	2023
EU contribution	23,633,000	24,475,757
Other revenue (EFTA)	574,625	707,738
<b>TOTAL</b>	<b>24,207,625</b>	<b>25,183,495</b>

Revenues	"2021 Executed Budget"	" 2022 Adopted budget "	VAR 2023 / 2022	Draft Estimated budget 2023	Envisaged 2024	Envisaged 2025
1 Revenue from fees and charges						
2 EU contribution	22 248 000	23 633 000	4%	24 475 757	24 610 000	25 010 000
- of which assigned revenues deriving from previous years' surpluses **	579 113			320 868	320 868	320 868
- of which Reserve conditional to approval of NIS2 Directive		610 000		610 000	610 000	610 000
3 third countries contribution (incl. EEA/EFTA and candidate countries)	585 060	574 625	23%	707 738	711 672	723 392
- of which EEA/EFTA (excl. Switzerland)	585 060	574 625	23%	707 738	711 672	723 392
- of which Candidate Countries						
4 Other contributions	317 071	*	N/A	*	*	*
5 Administrative operations						
- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6 Revenues from services rendered against payment						
7 Correction of budgetary imbalances						
<b>TOTAL REVENUES</b>	<b>23 150 131</b>	<b>24 207 625</b>	<b>4%</b>	<b>25 183 495</b>	<b>25 321 672</b>	<b>25 733 392</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 2024-2025 same surplus as indicated under 2023 is included with 2,93% EFTA proportionality factor

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



Table 6. Expenditure

Expenditure	2022		2023	
	Commitment appropriations	Commitment appropriations	Commitment appropriations	Payment appropriations
Title 1	12,494,335	12,494,335	12,719,412	12,719,412
Title 2	2,824,300	2,824,300	3,519,470	3,519,470
<b>Title 3</b>	<b>8,888,990</b>	<b>8,888,990</b>	<b>8,944,613</b>	<b>8,944,613</b>
<b>Total expenditure</b>	<b>24,207,625</b>	<b>24,207,625</b>	<b>25,183,495</b>	<b>25,183,495</b>

Table 7.

Expenditure (in EUR)	Commitment and Payment appropriations					
	Executed budget 2021	Adopted Budget 2022 Agency request	Draft estimated budget 2023	VAR 2023 / 2022	Envisaged in 2024	Envisaged in 2025
<b>Title 1. Staff Expenditure</b>	<b>10 799 493</b>	<b>12 494 335</b>	<b>12 719 412</b>	<b>2%</b>	<b>12 789 201</b>	<b>12 997 153</b>
11 Staff in active employment *	8 370 300	10 837 880	11 019 993	2%	11 080 457	11 260 625
12 Recruitment expenditure	306 022	412 000	404 684	-2%	406 904	413 521
13 Socio-medical services and training	1 371 493	853 000	923 735	8%	928 804	943 906
14 Temporary assistance	751 678	391 455	371 000	-5%	373 036	379 101
<b>Title 2. Building, equipment and miscellaneous expenditure</b>	<b>3 855 317</b>	<b>2 824 300</b>	<b>3 519 470</b>	<b>25%</b>	<b>3 538 781</b>	<b>3 596 312</b>
20 Building and associated costs	1 312 041	914 550	1 357 750	48%	1 365 200	1 387 398
21 Movable property and associated costs	271 592	160 000	0	-100%	0	0
22 Current corporate expenditure	686 263	320 000	472 650	48%	475 244	482 961
23 Corporate ICT	1 585 422	1 429 750	1 689 070	18%	1 698 338	1 725 953
<b>Title 3. Operational expenditure</b>	<b>8 383 370</b>	<b>8 888 990</b>	<b>8 944 613</b>	<b>1%</b>	<b>8 993 690</b>	<b>9 139 928</b>
30 Activities related to meetings and missions	504 740	387 000	438 600	13%	441 007	448 177
32 Horizontal operational activities	0	0	0		0	0
36/37 Core operational activities	7 878 630	8 501 990	8 506 013	0%	8 552 684	8 691 750
<b>TOTAL EXPENDITURE</b>	<b>23 038 179</b>	<b>24 207 625</b>	<b>25 183 495</b>	<b>4%</b>	<b>25 321 672</b>	<b>25 733 393</b>

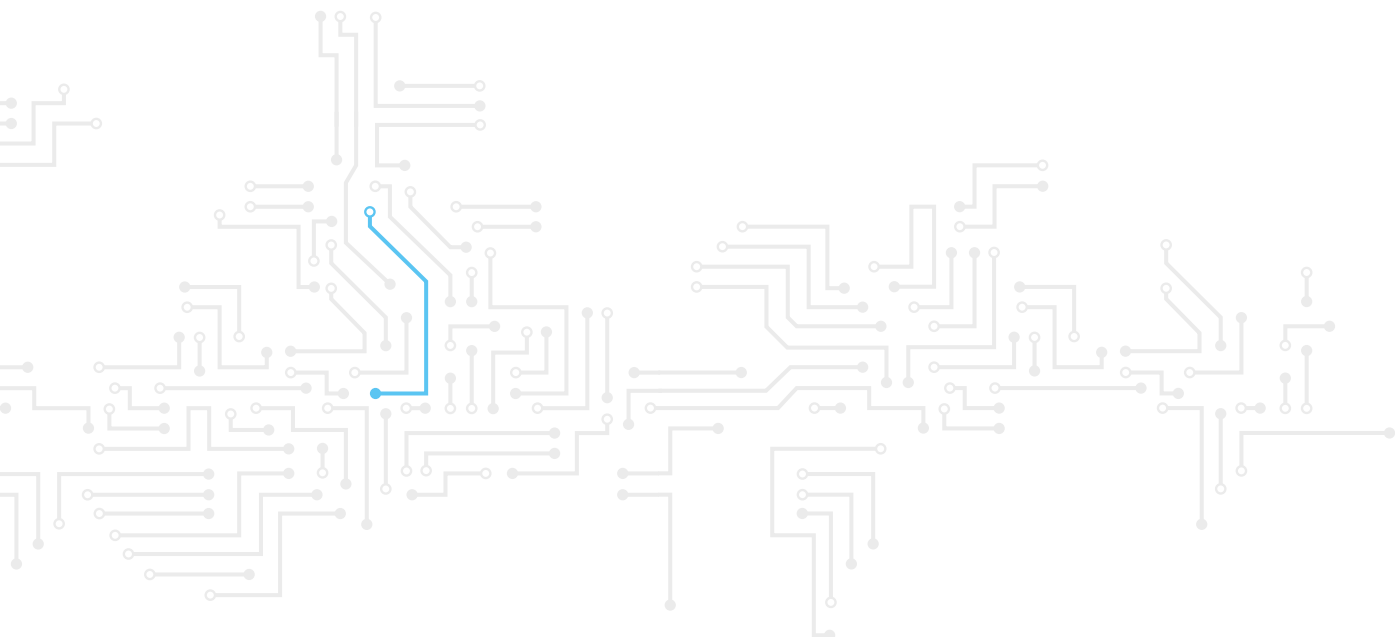
\* for years 2022-2025 chapter 11 includes an amount of EUR 610 thou as a reserve conditional to approval of NIS Directive (for salaries of new posts)

**Table 8. Budget out-turn and cancellation of appropriations**

Budget outturn	2019	2020	2021
Revenue actually received (+)	16,740,086	21,801,460	23,058,211
Payments made (-)	-11,980,352	-15,050,421	-17,989,374
Carry-over of appropriations (-)	-4,357,734	-6,200,614	-5,082,548
Cancellation of appropriations carried over (+)	62,522	180,023	209,385
Adjustment for carry-over of assigned revenue appropriations carried over (+)	116,393	10,403	125,622
Exchange rate difference (+/-)	-1,802	-1,291	-428
<b>TOTAL</b>	<b>579,113</b>	<b>739,560</b>	<b>320,868</b>

## CANCELLATION OF APPROPRIATIONS

In 2021, out of an EU budget contribution to ENISA's budget of 22,833,000 EUR (C1 funds), 22,721,000 EUR were committed, representing a budget execution rate of 99,51%, and a total of 112,000 EUR representing 0,49% of the budget was not used. A total of 17,672,000 EUR representing 77.4% of the 2021 budget was paid in 2021 and a total of 5,049,000 EUR representing 22.11% of the 2021 budget were carried forward to 2022.



## ANNEX 4

HUMAN RESOURCES –  
QUANTITATIVE

Overview of all categories of staff and staff evolution

Staff policy plan for 2023–2025

**Table 9. Staff population and its evolution; overview of all categories of staff**

● Statutory staff and SNE

Staff	2021			2022	2023	2024	2025
<b>Establishment Plan Posts</b>	Authorised Budget	Actually filled as of 31/12/2021	Occupancy rate %	Adopted	Envisaged staff	Envisaged staff	Envisaged staff
<b>Administrators (AD)</b>	57	52	91%	63	63	63	63
<b>Assistants (AST)</b>	19	17	89%	19	19	19	19
<b>Assistants/Secretaries (AST/SC)</b>							
<b>Total Establishment Plan Posts</b>	76	69	91%	82	82	82	82
<b>External Staff</b>	FTE corresponding to the authorised budget 2021	Executed FTE as of 31/12/2021	Execution Rate %	Adopted FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	30	27	90%	32	32	32	32
Seconded National Experts (SNE)	12	10	83%	12	14	16 <sup>1**</sup>	18 <sup>**</sup>
TOTAL External Staff	42	37	88%	44	46	48	50
<b>TOTAL STAFF<sup>2</sup></b>	<b>118</b>	<b>106</b>	<b>90%</b>	<b>126</b>	<b>128</b>	<b>130</b>	<b>132</b>

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

<sup>1\*\*</sup> In its budget proposal for the Single Programming Document (SPD) 2023-2025, the Agency asks for an extra 4 SNE posts introduced gradually (2+2 over 2 years) from 2024.

<sup>2</sup> Refers to TAs, CAs and SNEs figures.

**Table 10. Additional external staff expected to be financed from grant, contribution or service-level agreements**

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

**Table 11. Other human resources**

- Structural service providers

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

**Table 12.**

- Interim workers

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

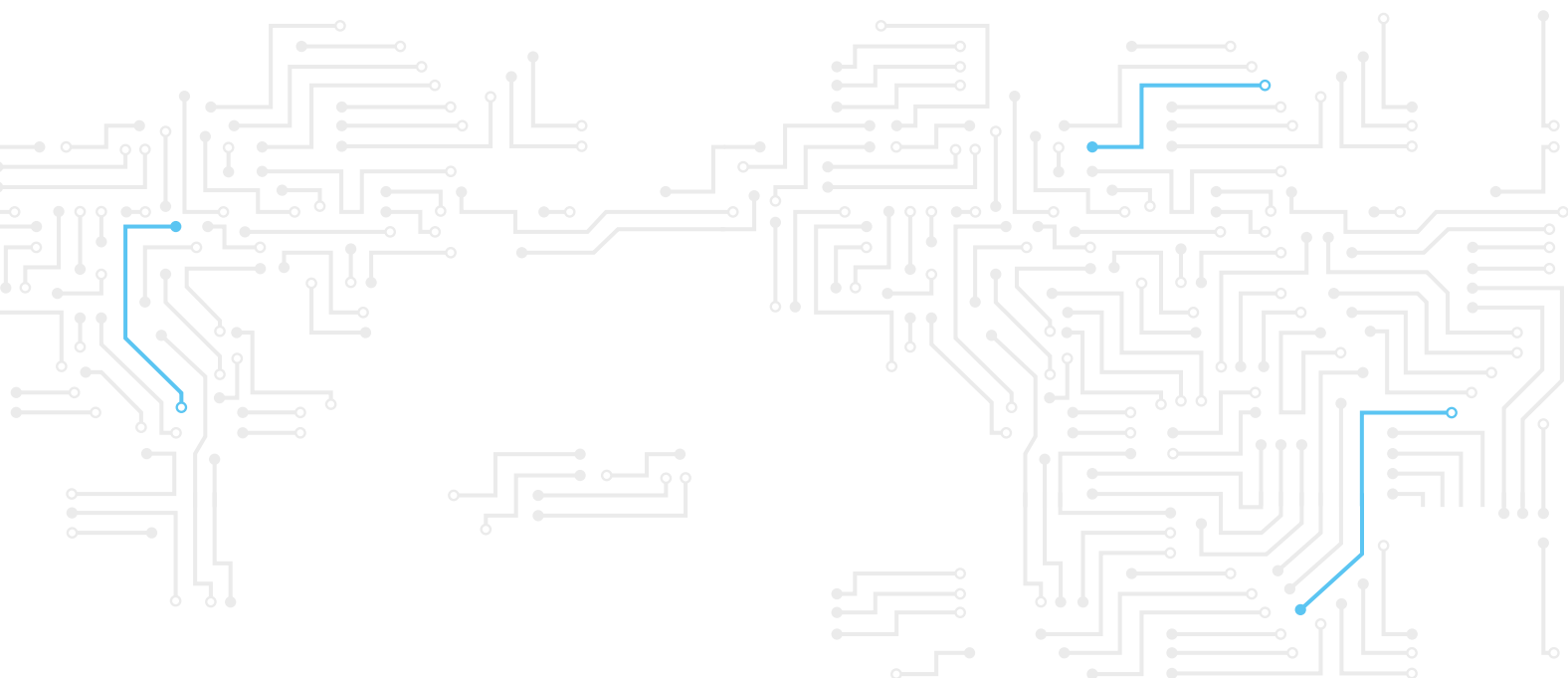


Table 13. Multiannual staff policy plan for 2021–2025<sup>3</sup>

Function group and grade	2021				2022		2023		2024		2025	
	Authorised budget		Actually filled as of 31 December 2021		Authorised		Envisaged		Envisaged		Envisaged	
	PP	TP	PP	TP	PP	TP	PP	TP	PP	TP	PP	TP
AD 16												
AD 15		1				1		1		1		1
AD 14				1								
AD 13		1		1		2		2		2		2
AD 12		5		5		4		4		4		4
AD 11		2				2		2		3		4
AD 10		3		3		4		4		4		3
AD 9		12		9		11		11		14		15
AD 8		21		9		22		25		23		24
AD 7		8		12		8		10		9		8
AD 6		4		12		9		4		3		2
AD 5												
AD TOTAL		57		52		63		63		63		63
AST 11												
AST 10												
AST 9												
AST 8		1		1		2		2		3		4
AST 7		4		3		3		4		4		4
AST 6		8		2		8		7		7		7
AST 5		5		4		5		5		5		4
AST 4		1		4		1		1		0		0
AST 3				2								
AST 2				1								
AST 1												
AST TOTAL		19		17		19		19		19		19
AST/SC 6												
AST/SC 5												
AST/SC 4												
AST/SC 3												
AST/SC 2												
AST/SC 1												
AST/SC TOTAL												
TOTAL		76		69		82		82		82		82
<b>GRAND TOTAL</b>		<b>76</b>		<b>69</b>		<b>82</b>		<b>82</b>		<b>82</b>		<b>82</b>

PP: Permanent Posts, TP: Temporary posts

<sup>3</sup> The change in the number in the establishment plan of up to 10% requested for the year 2022 is modified in accordance with Art 38 of the ENISA Financial Regulation. In 2022, ENISA will review its staffing strategy and will update a forecast for reclassification also in line with job mapping.

**Table 14. (b) External personnel**

● Contract agents

Contract agents	FTE corresponding to the authorised budget 2021	Executed FTE as of 31/12/2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025
Function Group IV	28	19	30	30	30	30
Function Group III	2	7	2	2	2	2
Function Group II	0	0	0	0	0	0
Function Group I	0	1	0	0	0	0
<b>TOTAL</b>	<b>30</b>	<b>27</b>	<b>32</b>	<b>32</b>	<b>32</b>	<b>32</b>

**Table 15.**

● Seconded national experts

SNEs	FTE corresponding to the authorised budget 2021	Executed FTE as of 31/12/2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025
<b>TOTAL</b>	<b>12</b>	<b>10</b>	<b>12</b>	<b>14</b>	<b>14<sup>4*</sup></b>	<b>14<sup>5*</sup></b>

**Table 16. Recruitment forecasts 2023 following retirement or mobility or new requested posts (indicative table)**

Job title in the agency	Type of contract (Official, ta or ca)		TA/Official Function group or grade of recruitment internal (Brackets) and external (single grade) foreseen for publication *		CA Recruitment Function Group (I, II, III and IV)
	Due to foreseen retirement/mobility	New post requested due to additional tasks	Internal (brackets)	External (brackets)	
Expert		n/a	n/a	n/a	n/a
Officer		n/a	n/a	n/a	n/a
Assistant		n/a	n/a	n/a	n/a

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

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

# ANNEX 5

## HUMAN RESOURCES – QUALITATIVE

### A. RECRUITMENT POLICY

**Table 17. Implementing rules in place**

		Yes	No	If no, what other rules of implementation are in place?
<b>Engagement of CA</b>	Model Decision C(2019)3016	x		
<b>Engagement of TA</b>	Model Decision C(2015)1509	x		
<b>Middle management</b>	Model decision C(2018)2542	x		
<b>Type of posts</b>	Model Decision C(2018)8800		x	C(2013)8979

### B. APPRAISAL AND RECLASSIFICATION/PROMOTIONS

**Table 18. Implementing rules in place**

		Yes	No
<b>Reclassification of TA</b>	Model Decision C(2015)9560	x	
<b>Reclassification of CA</b>	Model Decision C(2015)9561	x	

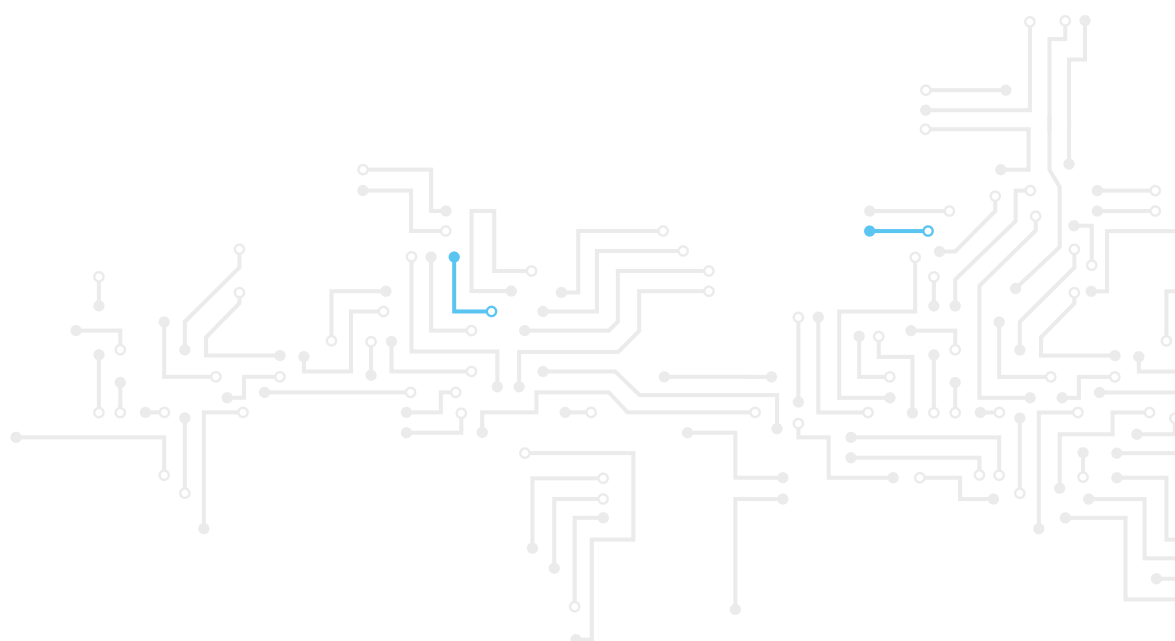
**Table 19. Reclassification of TA / promotion of officials**

Average seniority in the grade among reclassified staff								
Grades	2016	2017	2018	2019	2020	2021	Actual average over 5 years	Average over 5 years (according to decision C(2015)9563)
AD05	-	-	-	-	-	-	-	2.8
AD06	1	1	2	3	-	1	3.7	2.8
AD07	1	-	-	-	1	-	-	2.8
AD08	1	1	1	-	2	1	4.3	3
AD09	-	-	1	-	-	-	-	4
AD10	-	-	-	-	-	-	-	4
AD11	1	-	-	-	-	-	-	4
AD12	-	-	-	-	-	1	10	6.7
AD13	-	-	-	-	-	-	-	6.7
AST1	-	-	-	-	-	-	-	3
AST2	-	-	-	-	-	-	-	3
AST3	1	1	1	-	-	-	-	3
AST4	1	1	1	-	1	-	-	3
AST5	1	-	1	-	-	1	5.5	4
AST6	1	-	-	-	1	1	3.5	4
AST7	-	-	-	-	-	1	5	4
AST8	-	-	-	-	-	-	-	4
AST9	-	-	-	-	-	-	-	N/A
AST10 (Senior assistant)	-	-	-	-	-	-	-	5
There are no AST/SCs at ENISA: n/a								
AST/SC1								4
AST/SC2								5
AST/SC3								5.9
AST/SC4								6.7
AST/SC5								8.3



Table 20. Reclassification of contract staff

Function group	Grade	Staff active on 31.12.2021	How many staff members were reclassified in year 2021	Average number of years in grade of reclassified staff members	Average number of years in grade of reclassified staff members according to decision c(2015)9561
CA IV	17	1	-	-	Between 6 and 10 years
	16	0	-	-	Between 5 and 7 years
	15	2	-	-	Between 4 and 6 years
	14	15	5	3	Between 3 and 5 years
	13	1	-	-	Between 3 and 5 years
CA III	12	1	-	-	-
	11	0	-	-	Between 6 and 10 years
	10	5	1	3	Between 5 and 7 years
	9	1	-	-	Between 4 and 6 years
	8	0	0	-	Between 3 and 5 years
CA II	6	-	-	-	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
CA I	3	1	-	-	n/a
	2	-	-	-	Between 6 and 10 years
	1	-	-	-	Between 3 and 5 years



## C. GENDER REPRESENTATION

**Table 21. Data as of 31.12.2022 statutory staff (only temporary agents and contract agents on 31.12.2022)**

		Official		Temporary		Contract Agents		Grand Total	
		Staff	%	Staff	%	Staff	%	Staff	%
<b>Female</b>	Administrator level	-	-	18	26%	15	-	-	-
	Assistant level (AST & AST/SC)	-	-	11	16%	-	-	-	-
	Total	-	-	29	42%	15	56%	44	46%
<b>Male</b>	Administrator level	-	-	34	49%	12	-	-	-
	Assistant level (AST & AST/SC)	-	-	6	9%	-	-	-	-
	Total	-	-	40	58%	12	44%	52	54%
<b>Grand total</b>		-	-	69	100%	27	100%	96	100%

**Table 22. Data regarding gender evolution over 5 years of middle and senior management (31.12.2022)**

	2016		31.12.2021	
	Number	%	Number	%
<b>Female managers</b>	0	0	3 <sup>6</sup>	27%
<b>Male managers</b>	10	100	8 <sup>7</sup>	73%

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

<sup>6</sup> This category comprises Heads of Unit and Team Leaders.

<sup>7</sup> This category comprises Heads of Unit and Team Leaders.

## D. GEOGRAPHICAL BALANCE

Table 23. Data on 31.12.2022 – 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
BE	5	7%	2	8%	7	7%
BG	2	3%	-	-	2	2%
CY	1	1%	2	8%	3	3%
CZ	1	1%	-	-	1	1%
DE	2	3%	-	-	2	2%
Double <sup>8</sup>	4	6%	3	12%	7	7%
EE	1	1%	-	-	1	1%
ES	3	4%	1	4%	4	4%
FR	3	4%	1	4%	4	4%
GR	26	37%	12	48%	38	40%
IT	5	7%	-	-	5	5%
LT	-	-	1	4%	1	1%
LV	2	3%	-	-	2	2%
NL	2	3%	-	-	2	2%
PL	3	4%	1	4%	4	4%
PT	3	4%	1	4%	4	4%
RO	7	10%	0	0%	7	7%
SE	1	1%	-	-	1	1%
SK	-	-	1	4%	1	1%
<b>TOTAL</b>	<b>71</b>	<b>100%</b>	<b>25</b>	<b>100%</b>	<b>96</b>	<b>100%</b>

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

**Table 24. Evolution over 5 years of the most represented nationality in the Agency**

Most represented nationality	2016		31.12.2022	
	Number	%	Number	%
Greek	27 (out of 68)	39.7	38 (out of 96)	39.6

Looking back to 2021, it has been noted that positive measures to improve the diversity of nationalities, which took in 2020 and 2021, have borne fruit. This can be attributed to the continuation of broad outreach campaigns on popular media across the European Union, closer consideration of the spread of nationalities in relation to the competencies requested, and specific provisions in the vacancy notices<sup>9</sup>.

## E. SCHOOLING

**Table 25.**

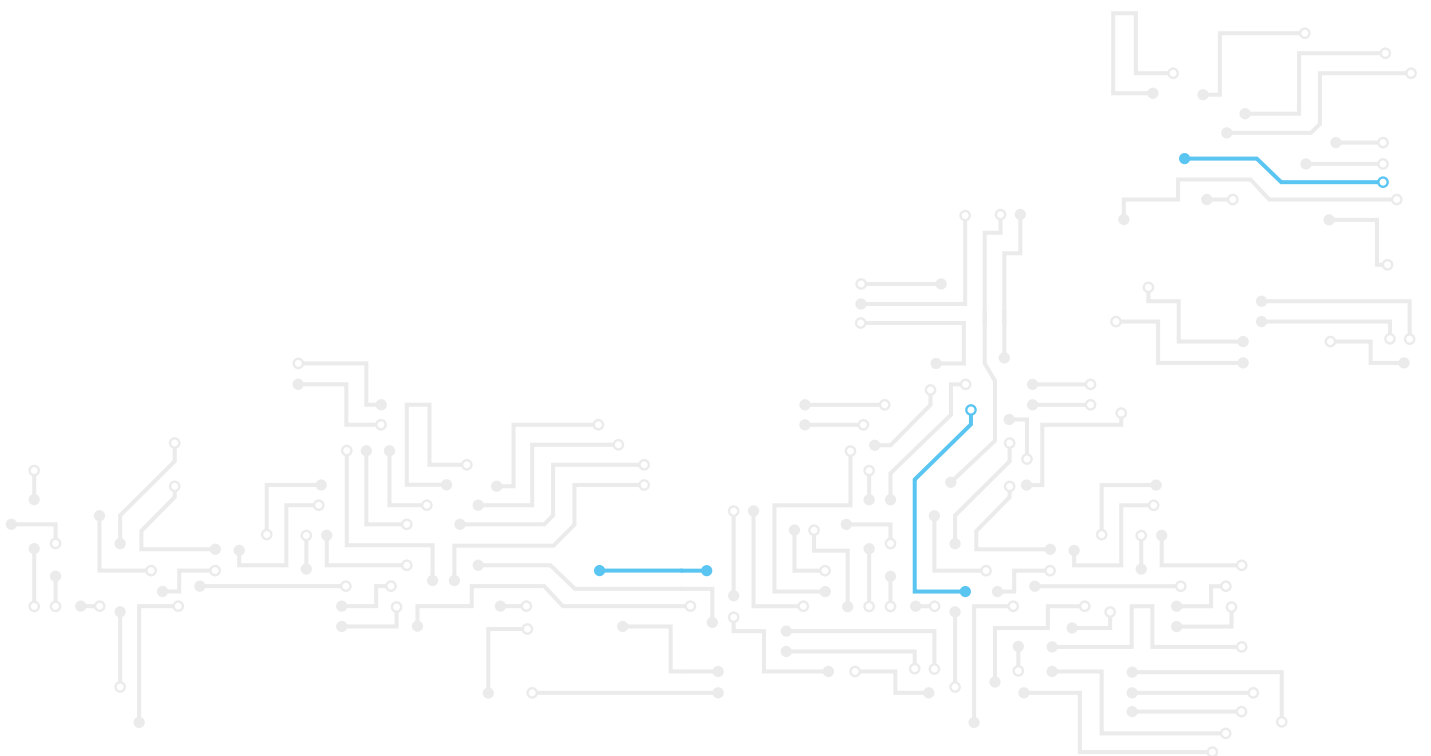
Agreement in place with the European School of Heraklion	
Contribution agreements signed with the EC on type I European schools	No
Contribution agreements signed with the EC on type II European schools	Yes
Number of service contracts in place with international schools:	Same as the previous school year, for school year 2022-2023, the process for the financial support for the staff of ENISA in relation to the cost of schooling has been updated via EDD 2021-41, leading to the abolishment of SLAs and remains unchanged.

<sup>9</sup> The seeming imbalance related to the most represented nationality at ENISA is related to several factors, such as, for example, the level of posts and related salaries which may be perceived as less appealing for job seekers in relatively more advanced member state economies, the fact that ENISA offers better prospects as an employer compared to the average conditions available in the Greek job market, the small job market in Greece for cybersecurity professionals, and historic decisions taken by previous AIPNs. Another reason that may be cited is the need for stability during the start up phase of the Agency as staff from the hosting member state (Greece) is less prone to resign (resulting in reduced turnover) which, in combination with the relatively young age of the Agency compared to others, still has its original impact, the relatively better academic profile of Greek candidates for lower level posts; the relatively smaller payroll cost for staff that is relatively better qualified than the average and costing less if expatriation allowance is considered, as well as the general predisposition to accept a lower level position to remain in the home country.

# ANNEX 6

## ENVIRONMENT MANAGEMENT

ENISA is investigating opportunities to strengthen its environmental management and, as such, a new output was introduced in 2022 to carry out an overarching audit on the CO<sub>2</sub> impact of all the Agency's operations and develop and implement a targeted action plan. The objective of this undertaking is for the Agency to be climate neutral by 2030.



# ANNEX 7

## BUILDING POLICY

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

**Table 26. 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 (€)
		Office space (m <sup>2</sup> )	non-office (m <sup>2</sup> )	Total (m <sup>2</sup> )	Rent (euro per year)	Duration	Type		
<b>Heraklion Office</b>	Heraklion	706		706		01/01/2021 to 28/02/2030;	Lease	Rent is fully covered by Hellenic Authorities	N/A
<b>Athens Office</b>	Chalandri	4,498	2,617	7,115		01/01/2021 to 28/02/2030;	Lease	Rent is fully covered by Hellenic Authorities	N/A
<b>Brussels office</b>	Brussel centre	98		98	56,496	N/A	SLA with OIB		N/A
<b>Total</b>	Location	5,302	2,617	7,920					

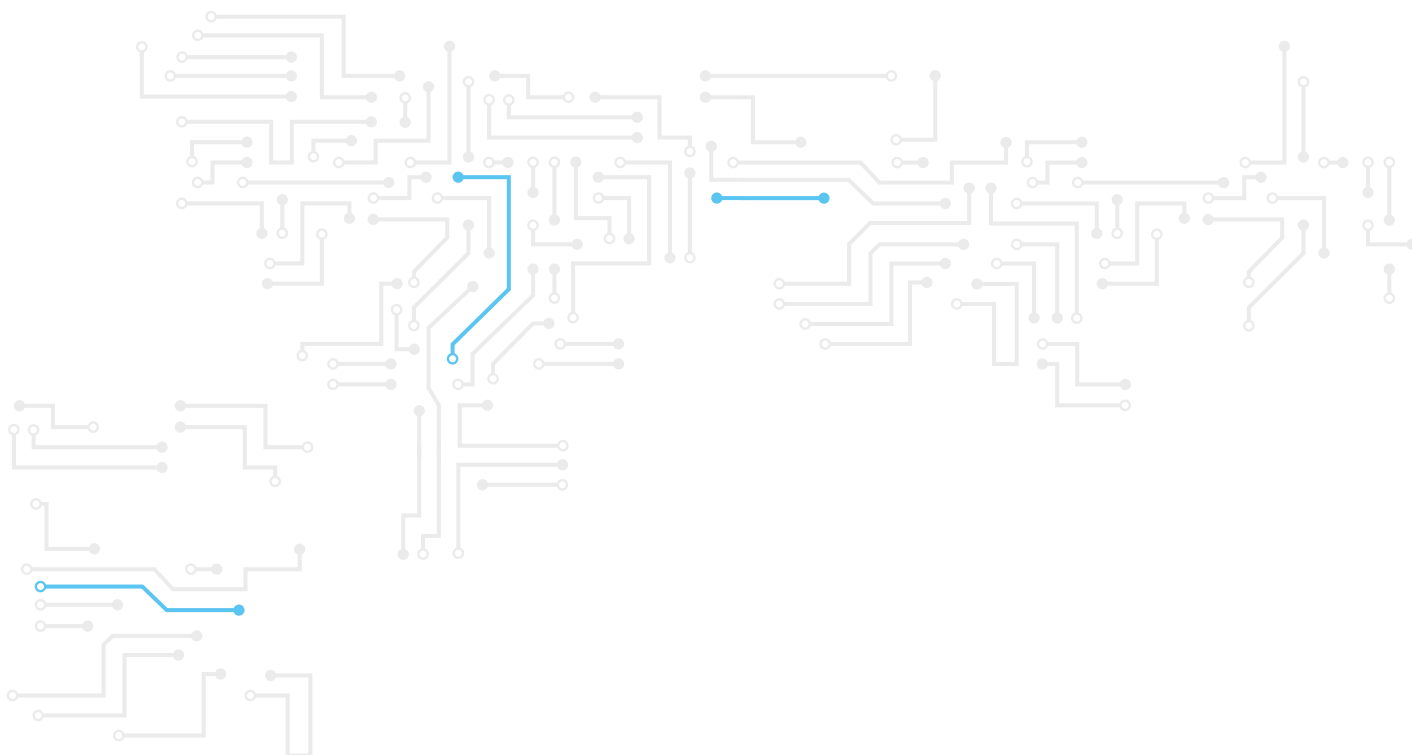
## BRUSSELS OFFICE

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

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

**Table 27.**

	2023	2024	2025
Head count (FTEs)	4-10	4-10	4-10
Budget (one-off & maintenance costs)	170,000	170,000	170,000



# ANNEX 8

## PRIVILEGES AND IMMUNITIES

**Table 28.**

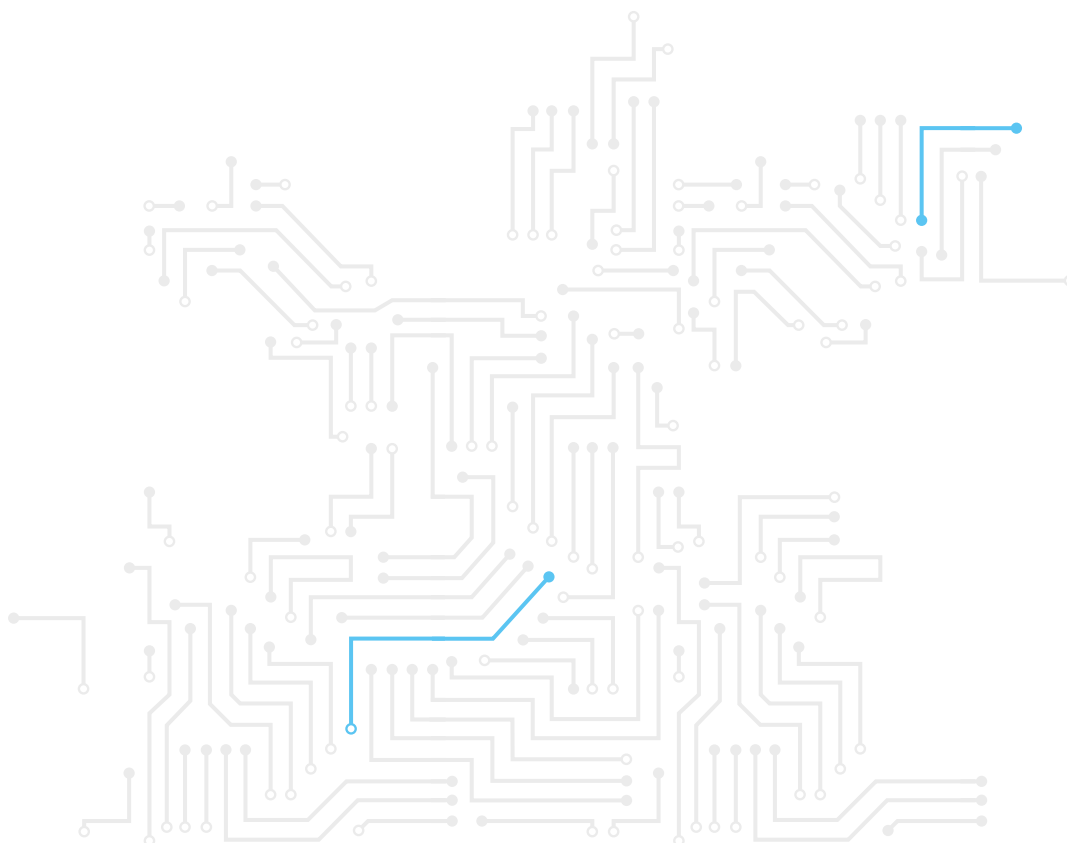
Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education / day care
<p>In accordance with Art. 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, Protocol No 7 on the privileges and immunities of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

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



# ANNEX 10

## STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

As adopted by the Management Board<sup>10</sup>, the Agency's strategy for effective internal control is based on international practices (COSO Framework's international Standards), as well as the relevant internal control framework of the European Commission.

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

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

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

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

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

---

<sup>10</sup> <https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202019-12%20on%20internal%20controls%20framework.pdf>

The Common Approach on EU Decentralised Agencies foresees that EU agencies should be more active concerning fraud prevention and that the related communication forms an essential part of its success. In 2021 ENISA adopted an anti-fraud strategy<sup>11</sup> as recommended by the European Anti-Fraud Office (OLAF).

Following relevant guidance and best practices developed within the EU Agencies network, in 2022 ENISA initiated a thorough review of its internal control framework and overall strategy. The review aims to consolidate input from different sources and integrate the results of various risk assessments within a single internal control assessment process. The revised ENISA's internal control framework will be put in place in 2023, together with a comprehensive methodology for the assessment of enterprise risk across the Agency,

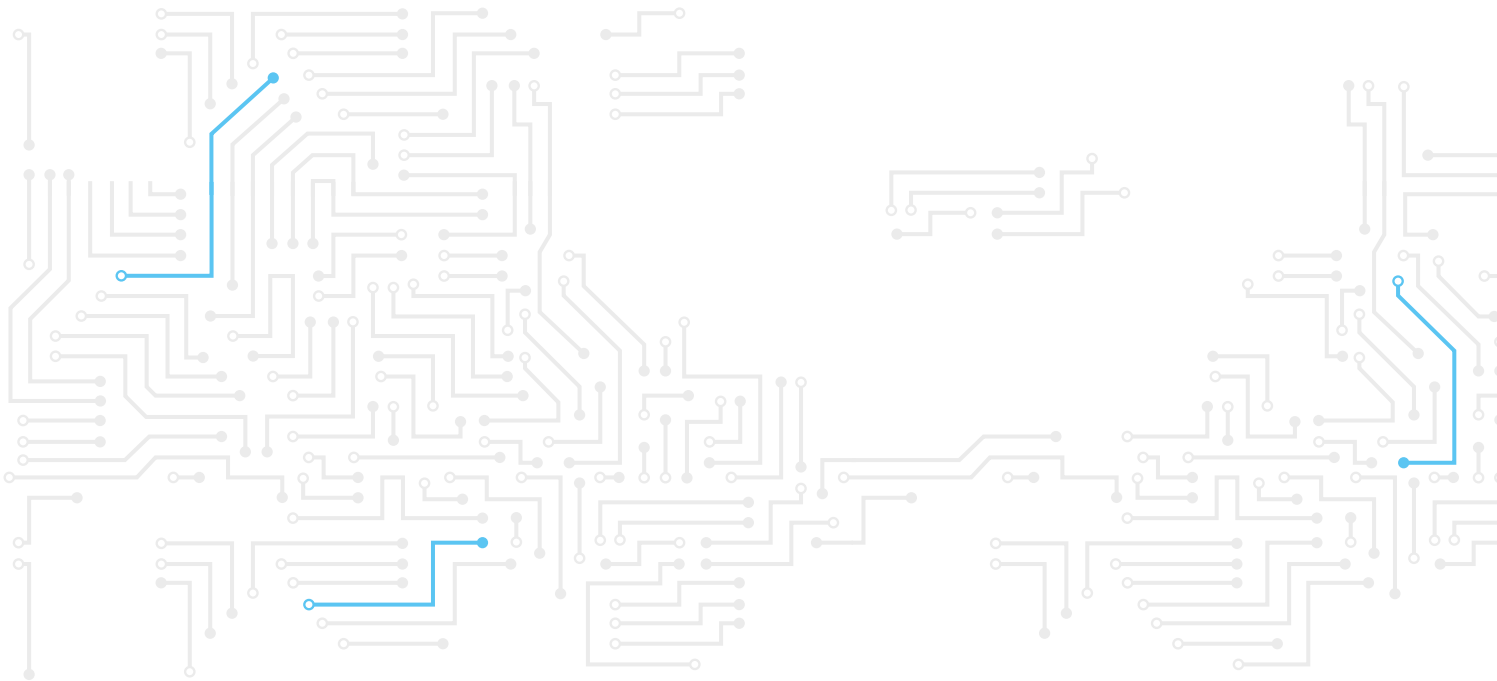
---

<sup>11</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, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS

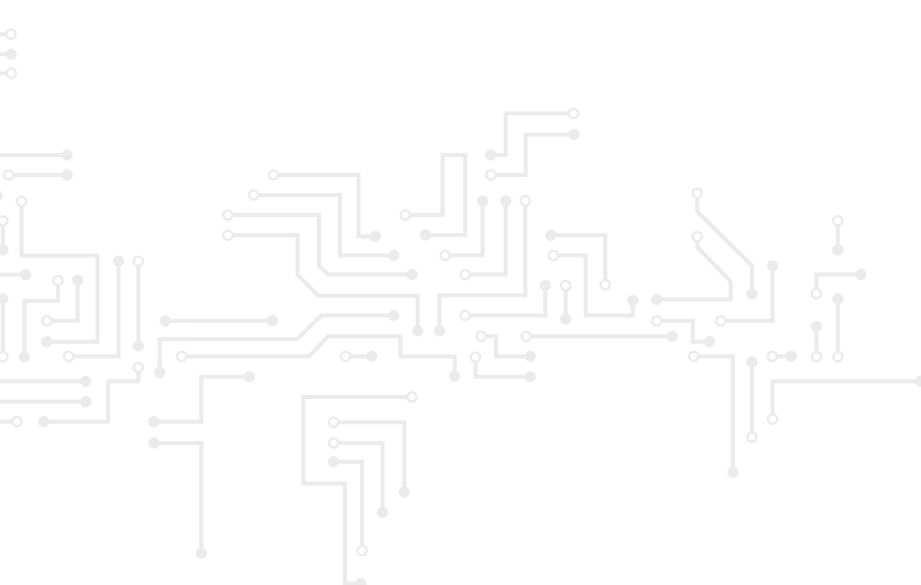
ENISA does not receive any form of grant, contributions or service level agreements that generate additional revenue.



## ANNEX 12

# STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

The international strategy foresees a continuation of the strong focus on the EU and EU actors, while also allowing increased flexibility to engage with international partners in line with the strategic objectives outlined in the ENISA Strategy for a Trusted and Cyber Secure Europe of July 2020. The Agency's international strategy <sup>12</sup> was adopted by the MB during its November 2021 meeting and the actions for international strategy are addressed under output 9.3 in activity 9.



---

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

# ANNEX 13

## ANNUAL COOPERATION PLAN 2023

This document is the provisional draft of 2023 Annual Cooperation Plan (ACP2023) between ENISA, the EU Agency for Cybersecurity, and CERT-EU, the CERT of the EU institutions, bodies and agencies, as foreseen in the co-signed Memorandum of Understanding. The ACP is expected to be endorsed by the CERT EU steering board during the course of 2023 Q1.

The plan aims to cover the cooperation activities planned for 2023.

The plan proposed in this document includes references to the activities included in the ENISA Work Program 2023 which is submitted to the Management Board for approval (MB).

Similarly, and in continuation of ACP2022, the proposed plan identifies actions on the following areas:

1. Capacity building as referred to in Articles 6.c and 6.i of the Cyber Security Act (CSA)
2. Operational cooperation as referred to in Article 7 of the CSA
3. The area of long-term strategic analyses of cyber threats as foreseen in Article 9.b of the CSA.

### CAPACITY BUILDING

Capacity building<sup>13</sup> covers assistance to relevant public bodies to improve capabilities to respond to cyber threats and incidents, including the provision of cybersecurity trainings and exercises.

Focus points of capacity building for the structured cooperation plan for 2023 remain Maturity, Training and Exercises. In particular, and following the findings from the European Court of Auditors in the Special Report 05/2022<sup>14</sup>, ENISA and CERT-EU plan to increase cooperation on training and exercise with the aim to increase the level of preparedness and response of EUIBAs.

### Maturity

Maturity assessments are useful means to identify current abilities and also existing gaps that require reinforcement of an organisation's capabilities and guide its efforts to improve its overall cybersecurity posture by achieving higher maturity levels over time.

In 2022, drawing on ENISA, CERT-EU's and other CSIRTs Network and EUIBA stakeholders' experience and expertise, ENISA has performed maturity-related development targeting the EUIBAs actors of the Blueprint<sup>15</sup> to assess their EU-level crisis management capabilities. This work resulted in a new maturity framework to perform a maturity assessment for EUIBAs.

13 As referred to in Articles 6.c and 6.i of the CSA.

14 <https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60922>

15 Commission Recommendation (EU) 2017/1584 (Blueprint).

Objective	Task	Deliverable	Lead	Work Program 2023
1. EUIBAs Cyber Hygiene	ICDT Task Force 1 - Measures for a high common level of cybersecurity (former common binding rules in ACP2021)	Proposal for a cybersecurity Regulation.	CERT-EU and the European Commission's DIGIT.S	Finalised
	Develop a cybersecurity maturity assessment methodology for all EUIBAs	Cybersecurity maturity assessment methodology.	CERT-EU	Service: Identify
2. CSIRTs Maturity	Maturity assessment methodology for crisis management for the Blueprint stakeholders	Applying new maturity framework developed and tested in 2022 into EUIBAs operational context	ENISA	Activity 4: Enabling operational cooperation Output 4.1

In 2023, following the European Commission's proposal for Regulation on measures for a common high level of cybersecurity it is expected for EUIBAs to start its adoption. This will initiate a CERT-EU led project in which a maturity assessment methodology will be developed for the EUIBAs.

The plan for 2023 will focus on continuing existing initiatives, in particular:

- **EUIBAs Cyber Hygiene:** CERT-EU will carry on the activities of finalising the proposal for a cybersecurity Regulation<sup>16</sup>, in close cooperation with the European Commission's DIGIT.S directorate, and develop a cybersecurity maturity assessment methodology for all EUIBAs.
- **CSIRTs Maturity:** ENISA will promote the new maturity framework among EUIBAs to implement ENISA Maturity Framework for their EU cyber crisis management capabilities. ENISA will foster the application of the maturity framework to relevant subjects to help identify current abilities and gaps.

CERT-EU and ENISA will maintain close contacts throughout the process to ensure their maturity-related activities feed each other in the most efficient way, avoiding duplication and misalignment.

## Training & Exercises

CERT-EU and ENISA have been successfully cooperating on training and exercises for many years. In particular, 2022 saw the execution of ENISA's flagship exercise, Cyber Europe 2022, where CERT-EU and ENISA cooperated on its setup and exercise roll-out.

This close cooperation will continue in 2023 by combining CERT-EU's and ENISA's strengths to lay the basis for developing a relevant, cost-efficient training portfolio that supports cybersecurity capacity building but also operational cooperation. The ambition of the cooperation is for ENISA to be able to provide state-of-the-art training portfolio that will be offered both to MSs and EUIBAs and to keep it up to date and relevant through its close collaboration with CERT-EU and its other key stakeholders.

Working methods already established in 2022 will continue throughout 2023 (e.g. CERT-EU collaborating with ENISA in the CSIRTs Network Working Group on Trainings and other similar fora).

The focus of 2023 will be to keep sustaining yearly ongoing activities (i.e. cyber exercise regularly organised by ENISA or in collaboration with ENISA) as well as finalising activities started in 2022. In the context of providing a common strong portfolio to a wider target audience, ENISA will work with CERT-EU in order to provide access to a self-paced online learning platform that provides a variety of high-quality training tracks adapted to specific target audiences.

In particular:

- **Custom Technical Courses:** building on the activity in 2022, ENISA will work with CERT-EU and the CSIRTs Network Training WG to enhance training programs based on audience knowledge level (e.g. elementary vs. advanced).
- **Self-paced online learning platform:** based on the experience gained via pilots, ENISA will offer the platform also to EUIBAs and will leverage the special relationship CERT-EU has with their

<sup>16</sup> The proposal has been finalised and the European Commission published it on 22 March 2022. See [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_1866](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1866) for more information.

Objective	Task	Deliverable	Lead	Work Program 2023
1. Training	Custom technical courses	Continuous enhancement of training program with elementary and advanced courses.	ENISA	Activity 3 Building capacity Output 3.3
	Self-paced online platform	Providing access to constituency members and providing suggested tracks to complete.	ENISA	Activity 3 Building capacity Output 3.3
	Technical workshops organised for constituents. Provide technical experience based on handled incidents.	Continuous enhancement of the technical workshops with specialised training.	CERT-EU	Service: Identify
2. Exercises	ENISA exercises	Conduct cyber exercises with varied Objectives and matching execution type.	ENISA	Activity 3 Building capacity Output 3.2
	Joint Awareness & Preparedness Cyber Security Exercise: JASPER	Perform joint exercise. Incorporate lesson learned from '22 pilot execution and working practice..	ENISA	Activity 3 Building capacity Output 3.2

constituency to offer to Agency staff suggested ideal tracks of modules. Furthermore the option to have custom trainings developed on demand will be explored.

- Technical, Specialised Workshops for CERT-EU constituents:** CERT-EU will further develop technical, specialised workshops, leveraging, where relevant, the experience and working practice of ENISA.
- Regular ENISA Cyber Security Exercises:** this is an ongoing activity led by ENISA, which materialises in several types of exercises involving different stakeholders. Through the structured cooperation, CERT-EU will be involved not only as participant in relevant exercises but also as a valuable planner for selected exercises (e.g. Cyber Europe). In this context CERT-EU's familiarity with the EU Agencies and their expertise with actual and relevant threats is very valuable.
- Joint Cyber Security Exercise:** When relevant and in reference to the structured operational cooperation, both parties will join efforts to participate in exercises under the capacity of planners and training audience. In addition, common operational activities, e.g. Joint Rapid Reports, will be evaluated through these occasions. ENISA will be collaborating closely with CERT-EU in order to find the most relevant

topics for these exercises (based on real threats and attacks observed by CERT-EU), using the long experience on running complex exercises with various stakeholders at the highest standards. In 2023 the lessons learned from the pilot execution in 2022 will be applied and this will result in an improved experience.

## OPERATIONAL COOPERATION

### Cyber Crisis Management Coordination and Common Situational Awareness

2022 has been a special year for Operational Cooperation pillars within the ENISA and CERT-EU Structured Cooperation (SC). Building on the SC, the two organisations teamed up to provide a continuous situational picture of cyber threats, related to the UA-RU conflict. In order to respond more effectively and share a common situation picture, ENISA and CERT-EU take part in a special task force (Interinstitutional Task Force) organised by the European Commission and European External Action Service.

In addition, 2022 saw the launch of the Joint Cyber Assessment Report (EU JCAR)<sup>17</sup> as well the establishment of the Joint Rapid Report (JRR) services.

<sup>17</sup> EU-JCAR implements a legal obligation under Article 7(6) of Regulation (EU) 2019/881 (Cybersecurity Act) and it has been drafted by European Union Agency for Cybersecurity (ENISA), the Computer Emergency Response Team for the EU institutions and bodies (CERT-EU) and the European Cybercrime Centre (EC3) with contribution from European Commission DG CONNECT Cyber Coordination Task Force as well as of the European External Action Service.



Objective	Task	Deliverable	Lead	Work Program 2023
1. SOP	Adopt EUIBAs SOP	Finalize EUIBAs SOP for Inter-institutional Task Force.	ENISA	Activity 4: Enabling operational cooperation Output 4.1
	Test SOP in a simulated scenario through exercise	Exercise read-out and EUIBA SOP lessons learned		
	Review the Security Incident Response (SIR) process.	SOP document	CERT-EU	Service: Respond
2. Common Situational Awareness	Operationalised, Common Situational Awareness	Continue and improve Joint Rapid Report service  Establish Joint Cyber Assessment Report service  Maintenance and enhancement of established information exchange mechanism and communication channels	ENISA	Activity 5: Contribute to cooperative response at Union and Member States level Output 5.1

As part of the efforts of further development of the procedures for EU and EUIBAs Cyber Crisis Management coordination, ENISA and CERT-EU will further align actions on developing Standard Operating Procedures (SOP) with particular focus on procedures to be adopted within the Interinstitutional Task Force and further build-on and improving Common Situational Awareness.

The target for 2023 is to further expand on the cooperation activities started with the ACP2022. In particular

- EUIBAs SOP for the Cyber Crisis Management stakeholders:** ENISA and CERT-EU will focus on finalising the EUIBAs SOP document and seek adoption within the Inter-institutional Task Force. EUIBAs SOP to be tested through exercise and in synergies with EU Cyber Crisis Management exercises.
- Security Incident Response – Continuous Improvement:** CERT-EU will leverage the aforementioned work in SOPs, lessons learnt in significant incidents and the proceedings on the information exchange domain with ENISA and the other Blueprint stakeholders to review and update its Technical SOPs – Security Incident Response (SIR) process.

- Common situational awareness:** With the 2022 activities both organisations have worked towards the establishment of a mechanism for information exchange at EU level, as well set the stage for joint reports to raise awareness on significant cyber security events<sup>18</sup>. Within the 2023 activity ENISA and CERT-EU will further operationalize the mechanism, seeking additional opportunity for joint reports and assessments, as well using exercises to enhance the production of situational awareness deliverables.

The Joint Rapid Report (JRR) service will be continue and further improved. EU-JCAR service is planned to be operational in 2023.

## MUTUAL ASSISTANCE

As stated in Article 7 of the Cybersecurity act, ENISA shall assist, at the request of one or more Member States, in assessing incidents having a significant or substantial impact within the meaning of Directive (EU) 2016/1148 through the provision of expertise, in facilitating the technical handling of such incidents and in providing support in relation to ex-post technical inquiries regarding such incidents.

In 2022 ENISA has further refined the mechanism and delivered its first assistance to a requiring party<sup>19</sup>. Additionally, EC's DG CONNECT has

<sup>18</sup> Cyber security events or incidents significantly affecting or potentially significantly affecting EU Member States, critical sectors within the meaning of the NISD or ICT technologies, services, platforms or ICT infrastructures widely applied and used across the internal market.

<sup>19</sup> Delivery of services is expected in December 2022.

Objective	Task	Deliverable	Lead	Work Program 2022
1. EU MS	Operationalization of the cyber security assistance mechanism	<p>Optimization of the mechanism as possible part of the Cyber Security Support Action Program</p> <p>Pilot the use of EUMSs and/or EUIBAs personnel as part of service fulfilment</p> <p>Execution of scenarios to test SOPs of the mechanism.</p> <p>Management of pool of experts.</p>	ENISA	Activity 5 Contribute to cooperative response at Union and Member States level Output 5.2
2. EUIBA	Operational capability to assist EUIBAs	Management a pool of EUIBA experts.	CERT-EU	Service: Respond

requested ENISA<sup>20,21</sup> to scale up its assistance mechanism to Member States and provided ENISA with additional means to support preparedness (ex-ante), and response (ex-post) to large-scale cybersecurity incidents.

The 2023 proposed plan aligns and build-on the work done in 2022, and focuses on further enhancing and operationalizing the cyber security assistance mechanism. In particular:

- **Cyber Security Assistance Mechanism:** ENISA will build-on the mechanism to deliver on the Cyber Security Support Action program. Due to this, the focus on the assistance mechanism will be primarily set on expanding it and pilot the use of EU and EUIBAs resources as service fulfilment.
- **Operational capability to assist EUIBAs:** CERT-EU will continue managing the pool of EUIBA experts and further enhance its operational capability.

## KNOWLEDGE AND INFORMATION SHARING

Knowledge and information are a horizontal activity that nurtures and sustains the previous two pillars as well as getting input from these.

As outlined in Article 9.b of the CSA, ENISA performs long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents. One of the activities in this field is the ENISA Threat Landscape (ETL) which provides an overview of threats, together with current and emerging trends. It is based on publicly available or voluntarily shared information data and provides an independent view on observed threats, threat agents and threat trends. CERT-EU is an important and structural contributor to the ETL and related activities and will remain so through 2023.

ENISA is leading long-term strategic analyses also through maintaining and collaborating with a working group of experts on foresight for emerging and future cybersecurity challenges and cyber threat landscape<sup>22</sup>.

In 2023 CERT-EU, through the inclusion as an observer in these ENISA working groups, will contribute, review and validate the findings and generally enhance the outputs created from those groups. Those activities refer to Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities of ENISA Work Program 2023.

The long-term strategic analyses will feed into the capacity building and operational activities outlined in the previous sections.

20 Letter of intent between DG CONNECT and ENISA on the provision of support to Member States to further mitigate the risks of large scale cybersecurity incidents in the short term - Ares(2022)5946722

21 Cybersecurity Support Action program.

22 ENISA Ad-Hoc Working Group on Foresight on Emerging and Future Cybersecurity Challenges and ENISA Ad-Hoc Working Group on Cyber Threat Landscapes.





## 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

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



Publications Office  
of the European Union



ISBN 978-92-9204-547-0