EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2022–2024

Including multiannual planning, 2022 work programme and multiannual staff planning

JANUARY 2022

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

Luxembourg: Publications Office of the European Union, 2022

Print	ISBN 978-92-9204-548-7	ISSN 2467-4397	doi: 10.2824/700553	TP-AH-22-001-EN-C
PDF	ISBN 978-92-9204-547-0	ISSN 2467-4176	doi: 10.2824/610337	TP-AH-22-001-EN-N

ENISA SINGLE PROGRAMMING DOCUMENT 2022–2024

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

ABBREVIATIONS

ABAC	accrual-based accounting
AD	administrator
AI	artificial intelligence
AST	assistant
BEREC	Body of European Regulators for Electronic Communications
CA	contract agent
Cedefop	European Centre for the Development of Vocational Training
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CSA	Cybersecurity Act
CSIRT	computer security incident response team
CyCLONe	Cyber Crisis Liaison Organisation Network
ECCG	European Cybersecurity Certification Group
EDA	European Defence Agency
EEAS	European External Action Service
EECC	European Electronic Communications Code
EFTA	European Free Trade Association
eID	electronic identification
eIDAS	electronic identification and trust services
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	full-time equivalent
ICT	information and communication technology
IPR	Intellectual property rights
ISAC	Information Sharing and Analysis Centre
IT	information technology
JCU	Joint Cyber Unit
MoU	memorandum of understanding
NATO	North Atlantic Treaty Organisation
NIS	network and information security
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
SC	secretary
SCCG	Stakeholder Cybersecurity Certification Group
SLA	service-level agreement
SME	small and medium-sized enterprise
SNE	seconded national expert
SOC	security operations centre
SOP	standard operating procedure
SPD	single programming document
TA	temporary agent

FOREWORD

Europe's digital decade has started with a wide range of important, ambitious and pioneering EU policy initiatives that will already have changed the digital landscape by the time we implement this 2022–2024 European Union Agency for Cybersecurity (ENISA) single programming document.

A great many of these initiatives either directly or indirectly integrate cybersecurity concerns, challenges and solutions, and they were introduced in December 2020 in the EU's new cybersecurity strategy. ENISA is ready and indeed very proud to contribute to making these initiatives and their implementation a success, whether by promoting the uptake of the EU's first cybersecurity certification schemes, revising the network and information security (NIS) directive and the electronic identification and trust services (eIDAS) regulation, supporting the full implementation of the EU's 5G Cybersecurity Toolbox or fulfilling its roles in the European Cybersecurity Competence Centre, the Network of National Coordination Centres and the new Joint Cyber Unit. ENISA will use its new mandate, the expanded tasks and the fresh resources given to it by the 2019 Cybersecurity Act to make sure that it remains a key and reliable player and partner within the EU's cybersecurity ecosystem, able to tackle the ever-moving target of cybersecurity. Furthermore, it will make sure that the need for future resources is understood and that resources remain tailored to the EU's cybersecurity prerogatives.

In the second year of my tenure, I have been inspired in my work by the motivation and drive of the EU cybersecurity community – from my ENISA colleagues in their daily work to the political leaders and the European stakeholder community across the EU and in the national institutions in their united vision and support. There is a real common determination and a 'let's do it' approach to making Europe more cybersecure. We will need to maintain that momentum to tackle the ever-growing sophistication of cyberattackers and cyber challenges. Only in this way will we be able to establish European technological autonomy in the area of cybersecurity.

I am particularly proud that we – the Agency's staff and Management Board together – have laid solid foundations to make ENISA more agile, more connected and more performance-orientated, and this is reflected in the new organisational structure of ENISA, operational since 1 January 2021, and in the way we work. This has been enshrined in the 2020 ENISA strategy A Trusted and Cyber Secure Europe. And the effects are showing: we are increasingly able to attract cybersecurity talent from all over the EU to help us make a difference. In addition, with the generous support of our Greek host authorities, we have moved to larger premises in Athens, and we are expanding our networks throughout the EU, specifically through the imminent opening of a local office in Brussels.

The full positive effects of these investments will be truly felt only once we have overcome the current pandemic, but I am convinced that we will come out of this stronger, more united and better prepared to embark on the European digital decade project.

Juhan Lepassaar
Executive Director

MISSION STATEMENT

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

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

STRATEGY

EMPOWERING COMMUNITIES

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

CYBERSECURITY POLICY

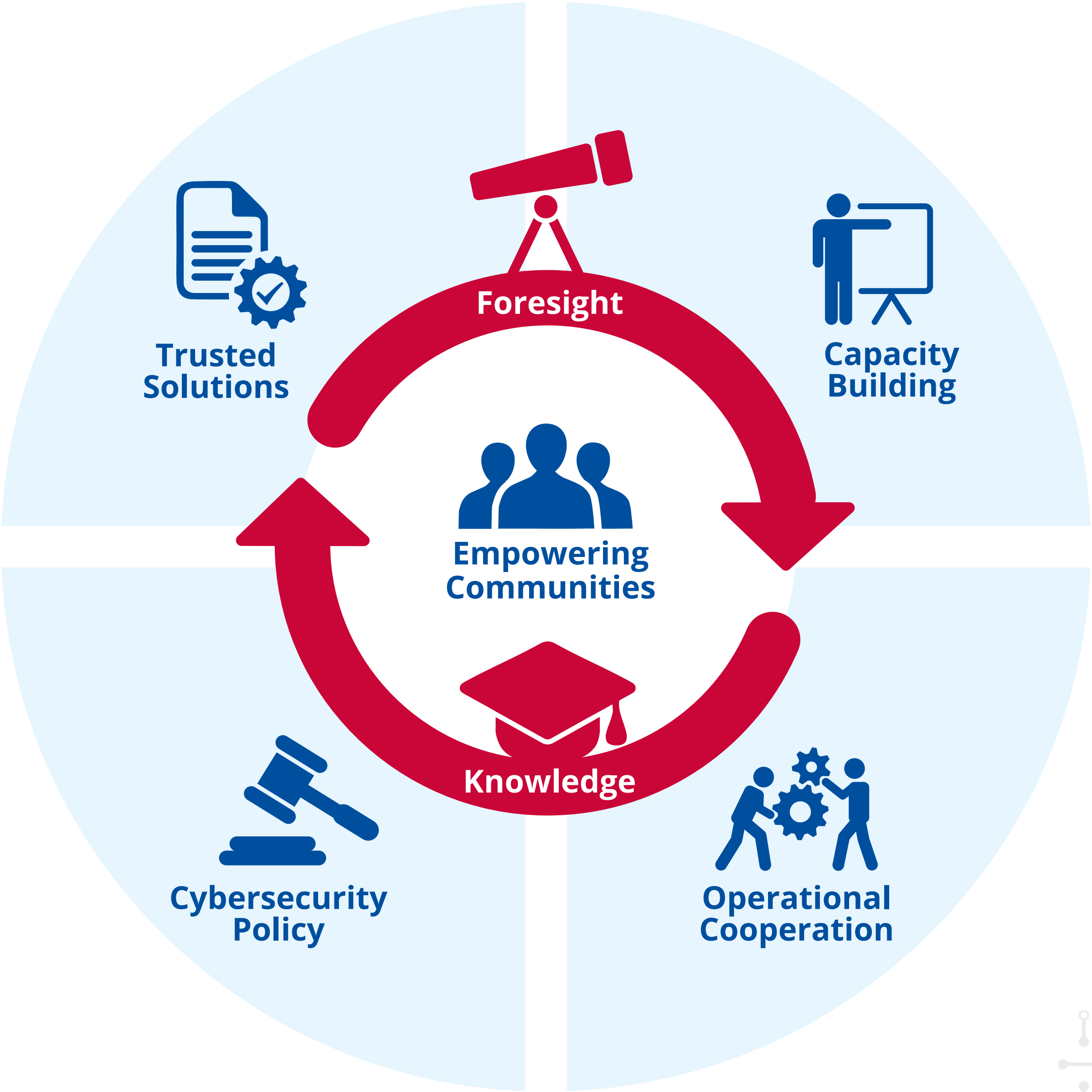
Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity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

OPERATIONAL COOPERATION

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

CAPACITY BUILDING

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



TRUSTED 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.

PART I
GENERAL CONTEXT

The year 2020 was characterised by the increased prioritisation of EU digital policies, through initiatives such as the Digital Services Act, the proposals for cybersecurity-specific revisions to the NIS directive, and many other digital initiatives, such as the European digital identity. The EU's ambition in this area were encapsulated in the phrase 'making 2020–2030 "Europe's Digital Decade"', used by Commission President Ursula von der Leyen in her State of the Union address[1] in September 2020. Where cybersecurity is concerned, these ambitions were made more concrete in the EU's cybersecurity strategy[2] for the digital decade, released in December 2020, and also in the context of ensuring the EU's technological autonomy. This prioritisation continued in 2021[3] and beyond.

ENISA welcomes the EU's new cybersecurity strategy. The strategy proposes, among many things, a review of the NIS directive, a new critical entities resilience directive, a network of security operations centres (SOCs), new measures to strengthen the EU Cyber Diplomacy Toolbox and the further implementation of the 5G Cybersecurity Toolbox. The Agency is ready to fully utilise its mandate and tasks to act in the areas outlined by the strategy that are covered by its mandate over the period of the 2022–2024 single programming document (SPD).

The COVID-19 pandemic has not only brought healthcare challenges; it has also had an impact on the process of digitalisation in Europe, worldwide and across sectors, increased technological complexities and exposed the need to boost technology skill sets. These effects in turn have accelerated exposure to a wide range of cybersecurity threats and threat actors, as documented by ENISA in 2021, on the one hand, and have increased the need for cybersecurity knowledge, awareness, resilience, cooperation and solutions on the other. This affects all aspects of ENISA's work and the cybersecurity ecosystem that the EU is building up.

ENISA's eighth edition of its annual threat landscape report[4] confirmed current and future trends of cyberattacks becoming ever-more sophisticated, targeted, widespread and undetected. Malware was again voted the EU's number one cyber threat in a poll of intelligence experts, and changes were observed in phishing, identity theft and ransomware that moved them to higher-ranking positions. Monetisation remains cybercriminals' top motivation, and the COVID-19 environment fuelled attacks

[1] https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[3] And has been fortified by the most recent State of the Union address (15 September 2021), which highlighted the concepts of cooperation, resilience and situational awareness (https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701).

[4] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

on homes, businesses, governments and critical infrastructure in 2020 and early 2021. Industries and governments alike continue to be hit by cyberespionage attacks. The number of data breach incidents continues to be very high, and the amount of stolen financial information and user credentials is growing. Unfortunately, we are getting used to hearing terms like 'Bad Rabbit ransomware', 'Winnti', 'Magecart' and 'watering hole attacks'. In December 2020, the European Medicines Agency was a victim of a cyberattack resulting in the leak of documents relating to the evaluation processes for COVID-19 vaccines. In the same month, another cyberattack on the software company SolarWinds through its supply chain resulted in a back-door infiltration into its commercial software application. The list has grown in 2021, with further supply chain attacks with global implications, such as the Kaseya and SITA attacks. The current escalation and the threat landscape status require the continual introduction of new methods and different approaches for Europe to become cybersecure.

The adoption and implementation of policy frameworks is one key area where the EU is making a difference. Indeed, the policies and initiatives that will be put in place in the coming years will determine how the EU faces the cybersecurity challenges of today and tomorrow. In this context, ENISA will determine and adapt the support that it provides, particularly in the following areas.

THE NIS2 DIRECTIVE AND THE JOINT CYBER UNIT

Improving cyber resilience, particularly for those who operate essential services such as healthcare and energy or for those who provide online marketplace services, has been the main focus of the current NIS directive since 2016. The proposed expansion of its scope, in the form of the new NIS2 directive, will see far more entities obliged to take measures to increase the level of cybersecurity in Europe.

A 2020 ENISA study on NIS investments[5] showed that, for organisations implementing the NIS directive, 'Unclear expectations' (35 %) and 'Limited support from the national authority' (22 %) were among the challenges faced. The NIS2 proposal addresses these areas, aiming to provide more clarity in terms of what is expected of national authorities, computer security incident response teams (CSIRTs), and essential and important entities in terms of reporting, crisis management and information sharing.

ENISA is already invested in the above areas, 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. This will also apply to increased cooperation under the potential Joint Cyber Unit (JCU) umbrella. ENISA will contribute to the implementation of the Commission's recommendation on 'building the Joint Cyber Unit', with a view to contributing to the establishment of an EU crisis management framework. This includes fostering cooperation among cybersecurity communities, among relevant EU institutions, bodies and agencies, and within (and between) civilian cooperation networks (i.e. the Cyber Crisis Liaison Organisation Network (CyCLONe), the CSIRTs Network and, to the extent needed, Cooperation Group).

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 with the support of area experts and in collaboration with public authorities in Member States. It is expected that the draft candidate cybersecurity certifications schemes proposed by ENISA will be adopted as Commission implementing regulations. A conformity assessment of digital products, services and processes in the digital single market will be enabled under the adopted schemes, therefore improving their cybersecurity. At the time of writing, ENISA has prepared a candidate scheme on common criteria (common criteria based European candidate cybersecurity certification scheme) and is advancing its work on cloud services (European cybersecurity certification scheme for cloud services) and 5G (EU5G).

Finalising the candidate schemes for the more specialised product categories under the common criteria and for cloud services is just the first step and should start bringing initial benefits in terms of EU-wide certification processes and higher consumer and user trust during 2022–2024.

RESEARCH AND INNOVATION

The EU is extending its support for and investments in the wealth of expertise and experience in cybersecurity research and technological and industrial development that exists in the EU by

[5] https://www.enisa.europa.eu/publications/nis-investments

prioritising cybersecurity in its research and innovation support efforts, and in particular through its Horizon Europe and Digital Europe programmes. It is also pooling resources and expertise by setting up the European Cybersecurity Competence Centre and the Network of National Coordination Centres[6]. ENISA is ready to contribute to this essential area in the coming years within the role given to it by the regulation establishing the European Cybersecurity Competence Centre and the Network of National Coordination Centres and by the mandate of the Cybersecurity Act (CSA). Some of this work is anticipated to take place in 2022–2024, and the particular tasks required will become clearer as the Cybersecurity Competence Centre becomes operational.

ARTIFICIAL INTELLIGENCE

With the EU's artificial intelligence (AI) agenda advancing rapidly following the European Commission proposal on AI[7] and 2021 coordinated plan on AI[8], the EU is addressing the major technological, ethical, legal and socioeconomic challenges that must be met 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 the availability, safety and resilience of future AI services and applications.

Building on ENISA's AI threat landscape report[9] of December 2020 and with the guidance of its Ad Hoc Expert Group on AI[10], the Agency can continue its open dialogue with EU institutions in support of the legislative initiatives reaching into 2022–2024. In this way, ENISA can continue to support the Commission and Member States by providing good security practices and guidelines.

THE EUROPEAN DIGITAL IDENTITY FRAMEWORK

The EU's eIDAS regulation provides a framework for interoperability of national electronic identification (eID) schemes and sets up an EU-wide market of electronic trust services. eID schemes 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 eIDAS regulation and identified several gaps. In June 2021, the Commission adopted a proposal for a revised legal framework establishing a European digital identity[11] that can be used by all EU citizens and by EU businesses when carrying out online transactions. In 2022–2024, ENISA will support Member States and the Commission in the implementation and development of the toolbox and the European digital identity framework as set out in the Commission's recommendation of 3 June 2021[12] in addition to promoting the exchange of good practices and capacity building of relevant stakeholders.

FURTHER DEVELOPMENTS

In 2020, ENISA put forward a proposal to open a local office in Brussels in accordance with Article 20(5) of the CSA. This will strengthen ENISA's position in the digital ecosystem of the EU and in particular its role in establishing synergies with EU institutions, bodies, offices and agencies in the field of operational cooperation at EU level. Moreover, the local office in Brussels will aim to ensure regular and systematic cooperation with EU institutions, bodies and agencies and other competent bodies involved in cybersecurity. Indeed, it will support the delivery of tasks mandated to ENISA under Article 7 of the CSA, in particular that of establishing and maintaining structured cooperation with the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU). A detailed and annual cooperation plan is being integrated into ENISA's SPD and is part of the memorandum of understanding (MoU) signed in early 2021. This will enable both organisations to benefit from synergies provided by proximity and daily contact and to avoid any duplication of activities.

[6] Regulation (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

[7] Proposal for Regulation (EU) 2021/206 of 21 April 2021 laying down harmonised rules on AI (Artificial Intelligence Act) and amending certain Union legislative acts.

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

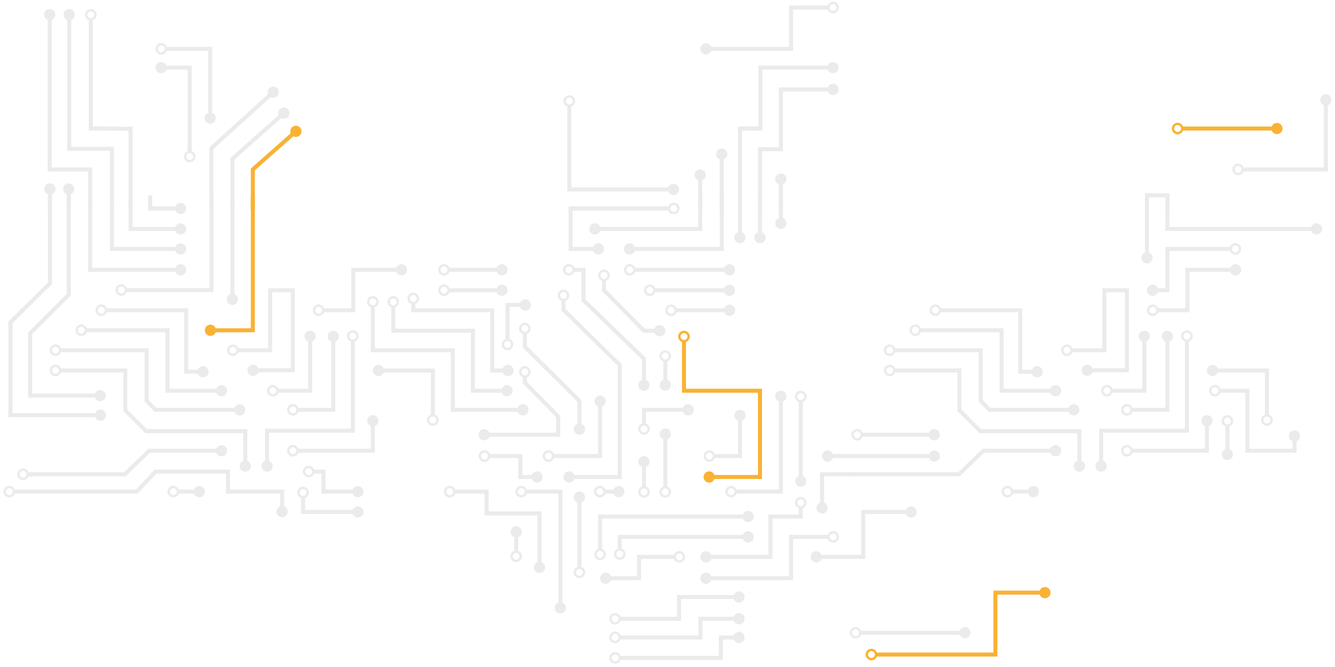
[9] https://www.enisa.europa.eu/news/enisa-news/enisa-ai-threat-landscape-report-unveils-major-cybersecurity-challenges

[10] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[12] Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common union toolbox for a coordinated approach towards a European digital identity framework.

In 2021, ENISA established a cooperation agreement[13] with the European Telecommunications Standards Institute (ETSI). ETSI and ENISA have the common objective of collaborating on, contributing to and promoting regional and international standardisation. There is mutual interest in avoiding any duplication of technical work, and in adopting an aligned and complementary approach to the standardisation process in specific domains.



[13] Signature pending.

II

PART II
MULTIANNUAL PROGRAMMING 2022–2024

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.

2.1. MULTIANNUAL WORK PROGRAMME

The following table maps the strategic objectives stemming from ENISA's strategy[14] against the relevant articles of the CSA. It furthermore integrates the activities of the work programme, showing how progress towards the achievement of the objectives is monitored. These objectives may be reviewed through the ENISA Management Board from 1 July 2024.

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

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	
1. Empowered and engaged communities across the cybersecurity ecosystem	Activities 1–9	Articles 5–12	Empowered ecosystem encompassing Member State authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, all of whom play their role in making Europe cybersecure	
2. Cybersecurity as an integral part of EU policies	Activities 1 and 2	Article 5	Cybersecurity aspects are considered and embedded across EU and national policies	
			• Consistent implementation of EU policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectoral specificities and needs • Wider adoption and implementation of good practices	
3. Effective cooperation amongst operational actors within the Union in case of massive[17] cyber incidents	Activities 4 and 5	Article 7	• All communities (EU institutions and Member States) use a rationalised and coherent set of standard operating procedures (SOPs) for cyber crisis management • Efficient framework, tools (secure and high availability) and methodologies for effective cyber crisis management	
			• Member States and institutions cooperating effectively during large-scale, cross-border incidents or crises • Public informed on a regular basis of important cybersecurity developments • Stakeholders aware of current cybersecurity situation	

[15] Baselines for these metrics should be known by the end of 2021. Therefore, targets linked to these baselines will be developed in 2022 for the 2023 work programme.

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

[17] Large scale and cross-border.

	Key performance indicator	Metrics[15]
	Community building across the cybersecurity ecosystem	Additional quantitative measures stemming from the stakeholder strategy that will be finalised in Q4 2021 Stakeholder satisfaction of ENISA's role as facilitator of community building and collaboration across the cybersecurity ecosystem
	ENISA's added value to EU institutions, bodies and Member States in providing support to policymaking (ex ante)	Number of relevant contributions to EU and national policies and legislative initiatives Number of references to ENISA reports, analysis and/or studies in EU and national policy documents Satisfaction with ENISA added value of contributions (survey)
	Contribution to policy implementation and implementation monitoring at EU and national levels (ex post)	Number of EU policies and regulations implemented at national level supported by ENISA Number of ENISA reports, analysis and/or studies referred to at EU and national levels (survey) Satisfaction with ENISA added value of support (survey)[16]
	Effective use of ENISA's tools, platforms and take-up of SOPs in operational cooperation	Number of users, both new and recurring, and usage per platform/tool/SOPs provided by ENISA Uptake of the platform/tool/SOPs during massive cyber incidents Stakeholder satisfaction with the relevance and added value of the platforms/tools/SOPs provided by ENISA
	ENISA's ability and preparedness to support response to massive cyber incidents	Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to the mitigation of Number of relevant incident responses ENISA contributed to as per Article 7 of the CSA Stakeholder satisfaction with ENISA's ability to provide operational support

Strategic objective	Actions to achieve objective	Article of the CSA	Expected results	
4. Cutting-edge competences and capabilities in cybersecurity across the Union	Activities 3 and 9	Article 6 and Article 7(5)	• Enhanced capabilities across the community • Increased cooperation between communities	
		Articles 10 and 12	• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience	
5. High level of trust in secure digital solutions	Activities 6 and 7	Article 8	• Draft cybersecurity certification schemes developed by ENISA under the European cybersecurity certification framework are adopted • Smooth transition to the EU cybersecurity certification framework • Certified ICT products, services and processes are preferred by consumers and, where relevant, operators of essential services or digital service providers	
			• Contribution towards understanding market dynamics • A more competitive European cybersecurity industry, small and medium-sized enterprises (SMEs) and start-ups	
6. Foresight on emerging and future cybersecurity challenges	Activity 8	Articles 9 and 11	Research and innovation agenda tied to the cybersecurity needs and requirements, including contributing to the work of the European Cybersecurity Competence Centre	
7. Efficient and effective cybersecurity information and knowledge management for Europe	Activity 8	Articles 9 and 11	• Decisions about cybersecurity are future-proof and take account of the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision-making	

	Key performance indicator	Metrics[15]
	Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Increase/decrease in maturity indicators Outreach, uptake and application of lessons learnt from capability-building activities Number of cybersecurity programmes (courses) and participation rates The number of exercises executed annually Stakeholder assessment on usefulness, added value and relevance of ENISA capacity-building activities
	• Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU • Level of outreach	Number of cybersecurity incidents reported having human error as a root cause Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics Geographical and community coverage of outreach in the EU Level of awareness of cybersecurity across the EU / among the general public (e.g. measured through Eurobarometer surveys)
	• Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions • Effective preparation of candidate certification schemes prepared by ENISA	Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions Stakeholders trust in digital solutions of certification schemes (citizens, public sector, businesses) Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework Number of candidate certification schemes prepared by ENISA Number of people/organisations engaged in the preparation of certification schemes Satisfaction with ENISA's support in the preparation of candidate schemes (measured through a survey)
	Effectiveness of ENISA's supporting role for participants in the European cybersecurity market	Number of market analyses, guidelines and good practices issued by ENISA Uptake of lessons learnt / recommendations from ENISA reports Stakeholder satisfaction with the added value and quality of ENISA's work
	ENISA's ability to contribute to Europe's research and innovation agenda	Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities (including in research)
	ENISA's ability to contribute to Europe's cyber resilience through the provision of timely and effective information and knowledge	Number of users and frequency of usage of dedicated portal (observatory) Number of recommendations, analyses and challenges identified and analysed Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities (including in research)

ENISA's strategy also establishes a set of values that guide the execution of its mandate and its functioning, as follows.

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 environments, 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.

These values are built on the ethos of the CSA, in particular the objectives set out in Article 3(4) and Article 4(1), and have been encapsulated into two corporate objectives, which form the baseline

Corporate objective	Actions to achieve objective	Article of the CSA	Expected results	
Sound resource and risk management	Activity 10	Article 4(1)	• Maximised quality and value provided to stakeholders and citizens • Building lasting credibility and trust	
Build an agile organisation focused on people	Activity 11	Article 3(4)	ENISA as an employer of choice	

from which the multiannual activities of the SPD will be delivered.

The corporate objective of **sound resource and risk management** is derived from requirements in Article 4(1) of the CSA, which sets an objective for the Agency to 'be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks'. In addition, the inspiration for this corporate objective stems from the values of **excellence** and **transparency** derived from the ENISA strategy and the principle of **efficiency** set out in the Management Board Decision MB/2020/5 on the principles to be applied for organising ENISA. This decision aims for ENISA to uphold the highest quality of standards, strive for continuous improvement and enhance its performance.

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

	Key performance indicator	Metrics
	• Organisational performance • Trust in ENISA	Proportion of key performance indicators reached Individual contribution to achieving the objectives of the Agency through clear links to key performance indicators (Career Development Report) Exceptions in risk register Number of complaints filed against ENISA including number of inquiries/ complaints to the European Ombudsman Number of complaints addressed in a timely manner and in accordance with relevant procedures Results of annual risk assessment exercise Observations from external audit bodies (e.g. European Court of Auditors) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed) Level of trust in ENISA (survey)
	Staff commitment, motivation and satisfaction	Staff satisfaction survey (including attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools) Quantity and quality of ENISA training and career development activities organised for staff Reasons for staff departure (established by exit interviews) Staff retention/turnover rate Resilience and quality of ENISA's information technology (IT) systems and services (including ability to consistently increase satisfaction with IT services and tools)

2.2. HUMAN AND FINANCIAL RESOURCES – OUTLOOK FOR 2022–2024

2.2.1. Overview of the past and current situations

Table 1.

	2019	2020	2021	2022[18]
Number of posts in the establishment plan	59	69	76	82
Fulfilment of the establishment plan (on 1 January)	76 %	80 %	80 %	94 %

As an agency, ENISA has historically struggled to meet its human resources needs and take steps to ensure timely and rapid fulfilment of its establishment plan. The gap between the available posts and the fulfilment is evidenced in Table 1. This has hampered the Agency in terms of making use of its potential capabilities in the most efficient manner, resulting in a smaller actual human resource capacity of the Agency.

In order to change this, in 2020 the Agency embarked on a large-scale call for expression of interest for temporary agents (TAs) and contract agents (CAs) following a novel approach, with the aim of creating a sufficiently diverse and broad reserve shortlist 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. The call, which was accompanied by a widespread promotional campaign, attracted 1 173 candidates for TA posts, 590 CA candidates and 229 manager candidates from across all Member States. This resulted in a reserve shortlist of 68 candidates for TA posts, 15 for CA posts and 8 for manager posts. The figures below depict the results of the recruitment exercise. The full table of results can be found in Annex IV, Table 4.

The second measure that the Agency put in place was to introduce an annual strategic workforce planning framework, which prompts the organisation to analyse its human resources needs in advance, on a multiannual basis on the basis of the SPD, and plan and review the allocation of human resources across different activities as well as prepare new recruitment calls well in advance of the enactment of the applicable annual establishment plans. This also enables the Agency to take corrective action if and when necessary, to achieve the aims set out in Article 3(3) of the Management Board Decision MB/2020/9, which foresees that the executive director will ensure that 'The average number of staff members assigned to the EDO and 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].'

In the course of the 2021 Strategic Workforce Review, the Agency, in addition to other measures, reallocated a total of four posts from executive director's office (EDO) and corporate support services (CSS), to be able to meet the threshold foreseen in Article 3(3) of Management Board Decision MB/2020/9. This resulted in a termination of one contract, and the prolongation of two contracts was put under review. The posts are now allocated to policy development & implementation unit (PDI), capacity building unit (CBU) and market, certification and standardisation unit (MCS), to be fulfilled through ongoing recruitment calls. The intended impact of the conclusions of the 2021 Strategic Workforce Review are summarised in the table below.

Table 2.

	Operational units		Supporting offices and services	
	Established staff	Average	Established staff	Average
Allocated as of 1 January 2021	48	12	38	19
Current allocation (1 October 2021)	67	16.75	40	20
Projected allocation (1 January 2022)	79	19.75	40	20

[18] Three administrator posts subject to budget approval (NIS2 proposal). Projection of establishment plan fulfilment on 1 January 2022 depends on successful conclusions of ongoing selections for Q4 2021.

Figure 1. Recruited

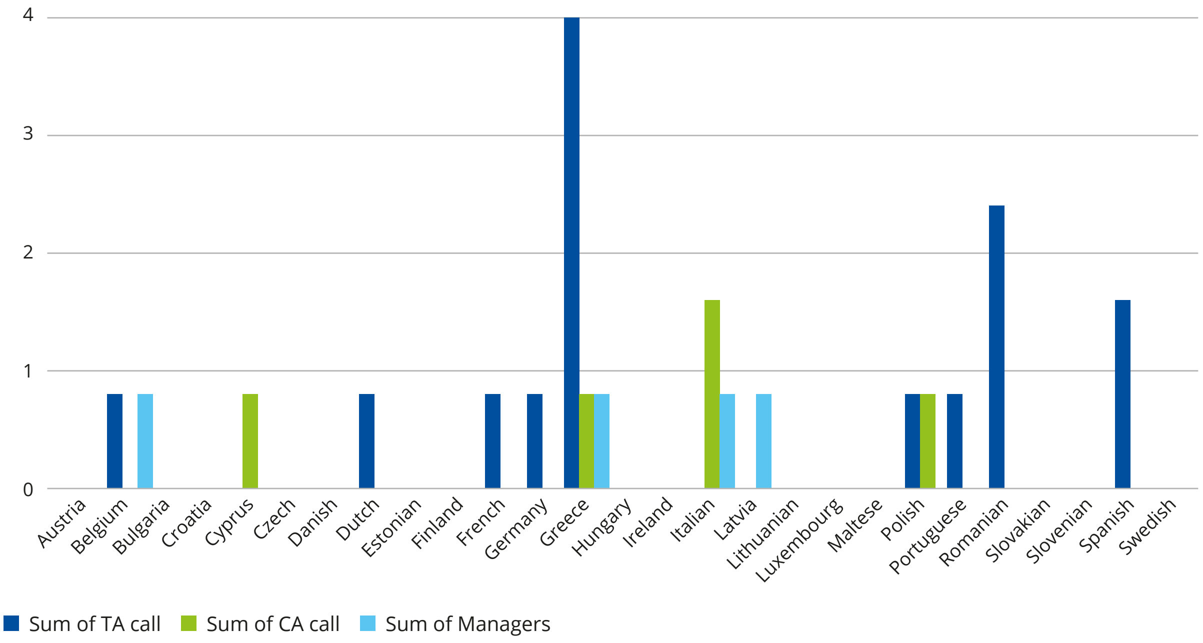
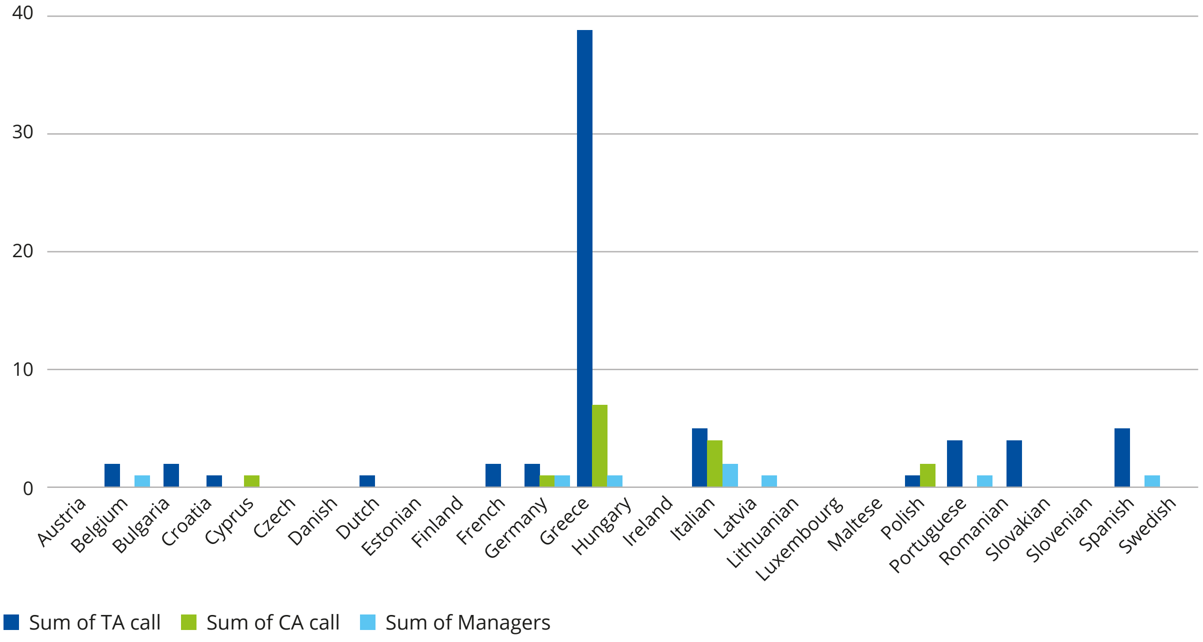


Figure 2. Reserve list



2.2.2. Outlook for 2022–2024

2.2.3. Resource programming for 2022–2024

2.2.3.1. Financial resources

The total EU contribution to ENISA over the period 2022–2024, as well as for the full period of the 2021–2027 multiannual financial framework, is intended to remain stable, with a slight annual increase of approximately 2 % to reflect inflation (see Table 3).

Table 3.

	2021	2022*	2023*	2024*
Total appropriations for ENISA	22 833 000[a]	24 208 000	24 707 000	25 220 000

* Source: Draft EU annual budget for the 2022 financial year (COM(2021) 300 and Commission forecast), including a reserve budget of EUR 610 000 as a result of the NIS2 proposal.

a Other contributions by the Greek authorities to cover rental payments up to a maximum amount of EUR 640 000 are not included.

As of 2022, 97.6 % of ENISA's revenue will be from the EU contribution and 2.4 % will be from the European Economic Area country contribution (see Annex III, Table 6). In absolute terms, the EU and European Economic Area contributions for 2022 are estimated to reach EUR 23.6 million and EUR 0.6 million respectively.

The general allocation of funds across titles is expected to remain stable during 2022–2024. Expenditure in 2022 is expected to amount to EUR 24.2 million, of which EUR 12.5 million in Title 1 covers all staff-related costs (52 %), EUR 2.8 million in Title 2 covers main items such as building-related expenditure and ICT expenses (11 %) and EUR 8.9 million in Title 3 covers all core operating expenditure (37 %). Total expenditures include the reserve budget of EUR 610 000 expected to be allocated to cover additional staff (three TAs and two CAs)[19] to manage part of the activities linked to the NIS directive being discussed by legislators.

2.2.3.2. Human resources

In its budget proposal for the 2022–2024 SPD, the Agency asks for an extra six seconded national expert (SNE) posts to be introduced gradually (two per year over 3 years). It stresses that the related costs would be budget-neutral (i.e. covered by ENISA's current budget and therefore additional budgetary resources would not be required). ENISA proposes to cover the related costs through the established operational budget (Title 3)[20], as the posts are directly linked to the operational needs and expectations of the Agency.

Specifically, the six additional SNE posts are crucial to the Agency's ability to address the tasks mandated by the CSA in the areas of development of the national cybersecurity strategies, incident reporting and indexing, and in particular in the area of operational cooperation (Article 7 of the CSA). They would therefore be justified both by the Agency's current activity areas and by those extra activities and requirements, as foreseen especially in the initial phases of the JCU, as per the Commission's recommendation on the Joint Cyber Unit of 23 June 2021.

It is clear that the request for the six SNEs cannot cover all the potential future developments of the JCU, nor that only exclusively SNE posts will be able to cater for future needs. It is however also clear that without the inclusion of such posts, it will be far more challenging for the Agency to support the crucial initial phases of the JCU. Based on the above approach, the request for the six SNE posts without additional budgetary resources has a 3-year time frame between 2022 and 2024 (e.g. they can be introduced gradually: two per year over 3 years).

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

[19] The Commission asks ENISA to amend its establishment plan and resource planning in order to include the additional five full-time equivalents (three temporary agent and two contract agent posts), as specified in the legislative financial statement accompanying the proposal for a directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ((COM 2020/823) final). These resources should be managed as reserves that the Agency can draw on once the final budget is adopted. The Commission invites the Agency to update the draft single programming document with the impact of this Commission proposal.

[20] In terms of process at the time of writing, the Commission opinion of 24 August 2021 (6130) did not support this proposal, as reflected in the 2022–2024 SPD. This had been endorsed by the Management Board in the past and is currently pending final outcome in the budgetary approval process among co-legislators.

Member States and offer a rich experience to SNEs following their posting.

In addition, and pending the final outcome of the proposed NIS directive proposal, NIS221, as of 2022/2023, ENISA may be 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 full-time equivalents (FTEs) (three TAs and two CAs) with a corresponding budget of around EUR 610 000 per year. This is an integrated part of the NIS2 proposal, which is subject to approval and managed as reserves that the Agency can draw on following the completion of the EU budget process.

As all those resources are required in order to fulfil the operational mandate of the Agency, the Agency also plans to allocate all the new posts to operational units. Thus, although the current average does not meet the threshold foreseen in Article 3(3) of Management Board Decision MB/2020/9, it should be regarded as a temporary derogation until such time as the new posts will become available and subsequently established. The Agency also commits itself not to raise the number of staff assigned to supporting offices and services (EDO and CSS) from the current level (a total of 40 staff members).

2.2.4. Strategy for achieving efficiency gains

ENISA is committed to continuously implementing measures to obtain efficiency gains in all activities. In 2021, the ENISA organisational structure was amended to follow the principles of sound budgetary management and building efficiencies in both executing its core mandate and fulfilling its corporate functions. Also, the Agency continues to implement its work programme by systematic use of its statutory bodies (National Liaison Officers (NLO) Network and ENISA Advisory Group), as well as other statutory groups ENISA is involved in (Stakeholder Cybersecurity Certification Group (SCCG) as set out in Article 22 of the CSA and NISD Cooperation Group and its work streams and expert groups created under EU law) and its own ad hoc expert groups where appropriate to peer review the scope and direction of actions undertaken to implement outputs, as well as validate the results. This way, the Agency will fulfil its obligation as outlined in Article 3(3) of the CSA: avoiding duplication of Member State activities and taking into consideration existing Member State expertise. Hence, all activities enlisted under Sections 3.1 and 3.2 of this SPD contain an indication of how specific deliverables and other actions undertaken to fulfil the outputs will be validated and peer reviewed or consulted as per the legal requirements in the area of certification.

In 2021, the framework for structured cooperation with CERT-EU to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation (Article 7 of the CSA) is being implemented, and a 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 EU bodies (through the Joint Research Centre) and will create synergies with the Cybersecurity Competence Centre and the Network of National Coordination Centres once established to pursue synergies in fulfilling their tasks in the field of research and innovation (Article 11 of the CSA).

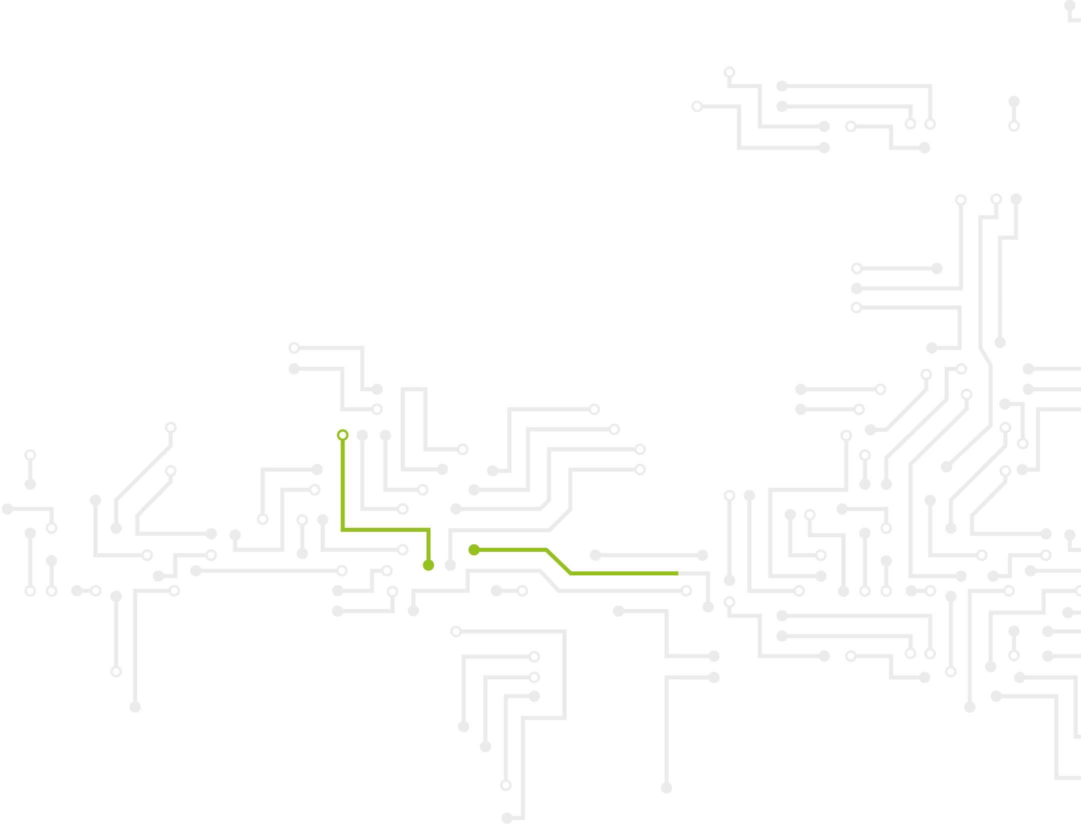
In its corporate functions, ENISA seeks to further rationalise its internal processes to improve its overall efficiency and to benchmark its activities with the best practices implemented by other EU institutions and agencies. The Agency is continuing and further expanding the sharing of services among other EU agencies. A number of collaborations and agreements are currently in place (e.g. with the European Union Intellectual Property Office) 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, share financial services, increase efficiency gains in human resources, explore IT solutions together and support each other in the area of data protection. The aim is to share knowledge and utilise human resources in the most efficient manner between the two agencies, resulting in better value for EU citizens.

Prompted by the COVID-19 crisis, the Agency established efficiency gains through digitalisation of its functions. It is already using EU tools such as accrual-based accounting (ABAC), ABAC assets, procurement and e-invoicing. Furthermore, in 2020 the Agency deployed Sysper and in 2021 the migration of its services to other tools, such as; Missions Integrated Processing System (MIPS) and Advanced Record System (ARES), is foreseen. Most administrative tasks are already supported

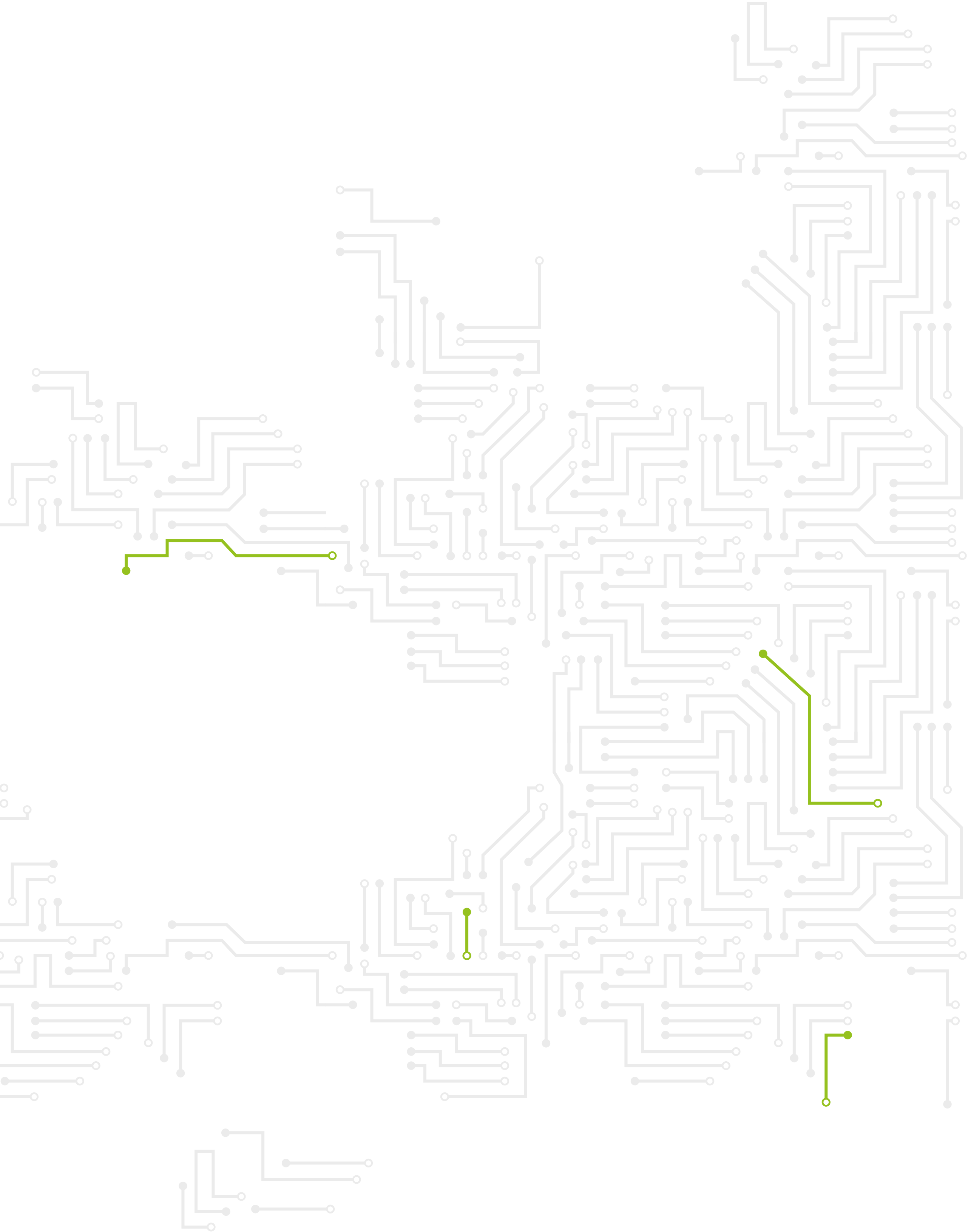
[21] Proposal COM 2020/823 of 16 December 2020 for a directive revising Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

by the application 'Paperless' and others, which is a significant step towards the goal of 100 % e-administration. E-training is also internally encouraged, with the aim, among others, of reducing the costs associated with 'classroom' training (travelling costs etc.).

In 2021, the Agency established a series of events and webinars for external parties and will upgrade its capabilities to use secure digital conferencing across the field, providing further opportunities in efficiency gains as well as expanding the scale and scope of its activities.



PART II. Multiannual programming 2022–2024



III

PART III

WORK PROGRAMME FOR 2022

This is the main body of the work programme, describing, as per operational and corporate activity, what the Agency aims to deliver in the respective year in terms of achieving its strategy and the expected results. In total, nine operational activities and two corporate activities have been identified to support the implementation of ENISA's mandate in 2022.

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

Activities 1, 2, 3 and 9 represent the Agency's most developed areas, with longstanding projects such as policy support, cyber exercises and training and European Cybersecurity Month. Activities 4–8 represent the areas of the Agency that are developing, such as contributing to cooperative response, certification, supporting the cybersecurity market and industry, and providing analysis on emerging challenges. Prioritisation in terms of resources is foreseen for these less-developed activities to support their development over the coming years.

In addition, the activities below do not reflect the additional five supplementary FTEs (three TAs and two CAs) and the corresponding budget of EUR 610 000 per year from the proposed NIS directive (NIS2)[22]. This allocation will take place in due course, in accordance with the final agreement of regulators and once tasks have been finalised.

[22] Proposal COM 2020/823 of 16 December 2020 for a directive revising Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

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 law initiatives where matters related to cybersecurity are involved, and on the basis of the new 2020 EU cybersecurity strategy. Aspects such as privacy and personal data protection are taken into consideration (including encryption).

This activity seeks to bolster policy initiatives on novel/emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. In addition to support in emerging policy areas (such as AI, 5G, EU eID, quantum computing, blockchain, big data, digital resilience and response to current and future crises), ENISA – in coordination with the Commission and Member States – will also conduct policy scouting to support the Commission and Member States in identifying potential areas of policy development, as well as develop monitoring capabilities and tools to regularly and consistently be able to give advice on the effectiveness of existing EU policy and law in accordance with the EU's institutional competencies in this area.

The added value of this activity is to support the decision-makers in a timely manner on developments at technological, societal and economic market levels that might affect the cybersecurity policy framework (see also activity 8). Given the cross-cutting nature of cybersecurity across the policy landscape, this 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 policymakers are regularly informed about the effectiveness of the existing frameworks and EU policymakers and stakeholders are provided with timely and tailor-made policy recommendations on future cybersecurity challenges and opportunities.

Link to strategic objective (ENISA strategy)

- Cybersecurity as an integral part of EU policies

Results

Cybersecurity aspects are considered and embedded across EU and national policies

Outputs

1.1. Issue reports, studies and analyses on the effectiveness of the current cybersecurity policy frameworks.

1.2. Carry out preparatory work and provide the Commission and Member States with tailor-made advice and recommendations on new policy initiatives in emerging technological, societal and economic trends, such as AI, 5G, eID, digital operational resilience in the finance sector, cyber insurance and other potential initiatives (e.g. The Once Only Technical Solution).

1.3. Assist the Commission in reviewing existing policy initiatives.

Key performance indicator

Indicator:

ENISA's added value to EU institutions, bodies and Member States in providing support to policymaking (ex ante).

Metrics:

1.1. Number of relevant contributions to EU and national policies and legislative initiatives[23].

1.2. Number of references to ENISA reports, analysis in EU and/or national policy documents.

1.3. Satisfaction with the added value of ENISA's contributions (survey).

Frequency: Annual (1.1 and 1.2), biennial (1.3)

Validation

- NIS Cooperation Group (NIS CG) and other formally established groups (outputs 1.1 and 1.2).
- ENISA ad hoc working groups[24] (output 1.2).
- NLO Network, ENISA Advisory Group and other formally established expert groups (when necessary).

Target groups and beneficiaries

EU and national policymaking institutions, EU and national experts (NIS CG, relevant/competent EU or Member State organisations/bodies) and electronic communications services.

Resources planned

Total Human resources (FTEs)	6[25]	Total Financial resources (EUR)	363 000

[23] Baselines for these metrics should be known by the end of 2021. Therefore, targets linked to these baselines will be developed in 2022 for the 2023 work programme.

[24] Created under Article 20(4) of the CSA.

[25] Allocation of an additional five FTEs from the NIS proposal will take place in due course according to the final agreement of regulators and once the tasks have been finalised.

ACTIVITY 2: Supporting implementation of Union policy and law

Overview of activity

This activity provides support to Member State and EU institutions in the implementation of European cybersecurity policy and the legal framework and advice on specific cybersecurity aspects related to the EU's 2020 cybersecurity strategy, the NIS directive, telecom and electronic communications security, data protection, privacy, eID (including the European digital identity framework and trust services), incident notification and the general availability or integrity of the public core of the open internet.

It further supports initiatives related to implementation of policy frameworks on novel digital technologies such as 5G (e.g. 5G Cybersecurity Toolbox) and assisting the work of the NIS Cooperation Group and its work streams.

Contribution towards the Commission's regular monitoring of the implementation of specific EU policies is envisaged, which considers relevant indicators and could contribute to possible indices that could capture the maturity of relevant cybersecurity policies, and provide input to the review of existing policies (output 1.3).

This activity helps to avoid fragmentation and supports a coherent implementation of the digital single market across Member States, following a consistent approach to cybersecurity, privacy and data protection.

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

Objectives

- Consistent development of sectoral Union policies with horizontal Union policy to avoid implementation inconsistencies.
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in Member States.
- Effective implementation of cybersecurity policy across the EU and aim to support consistency of Member State laws, regulations and administrative provisions related to cybersecurity.
- Improved cybersecurity practices, taking on board lessons learnt from incident reports.

Link to strategic objective (ENISA strategy)

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

Results

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

Outputs

2.1. Support the NIS Cooperation Group and work streams as per the NIS CG work programme and sectors under NISD.

2.2. Support Member States and the Commission in the implementation and monitoring of the 5G Cybersecurity Toolbox and its individual actions.

2.3. Provide advice, issue technical guidelines and facilitate exchange of good practices to support Member States and the Commission on the implementation of cybersecurity policies, in particular eID and the trust services framework, European Electronic Communications Code and its implementing acts, and security measures for data protection and privacy.

2.4. Assisting in establishing and implementing vulnerability disclosure policies considering also the NIS2 proposal.

Key performance indicator

Indicator:

Contribution to policy implementation and implementation monitoring at EU and national levels (ex post).

Metrics:

2.1. Number of EU policies and regulations implemented at national level supported by ENISA.

2.2. Number of ENISA reports, analyses and/or studies referred to at EU and national levels (survey).

2.3. Satisfaction with added value of ENISA's support (survey).

Frequency: Annual (2.1), biennial (2.2 and 2.3).

Validation

- NIS Cooperation Group or established work streams (outputs 2.1 and 2.2).
- Article 13a Expert Group and Article 19 Expert Group (output 2.3).
- Formally established bodies and expert groups as necessary (outputs 2.3 and 2.4).
- NLO Network (as necessary).

Target groups and beneficiaries

- Member State cybersecurity authorities (NISD CG members), national supervisory authorities, data protection authorities and national accreditation bodies.
- The Commission, EU institutions/bodies (e.g. Body of European Regulators for Electronic Communications (BEREC), European Data Protection Supervisor, European Data Protection Board, European Union Agency for Railways (ERA), European Maritime Safety Agency (EMSA), sectoral EU agencies (e.g. European Union Agency for the Cooperation of Energy Regulators (ACER) and Interinstitutional committees (e.g. ICT Advisory Committee (ICTAC), Interinstitutional committee for digital transformation (ICDT).
- Article 13a Expert Group and Article 19 Expert Group members.
- EU citizens.
- Conformity assessment bodies and trust service providers.
- Operators of essential services, including their associations and networks.

Resources planned

Total Human resources (FTEs)	**12**	**Total Financial resources (EUR)**	**798 475**

ACTIVITY 3: Building capacity

Overview of activity

This activity seeks to improve and develop the capabilities of Member States and EU institutions, bodies and agencies, as well as various sectors, to respond to cyber threats and incidents and to increase resilience and preparedness across the EU. Actions to support this activity include organising large-scale exercises and sectoral exercises and training, including CSIRT training. In addition, this activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem, including cross-border information sharing, and assist in reviewing and developing national- and EU-level cybersecurity strategies.

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

Objectives

- Increase the level of preparedness and cooperation within and between Member States, 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.
- Increase the supply of skilled professionals to meet market demand, and promote cybersecurity education.

Link to strategic objective (ENISA strategy)

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

Results

- Enhanced capabilities across the community.
- Increased cooperation between communities.

Outputs

3.1. Assist Member States to develop national cybersecurity strategies.

3.2. Organise large-scale biennial exercises and sectoral exercises (Cyber Europe, Blue OLEx, CyberSOPex, etc.) including through cyber ranges.

3.3. Organise training and other activities to support and develop maturity and skills of

Key performance indicator

Indicator:

Increased resilience to cybersecurity risks and preparedness to respond to cyber incidents.

Metrics:

3.1. Increase/decrease of maturity indicators.

3.2. Outreach, uptake and application of lessons learnt from capability-building activities.

Outputs

CSIRTs (including the NIS sectoral CSIRT) and other communities.

3.4. Develop coordinated and interoperable risk management frameworks.

3.5. Support the capacity-building activities of the NIS Cooperation Group and work streams as per the NIS CG work programme.

3.6. Support European information-sharing communities through information-sharing and analysis centres (ISACs) based on the core service platform of the Connecting Europe Facility, as well as other collaboration mechanisms such as public-private partnerships. Support the reinforcement of SOCs as well as their collaboration, assisting Commission and Member State initiatives in this area in line with the objectives of the EU cybersecurity strategy in the building and improving of SOCs[26].

3.7. Organise and support cybersecurity challenges including the European Cybersecurity Challenge.

3.8. Report on cybersecurity skills needs and gaps, and support skills development, maintenance and implementation (including a digital education action plan and a report on higher education programmes).

Validation

- NLO Network (as necessary).
- CSIRTs Network (output 3.3).
- CyCLONe members (as necessary).
- NIS Cooperation Group (outputs 3.5 and 3.6).
- Ad hoc working group on SOCs (output 3.6).

Key performance indicator

3.3. Number of cybersecurity programmes (courses) and participation rates.

3.4. Number of exercises executed annually.

3.5. Stakeholder assessment of usefulness, added value and relevance of ENISA capacity-building activities (survey).

Frequency: Annual (3.1, 3.2, 3.3 and 3.4), biennial (3.5).

Target groups and beneficiaries

- Cybersecurity professionals.
- EU institutions and bodies.
- Private industry sectors (operators of essential services such as health and transport).
- CSIRTs Network and related operational communities.
- European information-sharing and analysis centres.
- CyCLONe members.

Resources planned

Total Human resources (FTEs)	**13**	**Total Financial resources (EUR)**	**1 921 265**

[26] In particular, continue developing and updating the mapping of the current landscape of SOCs in the EU, including public and private, provide in-house or as a service, and main operators of SOCs services in the EU, and provide other relevant support to the Commission in implementing the SOCs-related objectives of the EU cybersecurity strategy (e.g. support for the design of calls for expressions of interest, procurements, etc., liaison with stakeholders and research activities).

ACTIVITY 4:
Enabling operational cooperation

Overview of activity

This activity supports operational cooperation among Member States and EU institutions, bodies, offices and agencies and between operational activities, in particular by establishing a local office in Brussels. Actions include establshing synergies with the different national cybersecurity communities (including civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors – notably CERT-EU – with the view to exchange know-how and best practices, provide advice and issue guidance.

In addition, this activity supports Member States with respect to operational cooperation within the CSIRTs Network by advising on how to improve capabilities and providing support to ex post technical inquiries regarding incidents.

Under this activity, ENISA supports operational communities by helping to develop and maintain secure and highly available networks / IT platforms and communication channels, in particular ensuring maintenance and deployment of the MeliCERTes platform.

In view of Commission Recommendation (EU) 2021/1086 and the Council conclusions of the 20 October 2021 (ST 13048 2021) 'Exploring the potential of the Joint Cyber Unit (JCU) initiative – Complementing the EU coordinated response to large-scale cybersecurity incidents and crises', ENISA will engage in the development of the JCU, along the lines and the roles defined according to ongoing discussions among Member State and EU operational actors.

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

Objectives

- Enhance and improve incident response capabilities across the EU.
- 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, European Union Agency for Law Enforcement Cooperation (Europol)).
- Improve maturity and capacities of operational communities (including CSIRTs Network, CyCLONe group).
- Contribute to preparedness, shared situational awareness, and coordinated response to and recovery from large-scale cyber incidents and crises across different communities.

Link to strategic objective (ENISA strategy)

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

Results

- All communities (EU institutions and Member States) use a rationalised and coherent set of SOPs for cyber crisis management.
- Efficient framework, tools (secure and high availability) and methodologies for effective cyber crisis management.

Outputs

4.1. Support the functioning and operations of the CSIRTs Network (also through MeliCERTes), CyCLONe, JCU, SOCs Network[27] and cyber crisis management in the EU, including cooperation with relevant Blueprint stakeholders (e.g. Europol, CERT-EU, European External Action Service and European Defence Agency).

4.2. Develop and enhance standard operating policies, procedures, methodologies and tools for cyber crisis management (also related to a future JCU).

4.3. Deploy and maintain operational cooperation platforms and tools (MeliCERTes, CyCLONe, MoUs, etc.), including preparations for a secure virtual platform for a future JCU.

Key performance indicator

Indicator:

Effective use of ENISA's tools, platforms and take-up of SOPs in operational cooperation.

Metrics:

4.1. Number of users, both new and recurring, and usage per platform/tool/SOPs provided by ENISA.

4.2. Uptake of the platform/tool/SOPs during massive cyber incidents.

4.3. Stakeholder satisfaction with the relevance and added value of the platforms/tools/SOPs provided by ENISA (survey).

Frequency: Annual (4.1 and 4.2) and biennial (4.3).

Validation

- NLO Network (as necessary).
- CSIRTs Network and CyCLONe (output 4.1).
- Blueprint actors.

Target groups and beneficiaries

- Blueprint stakeholders.
- EU decision-makers, institutions, agencies and bodies.
- Member State CSIRTs Network members.
- NISD Cooperation Group.
- Operators of essential services (OESs) and digital service providers (DSPs).

Resources planned

Total Human resources (FTEs)	10	Total Financial resources (EUR)	1 703 350

[27] Provide support for the design and development of cross-border platforms for pooling of CTI data at EU level (including definition of a blueprint architecture, data infrastructure requirements, data processing and analytics tools, data sharing protocols), CTI exchange initiatives already under way, legal aspects, interoperability, etc.

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

Overview of activity

This activity contributes to the development of a cooperative response at EU and Member States levels to large-scale, cross-border incidents or crises related to cybersecurity by aggregating and analysing reports to establish a common situational awareness, ensuring information flow and escalation measures between the CSIRTs Network and technical, operational and political decision-makers at EU level.

In addition, this activity can include, at the request of Member States, facilitating the handling of incidents or crises, public communication related to such incidents or crisis and testing cooperation plans for such incidents or crises. It can also include supporting EU institutions, bodies, offices and agencies with public communication regarding such incidents and crises. This activity also supports Member States with respect to operational cooperation within the CSIRTs Network by providing advice on a specfic cyber threat, assisting in the assessment of incidents, facilitating technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities.

This activity supports operational cooperation, including mutual assistance and the situational awareness in the framework of the proposed JCU.

Moreover, this activity seeks to engage with CERT-EU in structured cooperation (see Annex XIII of the annual cooperation plan). The legal basis for this activity is Article 7 of the CSA.

Objectives

- Effective incident response and cooperation among Member States and EU institutions, including cooperation of technical and political actors during incidents or crises.
- Common situational awareness of cyber incidents and crises across the EU.
- Information exchange and cooperation, cross layer and cross border between Member States and as well as with EU institutions.

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.

Results

- Member States and institutions cooperating effectively during large-scale, cross-border incidents or crises.
- Public informed of important cybersecurity developments.
- Stakeholders aware of current cybersecurity situation.

Outputs

5.1. Generate and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, operational and technical levels.

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. Initiate the development of a trusted network of vendors/suppliers.

Key performance indicator

Indicator:

ENISA's ability and preparedness to support the response to massive cyber incidents.

Metrics:

5.1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to the mitigation of (survey).

5.2. Stakeholders' satisfaction with ENISA's preparedness and ability to provide operational support (survey).

5.3. Number of relevant incident responses ENISA contributed to as per Article 7 of the CSA.

Frequency: Biennial (5.1 and 5.2), annual (5.3).

Validation

- Blueprint actors.

Target groups and beneficiaries

- EU Member States (including CSIRTs Network members and CyCLONe).
- EU institutions, bodies and agencies.
- Other type of CSIRTs and product security incident response teams.

Resources planned

Total Human resources (FTEs)	**8**	**Total Financial resources (EUR)**	**824 500**

ACTIVITY 6:
Development and maintenance of EU cybersecurity certification framework

Overview of activity

This activity emcompasses actions to establish a European cybersecurity schemes by preparing and reviewing candidate European cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the EU's rolling work programme. Actions also include evaluating adopted certification schemes and participating in peer reviews. In addition, this activity assists the Commission in providing secretariat of the European Cybersecurity Certification Group (ECCG) and providing secretariat of the Stakeholder Cybersecurity Certification Group (SCCG). ENISA also makes available and maintains a dedicated European cybersecurity certification website, as per Article 50 of the CSA.

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.

Link to strategic objective (ENISA strategy)

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

Results

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

Outputs

6.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes.

6.2. Implementation and maintenance of the established schemes, including evaluation of adopted schemes and participation in peer review.

6.3. Support the statutory bodies in carrying out their duties with respect to governance roles and tasks.

6.4. Development and maintenance of necessary tools for making effective use of the EU's cybersecurity certification framework (including the certification website, the core service platform (Connecting Europe

Key performance indicator

Indicators:

1. Uptake of the European cybersecurity certification framework and schemes as an enabler of secure digital solutions.
2. ENISA's effective preparation of candidate certification schemes.

Metrics:

6.1. Number of stakeholders (public authorities and/or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions.

6.2. Stakeholders' trust in digital solutions of certification schemes (citizens, public sector and businesses) (survey).

Outputs

Facility) for collaboration, and publication and promotion of the implementation of the cybersecurity certification framework).

Key performance indicator

6.3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework.

6.4. Number of candidate certification schemes prepared by ENISA.

6.5. Number of people/organisations engaged in the preparation of certification schemes.

6.6. Satisfaction with ENISA's support in the preparation of candidate schemes (survey).

Frequency: Annual (6.1, 6.4 and 6.5), biennial (6.2, 6.3 and 6.6).

Validation

- Ad hoc certification expert groups (output 6.1).
- ECCG (outputs 6.1 and 6.2).
- European Commission (outputs 6.1–6.3).
- SCCG (outputs 6.3 and 6.4).

Target groups and beneficiaries

- Public authorities, accreditation bodies at Member State and EU levels, certification supervisory authorities, conformity assessment bodies.
- Product manufacturers and service providers who have an interest in EU schemes for the certification of ICT products and services (industry).
- The European Commission; other EU institutions, agencies and competent authorities (e.g. European Data Protection Board); public authorities in the Member States; and members of the ECCG and SCCG.

Resources planned

Total Human resources (FTEs)	**11**	**Total Financial resources (EUR)**	**1 025 750**

ACTIVITY 7: Supporting the European cybersecurity market and industry

Overview of activity

This activity seeks to foster a cybersecurity market (products and services) in the EU and the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce the dependence from outside the Union and to reinforce supply chains inside the Union. 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 compiling guidelines on and examples of good practices in cybersecurity requirements, facilitating the establishment and take-up of European and international standards for risk management, and performing regular analysis of cybersecurity market trends on both the demand side and the supply side, including monitoring, collecting and identifying dependencies among ICT products, services, and processes, and vulnerabilities present therein. Platforms for collaboration among the cybersecurity market players improve visibility of trustworthy and secure ICT solutions in the internal digital market.

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

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.

Link to strategic objective (ENISA strategy)

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

Results

- Contribution towards understanding market dynamics.
- A more competitive European cybersecurity industry, SMEs and start-ups.

Outputs

7.1. Market analysis on the main trends in the cybersecurity market on both the demand side and the supply side.

7.2. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international standards for risk management in relation to certification.

7.3. Guidelines on and examples of good practices in cybersecurity certification requirements for ICT products, services and processes.

7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services.

Key performance indicator

Indicator:

Effectiveness of ENISA's supporting role for participants in the European cybersecurity market.

Metrics:

7.1. Number of market analyses, guidelines and good practices issued by ENISA.

7.2. Uptake of lessons learnt / recommendations from ENISA reports.

7.3. Stakeholder satisfaction with the added value and quality of ENISA's work (survey).

Frequency: Annual (7.1 and 7.2), biennial (7.3).

Validation

- SCCG (outputs 7.2 and 7.3).
- ENISA Advisory Group (output 7.1).
- NLO (as necessary).
- ECCG (output 7.4).

Target groups and beneficiaries

- European ICT industry, SMEs, start-ups, product manufacturers and service providers.
- European standardisation organisations (European Committee for Standardization, European Committee for Electrotechnical Standardization and ETSI) and international and industry standardisation organisations.

Resources planned

Total Human resources (FTEs)	**8**	**Total Financial resources (EUR)**	**373 800**

ACTIVITY 8:
Knowledge on emerging cybersecurity challenges and opportunities

Overview of activity

This activity shall provide strategic long-term analysis, guidance and advice on emerging technologies (such as in the area of artificial intelligence, quantum, distributed ledgers, cloud computing, edge computing, software development, etc). On the basis of risk management principles, the Agency will identify cyber threats, vulnerabilities and risks, and map threat landscapes and provides topic-specific as well as general assessments on the expected societal, legal, economic and regulatory impact, as well as targeted recommendations to Member States and Union institutions, bodies, offices and agencies. In addition to this the activity will continue its effforts in developing the EU cybersecurity index. The activity also seeks to identify and give advice on research and innovation needs and priorities in the field of cybersecurity, and contribute to strategic agenda setting for cybersecurity research and innovation.

A key new component of this activity will be the contribution to the work of the European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres ("Competence Centre and Network"). This will include contributing to the development of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, and the respective work programmes.

These activities leverage on expertise of relevant legal, regulatory, economic and society trends and data by aggregating and analysing information.

The legal basis for this activity is Article 9 ,Article 11 and Article 5(6) of the CSA.

Objectives

- Identify and understand future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase Member States' and Union's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities
- Understanding the current state of cybersecurity across the Union
- Link cybersecurity needs with the EU research & innovation agenda in the field of cybersecurity

Link to strategic objective (ENISA strategy)

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

Results

- Decisions about cybersecurity are future-proof and take account of the trends, developments and knowledge across the ecosystem.
- Stakeholders receive relevant and timely information for policymaking and decision-making.
- The research and innovation agenda is tied to cybersecurity needs and requirements.

Outputs

8.1. Develop and maintain an EU cybersecurity index.

8.2. Collect and analyse information to report on the cyber threat landscapes.

8.3. Analyse and report on incidents as required by Article 5(6) of the CSA.

8.4. Develop and maintain a portal (information hub), a one-stop shop to organise and make available to the public information on cybersecurity, and establish 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. Contribute to the EU's strategic research and innovation agenda and programmes in the field of cybersecurity (annual report).

8.7. Advise on potential investment priorities (e.g. capacity building and market and industry) and emergent cyber technologies, in particular supporting the activities of the Competence Centre and the Network.

Key performance indicator

Indicator:

ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge, including its contribution to the research and innovation agenda.

Metrics:

8.1. Number of users and frequency of usage of the dedicated portal (observatory).

8.2. Number of recommendations, analyses and challenges identified and analysed.

8.3. Number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities.

8.4. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research (survey).

Frequency: Annual (8.1–8.3), biennial (8.4).

Validation

- NLO Network (as necessary).
- ENISA Advisory Group (as necessary).
- ENISA ad hoc working group (as necessary).
- Formally established bodies and expert groups as necessary (output 8.3).
- The European Cybersecurity Competence Centre and Network of National Coordination Centres and Competence Centre Governing Board (outputs 8.6 and 8.7).

Target groups and beneficiaries

- General public.
- Industry, research and academic institutions and bodies.
- Article 13a Expert Group and Article 19 Expert Group members
- EU and national decision-making bodies and authorities.
- European Cybersecurity Competence Centre and Network.

Resources planned

Total Human resources (FTEs)	**10**	**Total Financial resources (EUR)**	**1 051 950**

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, EU institutions, bodies, offices and agencies and the EU's international partners, it aims to build an empowered global community that can counter risks in line with the values of the EU. Under this activity, the Agency will be organising regular outreach campaigns, providing guidance on best practices and support coordination across Member States on awareness and education.

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

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

The legal basis for this activity is Articles 10, 12 and 42 of the CSA.

Objectives

- Advance cybersecure 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.

Link to strategic objective (ENISA strategy)

- Empowered and engaged communities across the cybersecurity ecosystem.

Results

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

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 ENISA stakeholders' strategy.

9.3. Implement ENISA international strategy and outreach

9.4. Organise European Cybersecurity Month and related activities.

Key performance indicator

Indicator:

1. Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU.

2. Level of outreach.

Metrics:

9.1. Number of cybersecurity incidents reported having human error as a root cause.

9.2. Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics.

9.3. Geographical and community coverage of outreach in the EU.

9.4. Level of awareness of cybersecurity across the EU / general public (e.g. Eurobarometer and other surveys).

Frequency: Annual (9.1–9.3), biennial (9.4).

Validation

- Management Board (outputs 9.1 and 9.3), SCCG (for certification-related issues under output 9.2).
- NLO Network.
- ENISA Advisory Group (outputs 9.1 and 9.2).

Target groups and beneficiaries

- General public, businesses and organisations.
- Member States and EU institutions, bodies and agencies.
- International partners.

Resources planned

Total Human resources (FTEs)	**5**	**Total Financial resources (EUR)**	**439 900**

3.2. CORPORATE ACTIVITIES

Activities 10 and 11 encompass enabling actions that support the operational activities of the Agency.

ACTIVITY 10: Performance and risk management

Overview of activity

This activity seeks to achieve requirements set out in Article 4(1) of the CSA, which 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, which should be developed and implemented Agency wide.

Under this activity, ENISA will continue to enhance key objectives of its reorganisation, as described in the Management Board Decision MB/2020/5, including the need to address the gaps in the Agency's quality assessment framework, install proper and functioning internal controls and compliance checks, make best use of the internal resources of the Agency, impose sound financial and budgetary management, and utilise internal and external synergies within ENISA. These aspects are addressed in the new organisational architecture, but should also be built into the daily operations of the Agency as guided by the work programme. Actions undertaken will ensure that the Agency's outputs add real value, through making performance and ex post and ex ante evaluations integral to the work programme througout its life cycle, including by rigorous quality assurance through proper project management, internal peer reviews and independent audits and validations. Gaps in skills and training as well as resource planning will be reviewed and mitigated. The Agency will carry out a risk assessment of its organisational activities and IT systems and propose mitigation measures. The Agency will link its main business processes with information systems that serve these processes and will produce a single registry of corporate processes (SOPs).

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

Objectives

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

Link to strategic objective (ENISA strategy)

- Sound resource and risk management.

Results

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

Outputs

10.1. Implementation of a performance management framework.

10.2. Implementation of a communications strategy.

10.3. Develop and implement risk management plans (including cybersecurity risk assessment of IT systems and a quality management framework) and relevant policies and processes.

10.4. Develop and monitor the implementation of Agency-wide budgetary and IT management processes.

10.5. Implement single administrative practices across the Agency.

10.6. Carry out an overarching audit on the CO_2 impact of all operations of the Agency and develop and implement a targeted action plan.

Key performance indicator

Indicator:

1. Organisational performance culture.

2. Trust in ENISA.

Metrics:

10.1. Proportion of key performance indicators reaching targets.

10.2. Individual staff contribution to achieving the objectives of the Agency through clear links to key performance indicators (CDR report).

10.3. Exceptions in risk register.

10.4. Number of complaints filed against ENISA, including number of inquiries/complaints of the European Ombudsman.

10.5. Number of complaints addressed in a timely manner and in accordance with relevant procedures.

10.6. Results of the annual risk assessment exercise.

10.7. Observations from external audit bodies (e.g. European Court of Auditors) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed).

10.8. Level of trust in ENISA (survey).

Frequency: Annual (10.1–10.7), biennial (10.8).

Validation

- Management Team.
- Budget Management Committee.
- IT Management Committee.
- Intellectual Property Rights Management Committee.
- Staff Committee.
- ENISA Ethics Committee.

Target groups and beneficiaries

- Citizens.
- All stakeholders of the Agency.

ACTIVITY 11:
Staff development and working environment

Overview of activity

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

Moreover, the impact of the pandemic has shed new light on remote working and the Agency operates a flexible (50/50) office / home working arrangements to better balance work requirements in a pragmatic manner.

The actions that will be pursued under this activity will focus on attracting, retaining and developing talent and building ENISA's reputation as an employer of choice and as an agile and knowledge-based organisation in which staff can evolve personally and professionaly, keeping staff engaged, motivated and with a sense of belonging. This activity will seek to build an attractive workspace by establishing and maintaining excellent working conditions (premises, layout of office space) and developing user-centric (tele)working and conferencing tools (including IT systems and platfoms), delivering state-of-the-art services and supporting ENISA's business owners and stakeholders in line with the Agency's objectives.

Objectives

- Ensure that staff are engaged, committed and motivated to deliver, and empowered to fully use their talent, skills and competences.
- Digitally enabled workplace and working environment (including home workspace) that promote performance and balance social and environmental responsibility.

Link to strategic objective (ENISA strategy)

- Build an agile organisation focused on people.

Results

- ENISA as an employer of choice.

Outputs

11.1. Maintain and implement the competence framework into all HR processes (including into training strategy, CDR, internal competitions and exit interviews).

11.2. Develop a HR strategy with an emphasis on talent development, growth and innovation.

11.3. Undertake actions to develop and nourish talent and conduct necessary management development activities.

11.4. Develop and maintain a user-friendly and service-oriented teleworking and office environment (including digital tools and services).

11.5. Set up service provisions standards and provide quality support and services for ENISA staff, employees, corporate partners and visitors.

Key performance indicator

Indicator:

Staff commitment, motivation and satisfaction.

Metrics:

11.1. Staff satisfaction survey (including attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools).

11.2. Quantity and quality of ENISA's training and career development activities organised for staff.

11.3. Reasons for staff departure (exit interviews).

11.4. Staff retention/turnover rate.

11.5. Resilience and quality of ENISA's IT systems and services (including ability to consistently increase satisfaction with IT services and tools).

Frequency: Annual (or ad hoc for metric 11.3).

Validation

- Management Team.
- Joint Reclassification Committee.
- IT Management Committee.
- Task Force on Relocation of the Agency.
- Staff Committee.

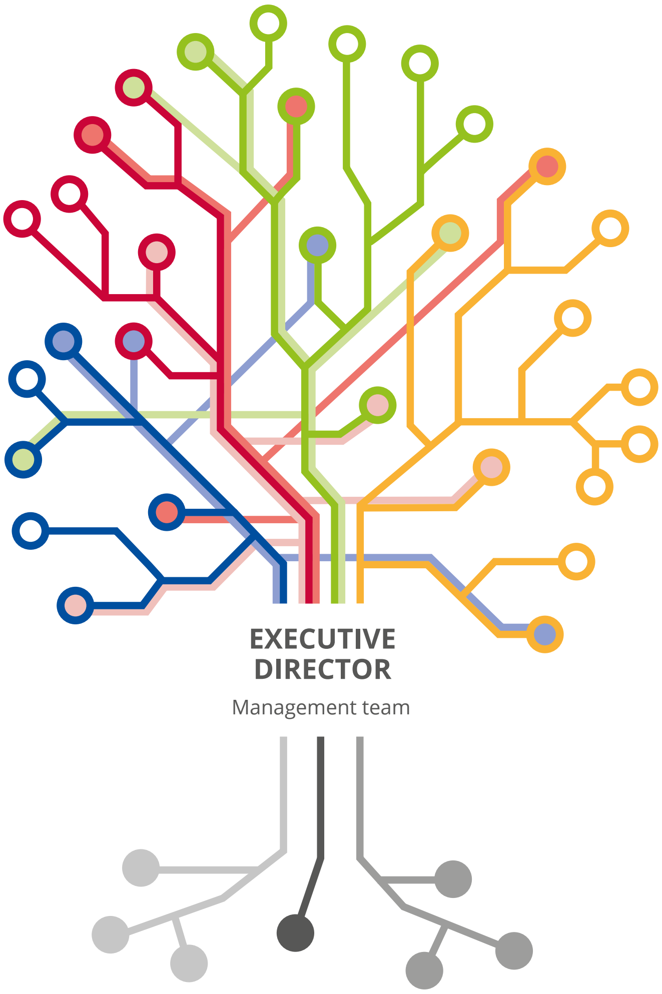
Target groups and beneficiaries

- ENISA staff members and employees.

A

ANNEX 1

ORGANISATION CHART AS OF 1 JANUARY 2021



○ **POLICY DEVELOPMENT AND IMPLEMENTATION UNIT**

○ **MARKET, CERTIFICATION AND STANDARDISATION UNIT**

○ **CAPACITY BUILDING UNIT**

○ **OPERATIONAL COOPERATION UNIT**

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

● **ACCOUNTANT**

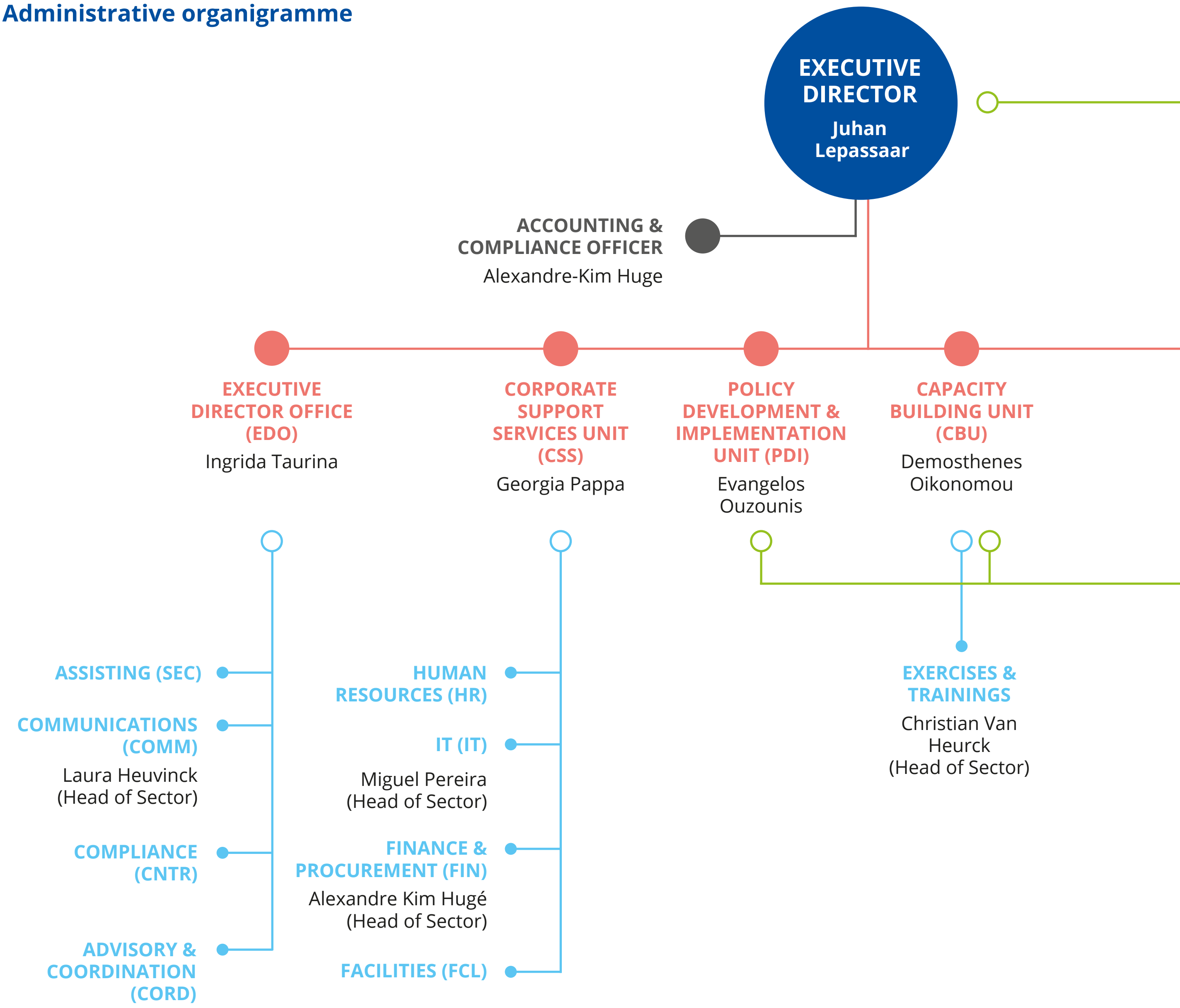
● **EXECUTIVE DIRECTOR'S OFFICE**

Communication
Coordination
Internal Control & Compliance
Administration

● **CORPORATE SUPPORT SERVICES**

Human Resources
Finance
Procurement
IT services

Administrative organigramme



EXECUTIVE DIRECTOR
Juhan Lepassaar

ACCOUNTING & COMPLIANCE OFFICER
Alexandre-Kim Huge

EXECUTIVE DIRECTOR OFFICE (EDO)
Ingrida Taurina

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

CORPORATE SUPPORT SERVICES UNIT (CSS)
Georgia Pappa

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

POLICY DEVELOPMENT & IMPLEMENTATION UNIT (PDI)
Evangelos Ouzounis

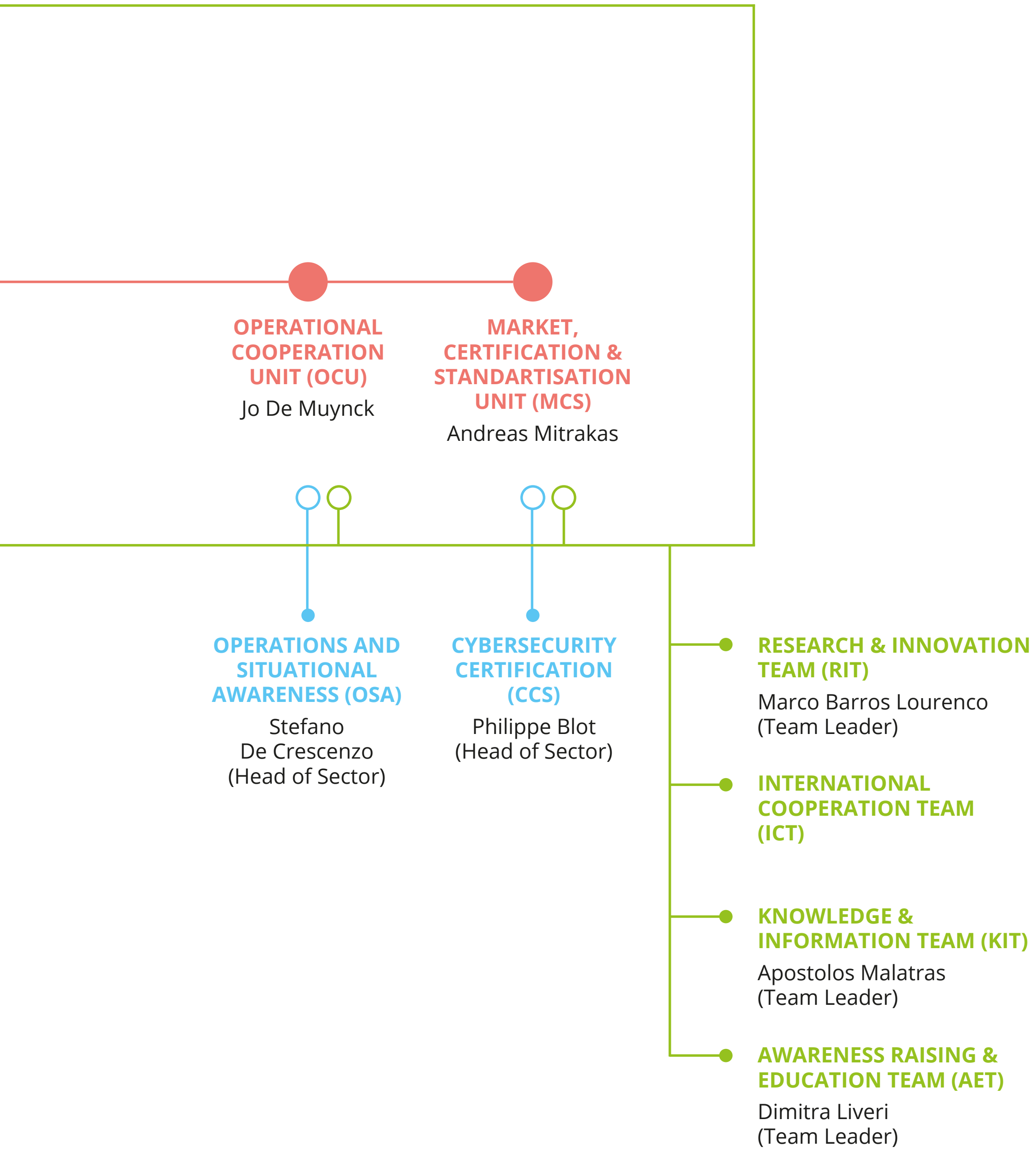
CAPACITY BUILDING UNIT (CBU)
Demosthenes Oikonomou

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

- ● 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 01. 09. 2021

ED*		EDO		CSS		PDI		CBU		OCU	
AD	2	AD	9	AD	3	AD	11	AD	7	AD	8
Total	**2**	AST	8	AST	6	AST	0	AST	2	AST	0
		CA	2	CA	10	CA	5	CA	5	CA	2,5
* ED and accountant		SNE	0	SNE	0	SNE	2	SNE	1	SNE	2
		Total	**19**	**Total**	**19**	**Total**	**18**	**Total**	**15**	**Total**	**12,5**



OPERATIONAL COOPERATION UNIT (OCU)
Jo De Muynck

MARKET, CERTIFICATION & STANDARTISATION UNIT (MCS)
Andreas Mitrakas

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

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

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

INTERNATIONAL COOPERATION TEAM (ICT)

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

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

MCS	
AD	14
AST	0
CA	2,5
SNE	2
Total	**18,5**

SUMMARY	
AD	**54**
AST	**16**
CA	**27**
SNE	**7**
Total	**104**

ANNEX 2
RESOURCE ALLOCATION PER ACTIVITY 2022–2024

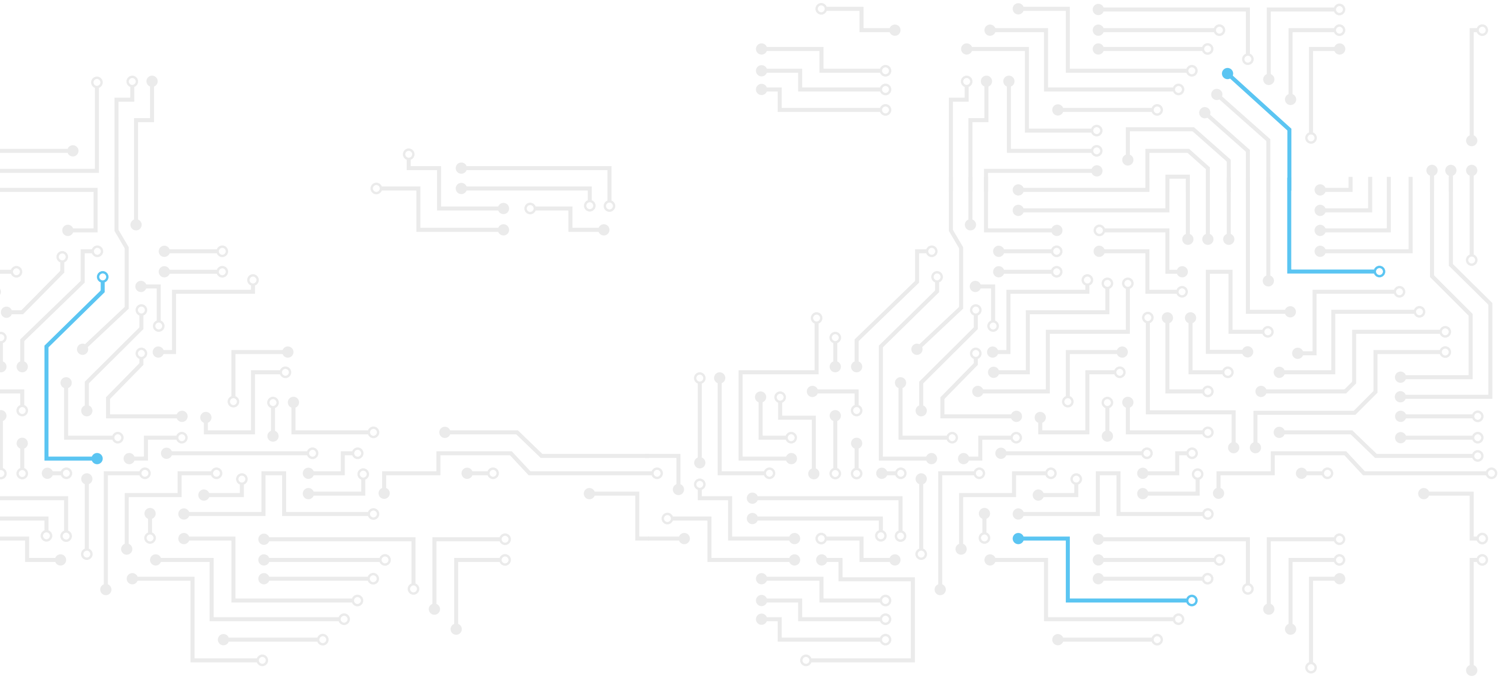
The indicative allocation of the total 2022 financial and human resources following the activities as described in Section 3.1 'Operational activities' and the corporate activities as described in Section 3.2 'Corporate activities' are presented in the table below. The allocation specifies direct budgets and FTEs for each activity, with indirect budgets being assigned based on causal relationships.

The following assumptions are used in the simplified activity-based budgeting methodology.

- The direct budget is the cost estimate of each of the nine operational activities and two corporate activities as indicated in Section 3 of this 2022–2024 SPD in terms of goods and services to be procured.
- The indirect budget is the cost estimate of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs attributable to each activity. The indirect budget is allocated to activities based on different drivers. The main driver for cost allocation was number of foreseen FTEs for each activity in 2022.
- The allocation of five additional FTEs and EUR 610 000 from the proposed NIS2 directive will be allocated in due course in accordance with the final agreement of the regulators and once the tasks have been finalised.

Table 4.

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES (2022)	Activities as referred to in Section 3	Direct and indirect budget allocation (EUR)	FTE allocation
Providing assistance on policy development	Activity 1	1 034 117	6
Supporting implementation of Union policy and law	Activity 2	2 140 710	12
Building capacity	Activity 3	3 395 444	13
Enabling operational cooperation	Activity 4	2 852 015	10
Contribute to cooperative response at Union and Member States level	Activity 5	1 749 460	8
Development and maintenance of EU cybersecurity certification framework	Activity 6	2 367 985	11
Supporting European cybersecurity market and industry	Activity 7	1 268 623	8
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	2 282 332	10
Outreach and education	Activity 9	999 165	5
Performance and risk management	Activity 10	2 395 205	19
Staff development and working environment	Activity 11	3 112 569	19
TOTAL		**23 597 625**[28]	**121**[29]



[28] EUR 610 000 foreseen under the NIS directive will be allocated to activities in due course and in accordance with the final agreement of regulators, including the finalised tasks.

[29] Five FTEs as per the NIS directive will be allocated to activities in due course and in accordance with the final agreement of regulators, once the tasks have been finalised.

ANNEX 3
FINANCIAL RESOURCES 2022–2024

Table 5. **Revenue**

Revenue	2020 executed budget	2021 revenue estimated by the Agency	2022 as requested by the Agency	VAR 2022 / 2021	Envisaged 2023	Envisaged 2024
1. Revenue from fees and charges						
2. EU contribution	20 646 000	22 248 000	23 633 000	6%	24 110 000	24 610 000
– of which assigned revenues deriving from previous years' surpluses **	-110 505.47					
– of which Reserve conditional to approval of NIS2 Directive			610 000		610 000	610 000
3. Non-EU countries' contribution (including EEA/EFTA and candidate countries)	503 120	585 060	574 625	-2%	597 182	609 888
– of which EEA/EFTA (excl. Switzerland)	503 120	585 060	574 625	-2%	597 182	609 888
– of which Candidate Countries						
4. Other contributions	533 764	640 000	*	N/A		
5. Administrative operations						
– of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6. Revenues from services rendered against payment						
7. Correction of budgetary imbalances						
TOTAL REVENUES	**21 682 884**	**23 473 060**	**24 207 625**	**3%**	**24 707 182**	**25 219 888**

* Due to move to a new building, it is expected that Hellenic Authorities will make rental payments directly to the building owner, therefore no subsidy will be paid to ENISA

Table 6. Expenditure

Expenditure (EUR)	2021		2022	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	10 775 409	10 775 409	12 494 335	12 494 335
Title 2	3 547 651	3 547 651	2 824 300	2 824 300
Title 3	9 150 000	9 150 000	8 888 990	8 888 990
Total expenditure	**23 473 060**	**23 473 060**	**24 207 625**	**24 207 625**

* As adopted in the amending budget 1/2020 (management board decision MB/2020/18).

Table 7. Expenditure details

Expenditure (EUR)	Commitment and Payment appropriations					
	Executed budget 2020	Budget 2021	Draft Budget 2022 Agency request	VAR 2022 / 2021	Envisaged in 2023	Envisaged in 2024
Title 1. Staff Expenditure	**11 203 334**	**10 775 409**	**12 494 335**	**16%**	**12 740 555**	**12 998 652**
11 Staff in active employment *	7 126 084	8 810 319	10 837 880	23%	11 049 781	11 271 904
12 Recruitment expenditure	704 686	410 087	412 000	0%	420 536	429 483
13 Socio-medical services and training	375 738	1 084 064	853 000	-21%	870 672	889 197
14 Temporary assistance	2 996 826	470 939	391 455	-17%	399 565	408 067
Title 2. Building, equipment and miscellaneous expenditure	**3 150 568**	**3 547 651**	**2 824 300**	**-20%**	**2 882 814**	**2 944 150**
20 Building and associated costs	929 820	1 404 608	914 550	-35%	933 498	953 359
21 Movable property and associated costs	54 074	99 000	160 000	62%	163 315	166 790
22 Current corporate expenditure	98 702	798 696	320 000	-60%	326 630	333 579
23 Corporate ICT	2 067 972	1 245 347	1 429 750	15%	1 459 372	1 490 422
Title 3. Operational expenditure	**7 328 981**	**9 150 000**	**8 888 990**	**-3%**	**9 083 813**	**9 277 086**
30 Activities related to meetings and missions	628 966	650 000	387 000	-40%	395 018	403 423
32 Horizontal operational activities	1 517 962	0	0		0	0
36/37 Core operational activities	5 182 053	8 500 000	8 501 990	0%	8 688 795	8 873 663
TOTAL EXPENDITURE	**21 682 884**	**23 473 060**	**24 207 625**	**3%**	**24 707 182**	**25 219 888**

* For years 2022-2024 chapter 11 includes an amount of EUR 610 thousand as a reserve conditional to approval of NIS Directive (for salaries of new posts)

Table 8. Budget out-turn and cancellation of appropriations

Budget out-turn	2018	2019	2020
Revenue actually received (+)	11 572 995	16 740 086	21 801 460
Payments made (–)	– 10 345 736	– 11 980 352	– 15 050 421
Carry-over of appropriations (–)	– 1 348 657	– 4 357 734	– 6 200 614
Cancellation of appropriations carried over (+)	108 302	62 522	180 023
Adjustment for carry-over of assigned revenue appropriations carried over (+)	124 290	116 393	10 403
Exchange rate difference (+/–)	– 689	– 1 802	– 1 291
Adjustment for negative balance from previous year (–)	—	—	—
Total	**110 505**	**579 113**	**739 560**

CANCELLATION OF APPROPRIATIONS

- Cancellation of commitment appropriations

In 2020, C1 commitment appropriations were cancelled at a cost of EUR 560 800, representing 3 % of the total budget. ENISA demonstrates a commitment rate of 97 % of C1 appropriations for 2020 at the year-end (31 December). The consumption of the 2020 budget at year-end shows the capacity of the Agency to fully implement its annual appropriations. The payment rate reached 69 %, and the amount carried forward to 2021 was EUR 6 074 991, representing 29 % of total C1 appropriations in 2020.

- Cancellation of payment appropriations for the year

No payment appropriations were cancelled during 2020.

- Cancellation of payment appropriations carried over

(Fund source: 'C8' – appropriations carried over automatically from 2019 to 2020.)

The appropriations of 2019 carried over to 2020 were utilised at a rate of 96 % (automatic carry-overs), which indicates a satisfactory capability of estimation of needs. From the amount of EUR 4 347 332 carried forward, EUR 180 024 was cancelled, mostly due to the circumstances caused by COVID-19. This cancellation represents 0.7 % of the total budget for 2020 (fund sources: C1 and C8).

ANNEX 4

HUMAN RESOURCES – QUANTITATIVE

Overview of all categories of staff and staff evolution

Staff policy plan for 2022–2024

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

(a) Statutory staff and SNEs

Staff	2021			2021	2022	2023	2024
Establishment plan posts	**Authorised budget**	**Actually filled as of 1 September 2021**	**Occupancy rate (%)**	**Authorised**	**Authorised[30]**	**Envisaged staff**	**Envisaged staff**
Administrators (ADs)	57	54[31]	95	57	63[32]	63	63
Assistants (ASTs)	19	17[33]	89	19	19	19	19
Assistants/secretaries (ASTs/SCs)							
Total establishment plan posts	76	71	93	76	82	82	82
External staff	**FTEs corresponding to the 2021 authorised budget**	**Active FTEs as of 1 September 2021**	**Execution rate (%)**	**FTEs corresponding to the authorised budget**	**Envisaged FTEs**	**Envisaged FTEs**	**Envisaged FTEs**
CAs	30	27	90	30	32[34]	32*	32*
SNEs	12	9[35]	75	12	12	12	12
Total external staff	**42**	**49**	**N/A**	**42**	**44**	**44**	**44**
TOTAL STAFF[36]	**118**	**107**	**91**	**118**	**126[37]**	**126**	**126**

[30] Pending approval of the NIS directive and request for additional SNE posts subject to the approval procedure of the co-legislators.

[31] Total AD includes 54 AD posts actually filled by 15 November 2021. Date of reference for the figures: 16 September 2021.

[32] An additional three TA posts for implementation of the NIS2 proposal directive.

[33] Total AST includes 17 AST posts actually filled by 1 October 2021. Date of reference for the figures: 16 September 2021.

[34] An additional two CA posts for implementation of the NIS2 proposal.

[35] Total SNE includes nine SNE posts filled by 1 November 2021. Data of reference: 16 September 2021.

[36] Refers to TA, CA and SNE figures.

[37] This includes the additional five full-time equivalents (three temporary agent and two contract agent posts), as specified in the legislative financial statement accompanying the proposal for a directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (COM 2020/823). These resources should be managed as reserves that the Agency can draw on following the adoption of the final EU budget.

Table 10. (b) Final statutory staff as of year-end (31 December 2020)

Staff	2020		
Establishment plan posts	Authorised budget	Actually filled as of 31 December 2020	Occupancy rate (%)
ADs	51	47[38]	92
ASTs	18	15	83
ASTs/SCs			
Total establishment plan posts	69	62	90
External staff	FTEs corresponding to the authorised budget	Active FTEs as of 31 December 2020	Execution rate (%)
CAs	30	29[39]	97
SNEs	12	8	67
Total external staff	**42**	**37**	**100**
TOTAL STAFF (TAs,CAs,SNEs)	**111**	**130**	**100**

Table 11. (c) Additional external staff expected to be financed from grant, contribution or service-level agreements

Human resources	2021	2022	2023	2024
	Envisaged FTEs	Envisaged FTEs	Envisaged FTEs	Envisaged FTEs
Contract agents	N/A	N/A	N/A	N/A
SNEs	N/A	N/A	N/A	N/A
TOTAL	N/A	N/A	N/A	N/A

Table 12. (c) Other human resources

- Structural service providers

	Actually in place as of 31 December 2020	Actually in place as of 1 September 2021
Security	5	5
IT	4	5

Table 13.

- Interim workers

	Actually in place as of 31 December 2020	Actually in place as of 1 September 2021
Number	31	13

[38] Total number includes the in-house AD staff as of 31 December 2020 and nine AD offers sent and accepted by 31 December 2020.

[39] Total number includes the in-house CA staff as of 31 December 2020 and three CA offers sent and accepted by 31 December 2020.

Table 14. Multiannual staff policy plan for 2020–2024[40]

Function group and grade	2020				2021				2022		2023		2024	
	Authorised budget		Actually filled as of 31 December [41]		Authorised budget		Actually filled as of 1 September 2021[42]		Authorised		Envisaged		Envisaged	
	PP	TP	PP	TP	PP	TP	PP	TP	PP	TP	PP	TP	PP	TP
AD 16														
AD 15		1				1				1		1		1
AD 14				1				1						
AD 13						1				2		2		2
AD 12		6		6		5		6		4		4		4
AD 11						2				2		2		2
AD 10		5		3		3		3		4		4		4
AD 9		12		7		12		9		11		11		11
AD 8		19		10		21		10		22		23		23
AD 7				11		8		12		8		10		10
AD 6				9		4		13		9		6		6
AD 5														
AD total		43		47		57		54		63		63		63
AST 11														
AST 10														
AST 9														
AST 8						1				2		2		2
AST 7		3		3		4		3		3		3		3
AST 6		7		1		8		2		8		8		8
AST 5		5		5		5		5		5		5		5
AST 4		1		3		1		4		1		1		1
AST 3				2				2						
AST 2				1				1						
AST 1														
AST total		16		15		19		17		19		19		19
AST/SC 6														
AST/SC 5														
AST/SC 4														
AST/SC 3														
AST/SC 2														
AST/SC 1														
AST/SC total														
Grand total	**59**		**62**		**76**		**71**		**82**		**82**		**82**	

PP: Permanent Posts, TP: Temporary posts

[40] The change in the number of establishment plan up to 10 % requested for 2022 is modified as per Article 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.

[41] Total number includes the in-house AD staff as of 31 December 2020 and nine AD offers sent and accepted by 31 December 2020. Data are available as of 1 January 2021 and refer to the taken-up duties.

[42] The figures include actually filled posts as of 15 November 2021. Date of reference for the figures: 16 September 2021.

Table 15. (b) External personnel

- Contract agents

Contract agents	FTEs corresponding to the 2020 authorised budget	Active FTEs as of 31 December 2020	Headcount as of 31 December 2020	FTEs corresponding to the 2021 authorised budget	Active FTEs as of 1 September 2021[43]	FTEs corresponding to the 2022 authorised budget	FTEs corresponding to the 2023 authorised budget	FTEs corresponding to the 2024 authorised budget
Function group IV	28	20[44]	20[45]	28	19	30[46]	30	30
Function group III	2	8	8	2	7	2	2	2
Function group II	0	0	0	0	0	0	0	0
Function group I	0	1	1	0	1	0	0	0
TOTAL	**30**	**29**	**29**	**30**	**27**	**32**	**32**	**32**

Table 16.

- Seconded national experts

SNEs	FTEs corresponding to the 2020 authorised budget	Active FTEs as of 31 December 2020	Headcount as of 31 December 2020	FTEs corresponding to the 2021 authorised budget	Active FTEs as of 1 September 2021 (47)	FTEs corresponding to the 2022 authorised budget	FTEs corresponding to the 2023 authorised budget	FTEs corresponding to the 2024 authorised budget
TOTAL	**12**	**8**	**8**	**12**	**9**	**12**	**12**	**12**

Table 17. 2022 recruitment forecasts following retirement/mobility or new requested posts (indicative table)

Job title in the agency	Type of contract (Official, TA or CA)		TA/Official		CA
			Function group / grade of recruitment internal (brackets) and external (single grade) foreseen for publication (*)		Recruitment function group (I, II, III and IV)
	Due to foreseen retirement/ mobility	New post requested due to additional tasks	Internal (brackets)	External (brackets)	
Experts		6 AD posts[48]	N/A	N/A	N/A
Officers		N/A	N/A	N/A	2[49]
Assistants		N/A	N/A	N/A	N/A

[43] Contract agents in-house as of 1 September 2021. Date of reference for the figures: 16 September 2021.

[44] Total number includes the in-house CA staff as of 31 December 2020 and three offers sent and accepted by 31 December 2020.

[45] Total number includes the in-house CA staff as of 31 December 2020 and three offers sent and accepted by 31 December 2020.

[46] This includes the additional two contract agent posts, as specified in the legislative financial statement accompanying the proposal for a directive revising Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (COM 2020/823). These resources should be managed as reserves that the Agency can draw on following the adoption of the final EU budget.

[47] In-house SNEs as of 1 October 2021. Data of reference: 16 September 2021.

[48] The total AD posts includes three AD posts already foreseen and the additional three new AD posts.

[49] New two CA posts, pending budget approval.

Table 18. 2021 recruitment exercise results for the TA, CA and manager call

Category		Number of eligible applications			Number of candidates put on reserve lists			Number of candidates recruited[50]		
Member State	Gender	TA call	CA call	Managers	TA call	CA call	Managers	TA call	CA call	Managers
Belgium	Male	13	2	5	2		1	1		1
	Female	9	4	1						
Bulgaria	Male	11	6	2	1					
	Female	17	5		1					
Czechia	Male	6	5	1						
	Female	1		2						
Denmark	Male	1								
	Female									
Germany	Male	16	2	4	2	1	1	1		
	Female	5	1	1						
Estonia	Male	7	3							
	Female	3								
Ireland	Male	7	2							
	Female	2								
Greece	Male	411	199	90	30	3		3	1	
	Female	254	182	42	9	4	1	2		1
Spain	Male	42	13	10	5		1	2		
	Female	19	12	1						
France	Male	25	8	8	1					
	Female	15	10	2	1			1		
Croatia	Male	4	3		1					
	Female	2	1	1						
Italy	Male	79	35	18	2	3	2		1	1
	Female	36	21	2	3	1			1	
Cyprus	Male	13	6	3						
	Female	7	5	4		1			1	
Latvia	Male	5								
	Female	3	4	2			1			1
Lithuania	Male	3								
	Female	3								

[50] The numbers include the offers sent and accepted as of 14 June 2021.

Category		Number of eligible applications			Number of candidates put on reserve lists			Number of candidates recruited[50]		
Member State	**Gender**	**TA call**	**CA call**	**Man-agers**	**TA call**	**CA call**	**Man-agers**	**TA call**	**CA call**	**Man-agers**
Luxembourg	Male	1	1							
	Female	1								
Hungary	Male	5	2	1						
	Female	3	2							
Malta	Male	3	1	2						
	Female	1								
Netherlands	Male	7	1	2	1			1		
	Female	2								
Austria	Male	6		2						
	Female	1		1						
Poland	Male	15	9	2		1			1	
	Female	11	7	1	1	1		1		
Portugal	Male	16	6	2	3		1	1		
	Female	7	1	1	1					
Romania	Male	24	8	3	3			2		
	Female	24	12	2	1			1		
Slovenia	Male	3	2	1						
	Female	4	3							
Slovakia	Male	2	2	1						
	Female	3	1							
Finland	Male	3	1	2						
	Female	6								
Sweden	Male	5	2	2						
	Female	1		5						

ANNEX 5
HUMAN RESOURCES – QUALITATIVE

A. RECRUITMENT POLICY

Table 19. Implementing rules in place

		Yes	No	If no, which other implementing rules are in place?
Engagement of CAs	Model Decision C(2019)3016	x		
Engagement of TAs	Model Decision C(2015)1509	x		
Middle management	Model Decision C(2018)2542	x		
Type of posts	Model Decision C(2018)8800		x	C(2013)8979

B. APPRAISAL AND RECLASSIFICATION/PROMOTIONS

Table 20. Implementing rules in place

		Yes	No	If no, which other implementing rules are in place?
Reclassification of TAs	Model Decision C(2015)9560	x		
Reclassification of CAs	Model Decision C(2015)9561	x		

Table 21. Reclassification of TAs / promotion of officials

Average seniority in the grade among reclassified staff							
Grades	**2016**	**2017**	**2018**	**2019**	**2020**	**Actual average over 5 years**	**Average over 5 years (according to decision C(2015)9563)**
AD 5	—	—	—	—	—	—	2.8
AD 6	1	1	2	3	—	3.7	2.8
AD 7	1	—	—	—	1	3	2.8
AD 8	1	1	1	—	2	6	3
AD 9	—	—	1	—	—	10	4
AD 10	—	—	—	—	—	—	4
AD 11	1	—	—	—	—	3	4
AD 12	—	—	—	—	—	—	6.7
AD 13	—	—	—	—	—	—	6.7
AST 1	—	—	—	—	—	—	3
AST 2	—	—	—	—	—	—	3
AST 3	1	1	1	—	—	4.42	3
AST 4	1	1	1	—	1	5.25	3
AST 5	1	—	1	—	—	5.5	4
AST 6	1	—	—	—	1	4	4
AST 7	—	—	—	—	—	—	4
AST 8	—	—	—	—	—	—	4
AST 9	—	—	—	—	—	—	N/A
AST 10 (senior assistant)	—	—	—	—	—	—	5
There are no AST/SCs at ENISA: N/A							
AST/SC 1							4
AST/SC 2							5
AST/SC 3							5.9
AST/SC 4							6.7
AST/SC 5							8.3

Table 22. Reclassification of contract staff

Function group	Grade	Active Staff as of 1 January 2019	Number of staff members reclassified in 2020	Average number of years in grade of reclassified staff members	Average number of years in grade for reclassified staff members according to decision c(2015)9561
CA IV	17	1	—	—	6–10
	16	0	—	—	5–7
	15	1	—	—	4–6
	14	9	—	—	3–5
	13	3	1	3.9	3–5
CA III	11	1	1	2	6–10
	10	5	1	3	5–7
	9	3	1	4.2	4–6
	8	0	0	—	3–5
CA II	6	—	—	—	6–10
	5	—	—	—	5–7
	4	—	—	—	3–5
CA I	3	1	—	—	N/A
	2	—	—	—	6–10
	1	—	—	—	3–5

C. GENDER REPRESENTATION

Table 23. Data on 1 September 2021 for statutory staff (only temporary agents and contract agents on 1 September 2021 and accepted offers and resignations up until and including 15 November 2021[51])

		Official		Temporary		Contract Agents		Grand Total	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	—	—	18	—	15	—	—	—
	Assistant level (AST and AST/SC)	—	—	11	—	—	—	—	—
	Total	—	—	29	66	15	34	44	44.9
Male	Administrator level	—	—	36	—	12	—	—	—
	Assistant level (AST and AST/SC)	—	—	6	—	—	—	—	—
	Total	—	—	42	77.8	12	22.2	54	55.1
Grand total		—	—	71	72.5	27	27.5	98	100

[51] Date of reference for the figures: 16 September 2021.

Table 24. Data on 31 December 2020 for statutory staff (only temporary agents and contract agents, including last entry into service on 16 December 2020)

		Official		Temporary		Contract Agents		Grand Total	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	—	—	11	—	15	—	—	—
	Assistant level (AST and AST/SC)	—	—	10	—	—	—	—	—
	Total	—	—	21	58	15	42	36	46
Male	Administrator level	—	—	27	—	11	—	—	—
	Assistant level (AST and AST/SC)	—	—	5	—	—	—	—	—
	Total	—	—	32	74	11	26	43	54
Grand total		—	—	53	67	26	33	79	100

Table 25. Data regarding gender evolution over 5 years for middle and senior management (1 September 2021 and accepted offers up until and including 16 October 2021)[52]

	2016		1 September 2021	
	Number	%	Number	%
Female managers	0	0	3	33.3
Male managers	10	100	6 (53)	66.7

The focus of the Agency being cybersecurity is likely to be a factor in the gender imbalance. Nevertheless, an improvement has been noted during the past 5 years. Continuous efforts to encourage female involvement in this domain have been fruitful; however, further efforts should be planned to achieve a higher percentage of female middle and senior managers at ENISA in the coming years.

[52] Date of reference for the figures: 16 September 2021.

[53] This category comprises heads of unit and team leaders.

D. GEOGRAPHICAL BALANCE

Table 26. Provisional data on 1 September 2021 – statutory staff only (TAs, CAs and accepted offers and resignations up until and including 15 November 2021)[54]

Nationality	ADs and CAs (Function Group IV)		AST/SCs, ASTs and CAs (FG I/II/III)		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	6.8	2	8	7	7.1
BG	2	2.74	—	—	2	2
CZ	1	1.37	—	—	1	1
DE	2	2.74	—	—	2	2
EE	1	1.37	—	—	1	1
EL	26	35.6	12	48	38	38.8
ES	3	4.2	1	4	4	4.1
FR	3	4.2	1	4	4	4.1
IT	5	6.8	—	—	5	5.1
CY	1	1.37	2	8	3	3
LV	2	2.74	—	—	2	2
LT	—	—	1	4	1	1
NL	3	4.2	—	—	3	3
PL	3	4.2	1	4	4	4.1
PT	3	4.2	1	4	4	4.1
RO	7	9.6	0	0	7	7.1
SK	—	—	1	4	1	1
SE	2	2.74	—	—	2	2
Double[a]	4	5.5	3	12	7	7.1
TOTAL	**73**	**74.5**	**25**	**25.5**	**98**	**100**

[a] 'Double' nationality refers to staff members who have dual nationality (other EU and non-EU nationalities) (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek).

[54] Date of reference for the figures: 16 September 2021.

Table 27. Evolution over 5 years of the most represented nationality in the Agency

Most represented nationality	2016		1 September 2021	
	Number	%	Number	%
Greek	27 (out of 68)	39.7	38 (out of 98)	38.8

Looking back to 2020, it has been noted that the positive measures to improve the diversity of nationalities that had been implemented in 2019 and 2020 have been fruitful. The most represented nationality has seen a decrease of 1 % over the past 5 years. This can be attributed to the broad outreach campaigns on popular media across the EU, closer consideration of the nationality spread in relation to competencies requested, and the continuation of specific provisions in recruitment [55].

E. LOCAL OFFICE IN BRUSSELS, BELGIUM

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

The main approval steps were:

- the June 2020 Management Board meeting gave the ED prior consent to proceed with the establishment preparations;
- Greek (January 2021) and Belgian (August 2020) authorities gave their positive opinion;
- in June 2021, Commission adopted Decision C(2021)4626 of 23 June 2021, giving its prior consent;
- in July 2021, ENISA's Management Board confirmed the establishment of the office.

Table 28. Indicative resources foreseen

Resources (indicative)	2021	2022	2023	2024
Headcount (FTEs)	2–3	4–7	4–10	4–10
Budget (one-off and maintenance costs) (EUR)	25 000	500 000	170 000	170 000

The practical preperations for the Brussels local office are at an advanced stage.

[55] The seeming imbalance related to the most represented nationality among ENISA staff is related to several factors, such as the level of posts and related salaries, which may be perceived as less appealing for job seekers in relatively more advanced Member State economies; the fact that ENISA has a better position as an employer compared with average conditions offered in the Greek job market; the small job market in Greece for cybersecurity professionals. Other reasons that may be cited are the need for stability during the start-up phase of the Agency, as staff from the hosting Member State (Greece) were considered less likely to resign (resulting in lower turnover), which in combination with the comparatively young age of the Agency, still has its original impact; the relatively better academic profile of Greek candidates appropriate for lower-level posts; the relatively lower payroll cost for staff that are relatively better qualified than average while costing less if expatriation allowance is considered; and the general predisposition to retain a lower-level position in the home country.

F. SCHOOLING

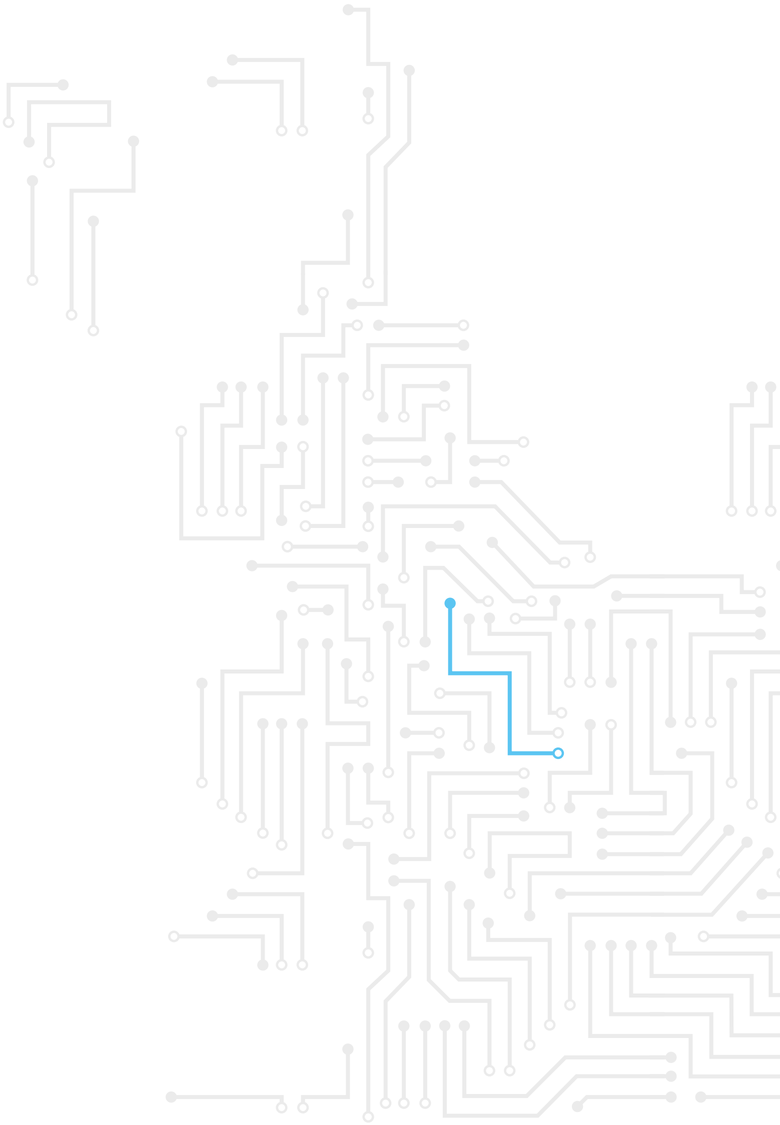
Table 29.

Agreement in place with the School of European Education of Heraklion	
Contribution agreements signed with the Commission on type I European schools	No
Contribution agreements signed with the Commission on type II European schools	Yes
Number of service contracts in place with international schools	For the 2021–2022 school year, the process for the financial support for the staff of ENISA in relation to the cost of schooling has been updated by the 2021/41 Executive Director Decision, leading to the abolishment of service-level agreements (SLAs)

ANNEX 6

ENVIRONMENT MANAGEMENT

This will depend on the new headquarters building; however, ENISA is looking into opportunities to strengthen its environmental management. A new objective has been introduced in 2022 to carry out an overarching audit of the CO2 impact of all operations of the Agency and to develop and implement a targeted action plan. The objective of this undertaking is for the Agency to achieve climate neutrality by 2030.



ANNEX 7
BUILDING POLICY

In 2021, ENISA relocated to a new headquarters building in Athens, Greece. The building policy will be developed in the course of 2022.

ANNEX 8

PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education/day care
In accordance with Article 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the EU annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 4 October 2019 and is applicable to ENISA and its staff.	In accordance with Article 35 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the EU annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement on 13 November 2018, which was ratified by Greek Law 4627/2019 on 25 September 2019 and entered into force on 4 October 2019 and is applicable to ENISA and its staff.	A public School of European Education, type II, was founded in 2005 by the Greek Government in Heraklion, Crete, for the children of ENISA staff. There is no European School operating in Athens.

ANNEX 9
EVALUATIONS

External consultants are contracted to carry out annual ex post evaluations of operational activities. The scope of the evaluation focuses on ENISA's operational activities. The overall aim of the annual evaluations is to evaluate the effectiveness, efficiency, coherence and relevance.

The consulted stakeholders generally agree that ENISA is the only entity that could achieve such results, is seen as a key enabler of knowledge, experience and expertise, and enables the creation of a strong cybersecurity community. The evaluation also revealed that ENISA is perceived as a strong and credible partner at EU level and its activities are seen as pertinent for Member States. The report therefore concludes on an extremely positive note, acknowledging the added value of ENISA's activities for the whole EU.

The ex ante evaluation included desk research and interviews with key ENISA stakeholders. It concluded that given the restructuring of the 2021–2023 programming document, the structure of ENISA's SPD would not require any changes, but it was recommended that certain outputs should be strengthened with a specific focus on the following areas:

- a proactive shaping of the political agenda;
- developing a transversal focus on digital strategic autonomy and its implications for cybersecurity;
- reinforcing the cooperative response by an insight-driven approach;
- focusing on stakeholder management, awareness raising and activities targeting industry.

ENISA uses an internal monitoring system that is intended to support the project management function, which includes the project delivery and resources allocation. The regular reporting and the ENISA management team use this information for managerial purposes. Moreover, ENISA has implemented a mid-term review procedure and regular weekly management team meetings. ENISA has undertaken a study to upgrade the use of electronic tools in the internal project management and overall delivery of the Agency work programme.

ANNEX 10

STRATEGY FOR ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The Agency's strategy for an effective internal control system is based on international best practices and on the internal control framework (the committee of sponsoring organization framework's international standards).

The control environment is the set of standards of conduct, processes and structures that provide the basis for carrying out internal control across ENISA. The Management Team set the tone from the outset with respect to the importance of the internal control, including expected standards of conduct.

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

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

Information is necessary for the organisation 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 specific Agency stakeholders and, more widely, EU citizens with information on ENISA's policy, objectives, actions and achievements. Internal communication provides ENISA staff with the information required to support the achievement of objectives and the awareness for day-to-day controls.

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

The Common Approach on EU Decentralised Agencies foresees that EU agencies should be more active concerning fraud prevention issues and that the related communication forms an essential part of its success. In order to implement this, the European Anti-Fraud Office recommended that each agency should adopt an anti-fraud strategy that is proportionate to its fraud risks. Rules for the prevention and management of conflicts of interest are part of the anti-fraud strategy of the Agency.

ANNEX 11
GRANTS, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS

ENISA does not receive any form of grant.

The table below provides a summary of the SLAs and other agreements of the Agency, including contracted amounts where necessary.

Table 30.

Title	Type	Contractor	Contracted amount (EUR)
10th amendment of SLA with CERT-EU-001-00	SLA	European Commission	24 480 00
Global SLA with DIGIT	SLA	European Commission	
SLA for provision of electronic data back up services with BEREC	SLA	Office of the Body of European Regulators for Electronic Communications (BEREC office)	
SLA and SDA with DG BUDG – Implementation and usage of ABAC System	SLA	DG BUDG European Commission	46 000 00
SLA for Shared Support Office (SSO)_EUAN	SLA	European Food Safety Authority	2 828 17
SLA with Cedefop	SLA	Cedefop	
SLA with DG HR	SLA	European Commission	
SLA with European Union Aviation Safety Agency – Permanent Secretariat	SLA	European Union Aviation Safety Agency	
SLA with EPSO and EUSA (updated)	SLA	European Personnel Selection Office	
SLA with European Administrative School	SLA	European Administrative School	
SLA with Office for Official Publications of the European Communities	SLA	Publications Office of the EU	
SLA with PMO	SLA	PMO	
Agreement on strategic co-operation with Europol	Agreement	Europol	
Agreement with Hellenic Postal Services A.E. – Athens office	Agreement	Ellinika Tachydromeia Elta Ae	50 per month

Title	Type	Contractor	Contracted amount (EUR)
Agreement with Hellenic Postal Services A.E. – Heraklion office	Agreement	Ellinika Tachydromeia Elta Ae	80 per month
Agreement with Translation Centre for the Bodies of the EU	Agreement	Translation Centre for the Bodies of the European Union	
Austrian signature scheme for e-card and mobile signature_A-Trust	Agreement	A-Trust Gesellschaft für Sicherheitssysteme im Elektronischen Datenverkehr GMBH	
Collaboration agreement in the field of standardisation	Agreement	European Committee for Standardization and European Committee for Electrotechnical Standardization	
Cooperation agreement between ETSI and ENISA	Agreement	ETSI	
Cooperation plan 2021–2023 between eu-LISA and ENISA	Agreement	eu-LISA	
Joint ENISA–Europol / European Cybercrime Centre (EC3) Working Group on Security and Safety Online	Agreement	Europol	
Lease agreement Athens office	Agreement	Prodea Investments	
Maintenance agreement for franking machines	Agreement	Papakosmas Ntatatechnika EPE	57 per month
Mandate and service agreement for 'Type II European School' with Commission	Agreement	Directorate-General for Human Resources and Security	
Mission Charter of the IAS_REVISED	Agreement	Internal Audit Service	
Non-Disclosure Agreement CT1607860_ Confidential and proprietary document between 12 parties	Agreement		
Provision of water fountain and water bottles for Athens office	Agreement	Efodiastiki Katalanotiki Agathon EPE	6/pc
Cooperation agreement with FORTH	MoU	Foundation for Research and Technology Hellas	
Cooperation between European Defence Agency and ENISA	MoU	European Defence Agency	
MoU on bilateral cooperation with EUIPO	MoU	European Union Intellectual Property Office	16 803 58
MoU with Universität der Bundeswehr München	MoU	Bundeswehr University Munich	
Structured cooperation between ENISA and CERT-EU	MoU	CERT-EU	
Working arrangement agreement with eu-LISA	MoU	eu-LISA	

ANNEX 12

INTERNATIONAL STRATEGY OF THE EU AGENCY FOR CYBERSECURITY

1. INTRODUCTION

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

1.2. Article 42 of the CSA requires the Management Board of ENISA to adopt 'a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent' [56]. The CSA also refers to specific international organisations (e.g. Organisation for Economic Co-operation and Development (OECD), Organization for Security and Co-operation in Europe (OSCE) and North Atlantic Treaty Organisation (NATO)) that ENISA is called to develop relations with (see recital 43).

1.3. Since the entry into force of the CSA, ENISA's exposure to partners outside the EU has increased both quantitatively and qualitatively[57]. ENISA is also often approached by third countries directly with high expectations of mutual collaboration, and is confronted each time on how best to react. Such welcomed developments call for a more strategic approach to the international dimension of ENISA's work in order to guide the engagement of the Agency with third country partners, as well to direct Agency's response to third country partners seeking cooperation with ENISA.

1.4. This international strategy covers the cooperation with international organisations and with non-EU countries. However, for those non-EU countries or regions with which the EU has special agreements this international strategy should be read in the light of such agreements, looking at where a closer cooperation in the area of cybersecurity is foreseen.

[56] Chapter II of Title II of the CSA covers all tasks of ENISA and thus outlines areas in which ENISA is competent.

[57] The expectations of various actors inside the EU institutions and of Member States for ENISA to engage more actively internationally have increased, as was stressed in the bilateral interviews undertaken by ENISA in spring 2021. This was also confirmed in the internal survey carried out by ENISA in early 2021.

2. ENISA’S OVERALL INTERNATIONAL APPROACH

The directions and provisions in this strategy will not in any way limit or hamper the provisions laid out by Article 12 of the CSA.

The mandate of the Agency is to achieve ‘a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity’. Under this mandate, ENISA’s strategic aim is to build a trusted and cybersecure Europe. ENISA’s international strategy must therefore be at the service of the Union, advance the achievement of the Agency’s mandate within the Union and contribute to its strategy[58].

This underlying premise directs the Agency to be **selective in engaging with international partners** and to limit its overall approach in international cooperation to only those areas and activities that will have high and measurable added value in achieving the Agency’s strategic objectives.

International cooperation should be resourced prudently and proportionally. This strategy outlines three approaches that the Agency can use in terms of level of commitment of resources: the **limited, assisting** and **outreach** approaches.

2.1. Limited approach

ENISA’s default international approach is ‘limited’. Under this approach, ENISA will, in line with its objectives enshrined in Article 4 of the CSA, exchange information with relevant international partners on an ad hoc basis[59], to strengthen and develop its expertise and anticipate changes prompted by global developments in cybersecurity. It will seek to promote the Union’s values and to advance its strategic objectives and cybersecurity policies when engaging with international partners in meetings, conferences and seminars. ENISA will not commit dedicated resources to pursue this approach beyond mission or conference costs.

2.2. Assisting approach

In line with its mandate to ‘actively support Member States, Union institutions, bodies, offices and agencies in improving cybersecurity’ (Article 3(1) of the CSA), ENISA may respond to requests for assistance – when the request is deemed to add significant value to a specific strategic objective and is in line with the Union’s policies – namely from third countries and international organisations with which the Union has agreements or frameworks that promote specific or general cooperation in cybersecurity. Under this approach, ENISA may exchange and share expertise, contribute to organising training sessions and exercises, support the Commission/EU in building and maintaining cybersecurity dialogues and support individual cybersecurity activities with international partners organised by the requester. To respond to such requests, ENISA might use resources dedicated to specific strategic objectives as set out in its single programming document (SPD).

[58] ENISA (2020), A Trusted and Cyber Secure Europe – ENISA strategy (https://www.enisa.europa.eu/publications/corporate-documents/enisa-strategy-a-trusted-and-cyber-secure-europe).

[59] For principles that govern selecting and engaging with international partners, please see Section 3 of this annex: ‘Principles governing ENISA’s international approach’.

2.3. Outreach approach

ENISA may follow an 'outreach' approach for specific aims and provisions of the strategic objectives outlined in this strategy, to proactively engage with specific international partners to be able to advance the Agency's strategic objectives and fulfil the objectives of the CSA. Under this approach, ENISA may plan dedicated resources in its SPD in pursuit of this approach.

3. PRINCIPLES GOVERNING ENISA'S INTERNATIONAL APPROACH

1. ENISA will focus its international cooperation on partners with which the Union has strategic economic relationships and which share the Union's values.

2. When cooperation in cybersecurity between the Union and an international partner is explicitly stated in an agreement, ENISA may follow an outreach approach, respecting the limits of the agreement provisions.

3. Beyond specific provisions outlined under Section 4 of this annex, 'Specific aims and provisions under individual strategic objectives', ENISA can, when relevant, pursue an outreach approach across all of its strategic objectives with European Economic Area countries.

4. ENISA will refrain from engaging with international actors if contacts or cooperation with such actors would be deemed incompatible with the Union's interests or policy goals.

5. The Agency's international cooperation activities should align with and add value to the partnerships of Member States.

6. When responding to requests under the assisting approach not explicitly covered in this strategy, and where otherwise appropriate, ENISA will consult and coordinate with the European External Action Service and the Commission, to ensure that the Agency's international engagement is in line with the Union's policy goals. ENISA will notify the Executive Board of requests under an assisting approach and those under an outreach approach. ENISA will furthermore ensure that its outreach activities are in line with the Union's policies by regularly consulting with the Directorate-General for Communications Networks, Content and Technology.

7. In its SPD, ENISA will proportionally evaluate the resources needed for involvement in any international activities with an assisting or outreach approach.

8. ENISA will seek endorsement of the Executive Board prior to developing cooperation frameworks or agreements with international organisations and third countries. When such agreements place financial or legal obligations on the Agency, they must be approved by the Management Board.

9. In its annual activity report, ENISA will outline all international activities it has pursued under different approaches. In particular, it will evaluate and provide assessment of the added value of international activities under an assisting or outreach approach in pursuit of its strategic objectives.

10. The Agency should be able to react in an agile manner while adhering to these principles.

4. SPECIFIC AIMS AND PROVISIONS UNDER INDIVIDUAL STRATEGIC OBJECTIVES

4.1. Strategic objective ‘Empowered and engaged communities across the cybersecurity ecosystem’

ENISA exchanges best practices and expertise and promotes international activities to enhance the cybersecurity awareness and education of the various communities of the Union. Furthermore:

- using the assisting approach, ENISA can give support in terms of expertise to the Western Balkans as a region and/or single countries of the region and to countries belonging to the European Eastern Partnership as a region and/or single countries of the region;
- using the outreach approach, and with the endorsement of the Management Board, ENISA can cooperate with third countries with which there are specific EU agreements to enhance mutual cybersecurity awareness and education in line with the respective specific provisions of such agreements.

4.2. Strategic objective ‘Cybersecurity as an integral part of EU policies’

ENISA collects and exchanges information on best practices in cybersecurity policy development and implementation internationally and promotes the projection of EU cybersecurity policies to the benefit of the Union. ENISA’s connections with international organisations working on digital security can both contribute to the promotion of EU *acquis* in this field and feed into EU cybersecurity policy development. Furthermore:

- using the assisting approach, ENISA can support Union representatives of relevant international organisations and regulatory forums by providing expertise on cybersecurity policies and cybersecurity aspects of Union legislation as outlined under Article 5 of the CSA;
- using the assisting approach, ENISA can provide expertise on cybersecurity policy implementation to the Western Balkans and Eastern Partnership countries;
- using the outreach approach, ENISA can cooperate with the OECD (and like-minded countries such as the Unites States) on mapping and promoting best practices in integrating cybersecurity into various policy domains.

4.3. Strategic objective ‘Effective cooperation among operational actors within the union in case of massive cyber incidents’

ENISA’s international cooperation should assist and contribute to the Union’s incident response and crisis management, in particular by building a trusted network of like-minded international partners – including major global cybersecurity companies and vendors – to contribute to the Union’s common situational awareness and preparedness. Furthermore, ENISA – in line with recital 43 of the CSA and using the outreach approach – can contribute to this by cooperating with international partners such as the OSCE and NATO on joint incident response coordination[60].

[60] Those activities are to be carried out in full respect of the principles of inclusiveness, reciprocity and the decision-making autonomy of the Union, without prejudice to the specific character of the security and defence policy of any Member State.

4.4. Strategic objective 'Cutting-edge competences and capabilities in cybersecurity across the Union'

ENISA will seek to reach out to international partners to exchange information and best practices in order to enhance and develop cybersecurity competences and capabilities within the Union. Where appropriate, it can participate as an observer in the organisation of international cybersecurity exercises in line with Article 12 of the CSA. Furthermore:

- using the assisting approach, ENISA can contribute to building competences and capabilities in the Western Balkans as a region and/or single countries by supporting training and exercises;
- using the assisting approach, ENISA can support, with relevant expertise, countries belonging to the Eastern Partnership as a region and/or single countries of the region or countries benefiting from the Union's development programmes;
- in line with recital 43 of the CSA and using the assisting approach, ENISA can contribute to the organisation of joint cybersecurity exercises with the OECD, the OSCE and NATO;
- under the outreach approach, ENISA can organise international cybersecurity challenges to promote and enhance the competitiveness of cybersecurity competences in the Union;
- using the outreach approach, and with the endorsement of the Management Board, ENISA can cooperate with third countries with which there are specific EU agreements to build and enhance mutual cybersecurity capacities in line with the respective specific provisions of such agreements.

4.5. Strategic objective 'A high level of trust in secure digital solutions'

Without prejudice to possible tasks stemming from Article 12(d) of the CSA, ENISA will seek to advance its expertise and monitor international developments in cybersecurity certification and related standardisation areas, also in line with Article 54 of the CSA[61]. It will engage with international actors on the supply and demand sides of the cybersecurity market to promote and advance European digital autonomy. Furthermore:

- using the outreach approach, ENISA will engage with the relevant key strategic economic partners of the Union to promote the EU's cybersecurity certification schemes or candidate schemes;
- using the outreach approach, and in line with recital 23 of the CSA, ENISA will support the global development and maintenance of standards that underpin the public core of the open internet and the stability and security of its functioning.

4.6. strategic objective 'Foresight on emerging and future cybersecurity challenges'

ENISA aims to exchange information on an ad hoc basis and participate in international forums to increase its expertise in international developments and map global cybersecurity threats as well as research areas and innovation trends that could address emerging challenges.

[61] Article 54 (elements of European cybersecurity certification schemes) of the CSA states that 'A European cybersecurity certification scheme shall include at least the following elements: […] (c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme; […] (o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels.'

4.7. Strategic objective ‘Efficient and effective cybersecurity information and knowledge management for Europe’

ENISA aims to gain a better overview and understanding of the international cybersecurity landscape and ensure that relevant cybersecurity information and knowledge generated internationally is shared and expanded within the EU cybersecurity ecosystem. ENISA will focus its outreach to partners deemed like-minded (e.g. Japan). Furthermore:

- using the outreach approach, ENISA will cooperate with the OECD and NATO in exchanging expertise for the development of cybersecurity indices and benchmarks;
- using the outreach approach, and with the endorsement of the Management Board, ENISA will cooperate with third countries with which there are specific EU agreements to enhance mutual knowledge and information in line with the respective specific provisions of such agreements.

ANNEX 13

ANNUAL COOPERATION PLAN 2022

This document is the draft 2022 annual cooperation plan for ENISA and CERT-EU, as foreseen in the co-signed MoU.

The plan aims to cover the cooperation activities planned for 2022.

The plan proposed in this document includes references to the activities included in the 2022 ENISA work programme, which has been submitted to the Management Board for approval.

In that regard, and because CERT-EU is in the process of drafting its annual programme for 2022, this plan should not be considered final.

In line with the 2021 annual cooperation plan, the proposed plan identifies actions in the following areas:

- capacity building, as referred to in Articles 6(c) and 6(i) of the CSA;
- operational cooperation, as referred to in Article 7 of the CSA;
- long-term strategic analyses of cyber threats, as foreseen in Article 9(b) of the CSA.

1. CAPACITY BUILDING

Capacity building[62] covers assistance to relevant public bodies to improve capabilities to respond to cyber threats and incidents as well as provision of cybersecurity training. Focus points of capacity building for the structured cooperation plan for 2022 remain maturity, training and exercises.

1.1. Maturity

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

In 2021, drawing on CERT-EU's and other CSIRTs Network and EU institutions', bodies' and agencies' stakeholders' experience and expertise, ENISA performed maturity-related activities targeting the CSIRTs Network to improve its members' capabilities for handling cyber incidents and EU institutions', bodies' and agencies' Blueprint[63] actors to assess their EU-level crisis management capabilities. This work is expected to result[64] in a new and updated methodology for performing maturity assessments.

In parallel, and with the help of ENISA, CERT-EU started developing a cybersecurity maturity assessment methodology for all EU institutions, bodies and agencies, in the context of the European Commission's upcoming proposal for a regulation on common binding cybersecurity rules for all EU institutions, bodies and agencies.

The plan for 2022 will focus on continuing the activities started in 2021, in particular the following.

- **EU institutions', bodies' and agencies' cyber hygiene.** CERT-EU will lead the activities of finalising the proposal for common binding cybersecurity rules regulation for all EU institutions, bodies and agencies and develop a cybersecurity maturity assessment methodology for all EU institutions, bodies and agencies.
- **CSIRT maturity.** ENISA will finalise the new proposed maturity framework for the CSIRTs Network and the maturity assessment methodology for EU-level crisis management. ENISA will foster the application of the methodologies to relevant subjects to help identify current abilities and gaps.

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

[62] As referred to in Articles 6(c) and 6(i) of the CSA.

[63] Commission Recommendation (EU) 2017/1584 (Blueprint).

[64] According to the 2021 annual cooperation plan, the work will be concluded by the end of 2021.

Objective	Task	Deliverable	Lead	2022 work programme
1. EU institutions', bodies' and agencies' cyber hygiene	ICDT TF1 common binding rules	Proposal for common binding cybersecurity rules regulation for all EU institutions, bodies and agencies	CERT-EU and EU Directorate-General for Informatics	To be decided
	Develop a cybersecurity maturity assessment methodology for all EU institutions, bodies and agencies	Cybersecurity maturity assessment methodology	CERT-EU	To be decided
2. CSIRT maturity	CSIRTs Network maturity – "SIM3" model	Finalisation of next-generation "SIM3" model, methodology and fostering its application across relevant subjects	ENISA	Activity 4: Enabling operational cooperation (output 4.1)
	Maturity assessment methodology for crisis management for the Blueprint stakeholders	Finalisation of the maturity assessment methodology for EU-level crisis management and fostering its application across relevant subjects	ENISA	Activity 4: Enabling operational cooperation (output 4.1)

1.2. Training and exercises

CERT-EU and ENISA have been efficiently cooperating for many years in the domain of training and exercises. This close cooperation will continue in 2022 and will be enhanced to the benefit of the cybersecurity community.

The proposed cooperation for 2022 will continue to combine 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 a state-of-the-art training portfolio that will be offered to Member States and EU institutions, bodies and agencies and to keep it up to date and relevant through close collaboration with CERT-EU and other key stakeholders.

Working methods already developed in 2021 will continue throughout 2022, with structured cooperation building on those (e.g. ENISA hosting CERT-EU training material and CERT-EU collaborating with ENISA when determining topics for working group training sessions).

The focus of 2022 will be to sustain ongoing activities (i.e. cyber exercises regularly organised by ENISA) and finalising activities started in 2021, particularly the following.

- **Custom technical courses.** Building on the activity in 2021, ENISA will work with CERT-EU and the CSIRTs Network Training Working Group to enhance training programmes based on audience knowledge level (e.g. elementary versus advanced).
- **Technical specialised workshop for CERT-EU constituents.** CERT-EU will further develop technical specialised workshops, leveraging, where relevant, the experience and working practice of ENISA.
- **Regular ENISA cybersecurity exercises.** This is an ongoing activity led by ENISA that materialises in several types of exercises involving different stakeholders. Through the structured cooperation, CERT-EU will be involved not only as a participant in relevant exercises, but also as a planner for selected exercises (e.g. Cyber Europe).

- **Joint exercises.** When relevant and in reference to the structured operational cooperation, ENISA and CERT-EU will join forces by participating in exercises alongside planners and a training audience. In addition, common operational activities (e.g. joint rapid reports) will be evaluated through these occasions.

Objective	Task	Deliverable	Lead	2022 work programme
1. Training	Custom technical courses	Continuous enhancement of training programme with elementary and advanced courses	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	To be decided
2. Exercises	ENISA exercises	Conduct cyber exercises	ENISA	Activity 3: Building capacity (output 3.2)
	Joint exercises	Perform joint exercises Incorporate lesson learnt in working practice	ENISA	Activity 3: Building capacity (output 3.2)

2. OPERATIONAL COOPERATION

2.1. Blueprint

As part of the efforts to further develop the Blueprint, both ENISA and CERT-EU will align actions on developing SOPs and improving common situational awareness.

The target for 2022 is to further expand on the cooperation activities started with the 2021 annual cooperation plan. In particular, the 2022 plan will still have SOPs and common situational awareness as key objectives of the cooperation.

- **Joint SOP for Blueprint stakeholders.** ENISA will continue leading at the operational layer whereas CERT-EU will continue leading at the technical level of the Blueprint. With the joint SOP document expected to be finalised during 2021, ENISA and CERT-EU will focus on further improving the SOP and testing the EU institutions', bodies' and agencies' SOPs through exercises.
- **Security incident response – continuous improvement.** CERT-EU will leverage the work on SOPs, lessons learnt in significant incidents and proceedings on the information exchange domain with ENISA and other Blueprint stakeholders to review and update its technical SOPs – security incident response process.
- **Common situational awareness.** As a result of the 2021 activities, both organisations have worked towards the establishment of a mechanism for information exchange at EU level, and set the stage for joint reports to raise awareness of significant cybersecurity events ([65]). Within the 2022 activity, ENISA and CERT-EU will further operationalise the mechanism, seeking additional opportunity for joint reports and using exercises to enhance the production of situational awareness deliverables.

[65] Cybersecurity 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.

Objective	Task	Deliverable	Lead	2022 work programme
1. SOPs	Enhance EU institutions', bodies' and agencies' SOPs Test SOP in a simulated scenario through exercise	Update joint SOP document Exercise read-out and lesson learnt from EU institutions', bodies' and agencies' SOPs	ENISA	Activity 4: Enabling operational cooperation (output 4.2)
	Review security incident response processes	SOP document	CERT-EU	To be decided
2. Common situational awareness	Operationalised common situational awareness	Production and operationalisation of the joint rapid report[66] Maintenance and enhancement of established information exchange mechanism and communication channels	ENISA	Activity 5: Contribute to cooperative response at Union and Member States levels (output 5.1)

2.2. Mutual assistance

As stated in Article 7 of the CSA, ENISA shall assist, at the request of one or more Member States, in assessing incidents with 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 2021, ENISA worked on establishing a mechanism supporting such assistance, including the development of necessary processes and procedures as well as the basis for a pool of experts. A similar mechanism has been established for EU institutions, bodies and agencies under the lead of CERT-EU, building on the major attacks paper (TF 03 18). This is combined with the aforementioned revision of the security incident response process.

The 2022 proposed plan aligns with the work done in 2021, and focuses on further enhancement and operationalisation of the provided mechanisms, in particular the following.

- **Cybersecurity assistance mechanism.** ENISA will continue focusing on the operationalisation of the assistance mechanism, by ensuring the adoption and endorsement of the mechanism by all involved actors, testing the mechanism in cooperation with Member States and further enhancing the effectiveness of the mechanism's SOPs.
- **Operational capability to assist EU institutions, bodies and agencies.** CERT-EU will continue managing the pool of experts and further enhance its operational capability.

[66] This is still in draft and the final name of the deliverable and service may change.

Objective	Task	Deliverable	Lead	2022 work programme
1. EU Member States	Operationalisation of the cybersecurity assistance mechanism	Finalisation and endorsement of the framework of delivering assistance, including processes, procedures and technical capability Execution of the scenario to test the mechanism's SOPs Management of a pool of experts	ENISA	Activity 5: Contribute to cooperative response at Union and Member States levels (output 5.2)
2. EU institutions, bodies and agencies	Operational capability to assist EU institutions, bodies and agencies	Management of a pool of experts from EU institutions, bodies and agencies	CERT-EU	To be decided

3. KNOWLEDGE AND INFORMATION SHARING

Knowledge and information sharing is a horizontal activity that nurtures and sustains the previous two pillars (capacity building and operational cooperation), as well as receiving input from them.

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, which provides an overview of threats, together with current and emerging trends. It is based on publicly available or voluntarily shared information and data, and provides an independent view on observed threats, threat agents and threat trends. CERT-EU is an important and structured contributor to the ENISA threat landscape and related activities and will remain so in 2022.

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 the cyber threat landscape[67]. Those two groups were formalised in 2021.

In 2022, CERT-EU, through its inclusion as an observer in these ENISA working groups, will contribute to, review and validate the findings and generally enhance the outputs of the groups. These activities refer to Activity 8 of the 2022 ENISA work programme: knowledge on emerging cybersecurity challenges and opportunities.

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

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

NOTES

TP-AH-22-001-EN-N

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.

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

Publications Office
of the European Union

ISBN 978-92-9204-547-0