EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2024–2026 ENISA SINGLE PROGRAMMING DOCUMENT

Condensed work programme 2024

JANUARY 2024

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

COPYRIGHT NOTICE

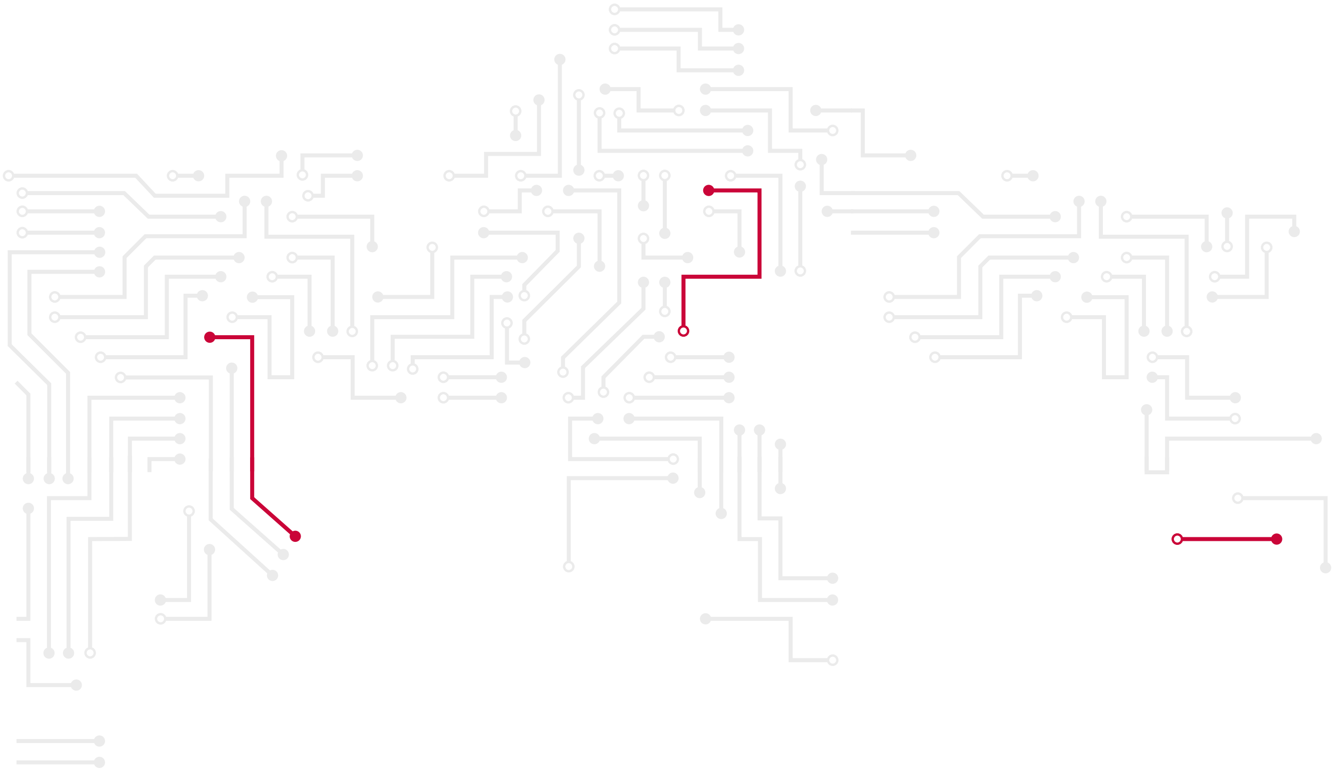
Luxembourg: Publications Office of the European Union, 2024

Linguistic version	**Catalogue number**	**ISBN**	**ISSN**	**DOI**
BOOK	TP-AH-24-002-EN-C	978-92-9204-666-8	2467-4397	10.2824/82006
PDF	TP-AH-24-002-EN-N	978-92-9204-667-5	2467-4176	10.2824/50732

ENISA SINGLE PROGRAMMING DOCUMENT 2024–2026

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS



FOREWORD

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

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

Thus, besides building on ENISA's accumulated expertise and strengths, it is important to further enhance its proactive capabilities at the service of the MSs in 2024. The agency has introduced a new activity within this single programming document (SPD) with the aim of putting the ENISA support action on a firmer ground, enabling it to better organise its assistance to MSs. In this way, ENISA can better help the MSs in their efforts to improve the capability to respond to cyber threats and incidents while providing them with knowledge and expertise and increasing preparedness in key sectors. Here the agency acknowledges the importance of the additional financial resources made available to it by the European Commission, without which this activity would not be possible.

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

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

Juhan Lepassaar
Executive Director

FAKE
STOP
AI
01010
11101
00101

WORK PROGRAMME FOR 2024

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

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

3.1. OPERATIONAL ACTIVITIES

ACTIVITY 1: Providing assistance on policy development

Overview of activity

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

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

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

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

Link to strategic objective (ENISA strategy)

- Cybersecurity as an integral part of EU policies

Indicator for strategic objectives

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

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

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

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

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
1.1 Advise the Commission and MSs on reviewing the effectiveness of current cybersecurity policy frameworks	Stakeholders will use evidence to understand how implemented policies have affected the targeted entities	DG Communications Networks, Content and Technology NIS CG NLOs	Stakeholder satisfaction [31]	Biennial (Survey)	93%	>90%
			Number of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	21	30
1.2 Advise the EC and MS on new policy development, as well as carrying out preparatory work	Stakeholders will use ENISA's advice to develop effective and consistent EU cybersecurity policies	DG CONNECT and other DGs or EUIBAs depending on policy file owner.	Stakeholder satisfaction	Biennial (Survey)	93%	>90%
			Number of EU policies supported by ENISA	Annual (internal report)	7	5
			Number of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	21	30
1.3 Monitor and analyse new and emerging policy areas	Stakeholders are informed in a timely manner about gaps, overlaps and inconsistencies across EU policy initiatives under development	NLOs NIS CG DG Communications Networks, Content and Technology and other DGs or EUIBAs depending on the policy file owner	Stakeholder satisfaction	Biennial (Survey)	93%	>90%

Stakeholders and engagement levels

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

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

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

[31] Stakeholder satisfaction conducted every 2 years to measure the uptake of results / outcome, added value, duplication of ENISA work, etc. by stakeholders.

ACTIVITY 2: Supporting implementation of Union policy and law

Overview of activity

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

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

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

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

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

Link to strategic objective (ENISA strategy)

- Cybersecurity as an integral part of EU policies

Indicator for strategic objectives

- Level of maturity of cybersecurity capabilities and resources across the EU at the sector level ([33])

[32] st09364-en22.pdf (europa.eu)

[33] As part of the report on the state of cybersecurity in the EU in Article 18(1), point (e), of NIS2.

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

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
2.1 Support MSs and the Commission in the implementation of the NIS CG work programme and the NISD	MSs will use ENISA advice to implement the NISD.	DG Communications Networks, Content and Technology, NIS CG	Stakeholder satisfaction ([34])	Biennial (Survey)	94%	>90%
			EU register for digital entities is used by all MSs	Biennial (Survey)	n/a	Used by all MS
			Coordinated vulnerability disclosure (CVD) guidance is implemented by MS and all MS are on the CVD map	Biennial (Survey)	n/a	Used by all MS
2.2 Support MSs with EU-wide risk evaluations and EU toolboxes scenarios	• Support EU-wide risk evaluations and risk scenarios • Follow-up of previous EU-wide risk assessments (5G, Nevers) • Sectorial situational awareness reporting	DG Communications Networks, Content and Technology, NIS CG	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of stakeholders involved in the NIS360	Annual (internal count)	n/a	120
			Number of sectorial situational awareness reports	Annual (internal count)	6	12
2.3 Improve cybersecurity and resilience of the NIS sectors	Stakeholders use the NIS service packages to improve security and resilience of the sectors	DG Communications Networks, Content and Technology, NIS CG, sectorial DGs, sectorial EU agencies	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of critical sectors with high level of cybersecurity maturity (NIS sector 360)	Annual (internal count)	3	4
			Number and frequency of services delivered to NIS sectors according to the maturity of the sector	Annual (internal count)	21	24

[34] Results/outcome taken up, added value, duplication of existing work, etc. and effectiveness of ENISA guidance in helping MSs implement their tasks and deliver the NIS CG work programme

Stakeholders and engagement levels

Partners: DG Communications Networks, Content and Technology, NIS CG, national competent authorities, sectorial DGs, sectorial EU agencies
Involve / Engage: NLOs, OES and DSP under NIS1 and overall entities within the scope of NIS2 and industry associations/representatives

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

ACTIVITY 3:
Building capacity

Overview of activity

This activity seeks to improve and develop the capabilities of MSs, EUIBAs and various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the EU. This is achieved through the development of frameworks (risk management, strategies, etc.) that are based on lessons learnt from MSs through the implementation and development of their national cybersecurity strategies.

Measures to support this activity include the organisation of large scale exercises, sectorial exercises and training [35].

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

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

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

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

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

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

[35] CSIRT trainings and ‘capture the flag’ and ‘attach defence’ competitions.

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
3.A Increase the level of alignment and cooperation within and between MSs as well as sectors and EUIBAs	Articles 6 and 9 CSA	2024	• Number of MSs that use ENISA support and tools for the implementation review and update of their national cybersecurity strategy.	• All MSs that have reviewed their national cybersecurity strategy use ENISA support and tools.
3.B Prepare and test capabilities to respond to cybersecurity incidents	Article 6 CSA	2024	• Proportion of beneficiaries who take part in relevant ENISA exercises and trainings • Added-value of ENISA exercises and training	• All MSs participate in Cyber Europe 2024 • >80 % of EUIBAs have participated in JASPER exercises over 3 years (number of participants in 2024 increases compared to 2023) • 90 % of participants see positive added value
3.C Increase skill sets and align cybersecurity competencies	Article 6 CSA	2024	• Assessment of average level of cybersecurity technical competences of participants in European cybersecurity challenge finals • Number of participants that take part in national competitions improving cybersecurity skills and capabilities • Level of alignment of cybersecurity competences across the EU	• A relevant metric is in the process of being developed in the ENISA security index • More than 10 000 participants take part in the annual 'capture the flag' competitions that are organised prior to the European cybersecurity challenge (ECSC) final • MS national competence frameworks are aligned with the ECSF

[36] As part of the report on the state of cybersecurity in the EU in Article 18(1), point (b), of NIS2.

[37] As part of the report on the state of cybersecurity in the EU in Article 18(1), point (e), of NIS2.

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
3.1 Assist MSs to develop, implement and assess national cybersecurity strategies	• Increase the level of preparedness and cooperation • Prepare capabilities to respond to cybersecurity incidents • Increase skill sets • Align cybersecurity competencies • Improved national cybersecurity strategies	NLO subgroup on national cybersecurity strategies	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			• Maturity of national cybersecurity strategies, • information sharing and analysis centres (ISACs), SOCs, etc.	Annual (Report)	n/a	n/a
3.2 Organise large scale biennial exercises and sectorial exercises	• Increase the level of preparedness and cooperation • Prepare and test capabilities to respond to cybersecurity incidents • Stakeholder test and improve capabilities and increase capacity	• NLO Network (as necessary) • CSIRTs Network (as applicable) • EU-CyCLONe members (as applicable) • NIS Cooperation Group (as applicable) • EU ISACs (as applicable) • NLO subgroup of Cyber Europe planners (as applicable)	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Evaluation of capacity building actions by participants in exercises and trainings	Annual (report)	• 40 % high usefulness • 53.5 % medium usefulness • 6.5 % low usefulness	>50% high usefulness
			Number of participants in trainings and organized by ENISA	Annual (report)		>500 (incl online exercises)
3.3 Organise trainings and other activities to support and develop the maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS CG, EU-CyCLONe and work streams, ISACs and other communities	• Increase the level of preparedness • Prepare capabilities to respond to cybersecurity incidents • Increase skill sets • Stakeholders improve capabilities and skill set	• NLO Network (as necessary) • CSIRTs Network (as applicable) • EU-CyCLONe members (as applicable) • NIS CG (as necessary) • EU ISACs (as applicable) • NLO subgroup of Cyber Europe planners (as necessary)	Stakeholder satisfaction	Biennial (Survey)	91%	90%
			Number of participants in training and in challenges organised by ENISA	Annual (report)	n/a	>1 000 (including online training)
3.4 Organise and support cybersecurity challenges including the ECSC	• Align cybersecurity competencies • Increase skill sets	• ECSC Steering Committee (NLO Subgroup)	Stakeholder satisfaction	Biennial (Survey)	91%	90%

Stakeholders and engagement levels

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

<table>
<tr><th colspan="10">RESOURCE FORECAST</th></tr>
<tr><th rowspan="2">*Outputs*</th><th>*Service package related to category A*</th><th colspan="2">***A** (reserved for tasks to maintain statutory service)*</th><th colspan="2">***B** (reserved for other regular statutory tasks)*</th><th colspan="2">***C** (reserved for ad hoc statutory tasks)*</th><th colspan="2">*Total*</th></tr>
<tr><th></th><th>FTE</th><th>EUR</th><th>FTE</th><th>EUR</th><th>FTE</th><th>EUR</th><th>FTE</th><th>EUR</th></tr>
<tr><td>Output 3.1</td><td>TREX, INDEX</td><td>2.00</td><td>70.000</td><td>0,00</td><td>0</td><td>0.00</td><td>0</td><td>2.00</td><td>70 000</td></tr>
<tr><td>Output 3.2 ([38])</td><td>TREX, NIS</td><td>3.35</td><td>500 000</td><td>0,00</td><td>0</td><td>0.00</td><td>0</td><td>3.35</td><td>500 000</td></tr>
<tr><td>Output 3.3</td><td>TREX</td><td>4.30</td><td>546 591</td><td>0,00</td><td>0</td><td>0.00</td><td>0</td><td>4.30</td><td>546 591</td></tr>
<tr><td>Output 3.4</td><td>TREX TREX</td><td>2.3</td><td>120 000</td><td>0,00</td><td>0</td><td>0.50</td><td>0</td><td>2.8</td><td>120 000</td></tr>
<tr><td>Activity total</td><td colspan="9">FTE: 12.45 Budget: EUR 1 236 591 ([39])</td></tr>
<tr><td>Actual resources used in previous year (2022)</td><td colspan="9">FTE: 10.32 Budget: EUR 1 921 221 ([40])</td></tr>
</table>

[38] By the end of 2023, ENISA expects to sign a new multiannual SLA with eu-LISA to provide support on exercises.

[39] In addition EUR 120 000 from SLA with eu-LISA (see Annex XI).

[40] Carried over into 2023: EUR 328 339.

ACTIVITY 4:
Enabling operational cooperation

Overview of activity

The activity supports operational cooperation among MSs, EU institutions, bodies, offices and agencies and between operational activities. The main goal of the activity is to provide support and assistance in order to ensure the efficient functioning of EU operational networks and cyber crisis management mechanisms. ENISA, as mandated by NIS2, provides the organisational support and tools for both the technical (EU CSIRTs Network) and operational layer (EU CyCLONe) of EU operational cooperation networks. As part of this activity, ENISA is supporting operational communities through helping to develop and maintain secure and highly available networks / IT platforms and communication channels in particular ensuring maintenance, deployment and uptake of the MeliCERTes platform and the EU vulnerability database. Thus, this activity could also prepare some of ENISA's proposed tasks in coordinating information and notification about vulnerabilities at the EU level as outlined in the Commission's legislative initiative on CRA.

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

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

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

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

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
4.A. Enable trust and effective cooperation and operations of CSIRTs Network and EU-CyCLONe members.	Article 7 & NIS2	2024	• Satisfaction with scalable ENISA support • Maturity of operational communities	• 80 % satisfaction of stakeholders • Average overall level of maturity increases year by year
4.B. Ensure a high level of coordination of the vulnerability disclosure services within the EU.	Article 7 and NIS2	2026	• EU vulnerability database usage and added-value	• EU vulnerability disclosure services are gradually available (numbering services in place) and aligned with national mechanisms • EU vulnerability database is functional and aligned with national mechanisms
4.C. Robust and secure tools/platforms are established, and actively utilised to facilitate seamless operational collaboration at the EU level.	Article 7 and NIS2	2024	• Continuous operations and use of secure communication tools and platforms for EU-CyCLONE and Cooperation Network including the use of regular checks and controls	• No significant disruption or incidents in the working of operational tools and platforms recorded against standard checks and controls • Beneficiaries use the tools

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs Network and EU-CyCLONe members.	Enhanced information sharing and cooperation among the CSIRTs Network and EU-CyCLONe members	CSIRTs Network and EU-CyCLONe members	Stakeholder satisfaction	Biennial (Survey)	89%	>90%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (Report)	n/a	
4.2 Design and architect processes and tools to build an EU vulnerability database in close cooperation with the MSs	ENISA provides numbering services for common vulnerabilities and exposures with a view to gradually establishing the EU vulnerability database.	CSIRTs Network and NIS CG.	Stakeholder satisfaction	Biennial (Survey)	89%	>90%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (Report)		
4.3. Operate, maintain and promote operational cooperation infrastructure for the EU cybersecurity communities.	Usage of the available tools	CSIRTs Network and EU-CyCLONe members.	Stakeholder satisfaction	Biennial (Survey)	89%	>90%
			Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA	Annual (Report)		>5% increase
			CSIRTs active users % increase year on year		19%	
			CSIRTs number of exchanges/ interactions % increase year on year		104%	
			EU-CyCLONe active users % increase year on year		2%	
			EU-CyCLONe number of exchanges/ interactions % increase year on year		548%	

Stakeholders and engagement levels

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

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

RESOURCE FORECAST									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 4.1	NIS, SITAW	3.5	144 567	0	299 557	0	0	3.5	444 124
Output 4.2	NIS, SITAW	3.5	266 474	0	0	0	0	3.5	266 474
Output 4.3	SITAW, NIS	3.5	786 908	0	278 988	0	0	3.5	1 065 896
Activity total	FTE: 10.50 Budget: EUR 1 776 494								
Actual resources used in previous year (2022)	FTE: 5 Budget: EUR 1 682 555 (41)								

(401) Carried over into 2023: EUR 602 393.

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

Overview of activity

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

The activity includes the development of a regular in-depth EU cybersecurity technical situation report in accordance with Article7(6) CSA, also known as the joint cyber assessment report (JCAR), regular weekly open-source intelligence reports, a joint rapid report together with CERT-EU and other ad hoc reports as needed.

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

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

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

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

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

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
5a.A Threat and information are disseminated in a timely and accurate manner and/or available on demand	Article 7	2025	• Recipients are informed accurately and in a timely manner about the latest threat, vulnerabilities and incidents • Usefulness of situational reports	• At least 80 % of recipients found the information to be communicated accurately and in a timely manner based on the level of confidence of the information • At least 80 % of recipients found the reports useful
5a.B Improved common situational awareness through joint assessment, threat and risk analysis	Article 7	2025	• Stakeholders ability to make informed decisions based on joint situational reports • Usefulness and timeliness of joint situational reports	• 100% quarterly JCAR reports have been issued on time • At least 80% of recipients find the reports useful
5a.C Information exchange to augment EU common situational awareness through cooperation with private sector and non-EU entities	Article 7	2026	• Cyber partnership programme is established • Information coming from private sector partners and non-EU entities are part of operational cycle of situational awareness production	• 90 % of selected entities are enrolled in the ENISA cyber partnership programme • 90 % of the participating entities are actively contributing by exchanging information

Outputs	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2024
5a.1 Collect, organise and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports and threats, and support consolidation and exchange of information on strategic, operational and technical levels [42]	• Establishment of a threat information management platform • Production of briefings, reports and summaries of incidents, threats and vulnerabilities • Increased understanding and timely access to information regarding latest threats, incidents and vulnerabilities	CSIRT Network, EU CyCLONe, EUIBAs, national authorities within MSs subscribed to the products	Stakeholder satisfaction	Biennial (Survey)	84%	>90%
			Timeliness and accuracy of reports	Annual (survey)	n/a	
5a.2 Provide analysis and risk assessment jointly with other operational partners including EUIBAs, MSs, industry partners and non-EU partners	• EU joint assessment and reports, sectorial analysis, threat and risk analysis [43] • Recipients receive accurate and timely assessment of threat actors and associated risk to the EU internal marke	CSIRT Network, EU CyCLONe, EUIBAs, Horizontal Working Party on Cyber Issues, MB	Stakeholder satisfaction	Biennial (Survey)	84%	>90%
			Number of contributing MSs and relevant EUIBAs	Annual (survey)	n/a	
5a.3 Maintain, develop and promote ENISA cyber partnership programme aimed at information exchange to support the agency's understanding of threats, vulnerabilities, incidents and cybersecurity events	• Establishment and operationalisation of the cyber partnership programme • ENISA situational awareness leverages private sector partnerships to augment context and understanding of threats, vulnerabilities and incidents	CSIRT Network, EU CyCLONe, EUIBAs, Horizontal Working Party on Cyber Issues, MB	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Number of new and total partners in the ENISA partnership programme	Annual (report)	n/a	10/4
			Percentage of requests for information answered by members of partnership programme	Annual	n/a	80%

[42] Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.

[43] Including JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and DG Communications Networks, Content and Technology Situation Centre.

Stakeholders and engagement levels

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

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

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

[44] Includes allocation of EUR 450 000 from the contribution agreement related to the cybersecurity support action, refer to Annex XI and activity 5b for further information.

[45] Includes allocation of EUR 450 000 from the contribution agreement related to the cybersecurity support action, refer to Annex XI and activity 5b for further information.

[46] Carried over into 2023: EUR 276 749.

ACTIVITY 5b: Contribute to cooperative response at Union and Member States level through ex-ante and ex-post services provision

Overview of activity

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

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

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

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

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

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

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

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

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

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

Stakeholders and engagement levels

Partners: EU MSs, selected beneficiary entities, Commission
Involve / Engage: EU-CyCLONe, CSIRT Network, DG Communications Networks, Content and Technology

[48] Target response to qualitative survey regarding ENISA's ability to support MSs on a scale of 1 to 5, with 5 being the highest rating.

[49] Beneficiaries of the activity 5b services are specified in the [Contribution Agreement].

[50] Beneficiaries of the activity 5b services are specified in the [Contribution Agreement].

[51] Beneficiaries of the activity 5b services are specific in the [Contribution Agreement].

[52] Beneficiaries of the activity 5b services are specific in the [Contribution Agreement].

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

[53] Cyber support action programme.

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

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

[56] Minus 450 000 allocated to activity 5a, please refer to Annex XI for further details regarding the contribution agreement.

ACTIVITY 6: Development and maintenance of EU cybersecurity certification framework

Overview of activity

This activity encompasses measures that seek to establish and support the EU cybersecurity certification framework by preparing and reviewing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the Union rolling work programme. Measures also include maintaining and evaluating adopted cybersecurity certification schemes and participating in peer reviews. In addition, in this activity, ENISA assists the Commission with regard to the ECCG, co-chairing and providing the secretariat for the SCCG; ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Article 50 of the CSA. As from 2024, ENISA seeks to support the cybersecurity certification stakeholders with an online platform that has been set up by the Commission. Furthermore, ENISA contributes to the cybersecurity framework by analysing pertinent aspects of certification along the lines of legislation adopted, notably NIS2 and the DGA as well as legal instruments in the legislative process that include the amendment to the CSA, CRA, EUDIW, AI Act, Chips Act, Data Act, amendment of CSA regarding managed security services certification, etc.

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

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

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

Link to strategic objectives (ENISA STRATEGY)

- sHigh level of trust in secure digital solutions

Indicator for strategic objectives

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

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
6.A Improve the certification requirements concerning security posture management of certified products, services, processes and gradually of managed security services	Article 8 and Title III	2025	• Monitor ENISA take-up of technical standards and technical specifications in support of EU legislation (document monitoring)	Applicable standards and cybersecurity requirements have been considered by ENISA to promulgate better cybersecurity certification schemes
6.B Efficient and effective implementation of the European cybersecurity certification framework	Article 8 and Title III	2025	• Number of stakeholders (public and private) in the internal market, implementing the cybersecurity certification framework for their digital solutions	A scheme is implemented in a timely manner across all relevant market sectors
6.C Increase use and uptake of European cybersecurity certification	Article 8 and Title III	2024	• Number of schemes and additional requests addressed to ENISA by the Commission • Number of schemes and additional requests processed by ENISA • Uptake of certified digital solutions (products, services, processes and gradually managed security services) using certification schemes under the CSA framework as well as other directly applicable instruments, i.e. CRA, EUDIW, etc.	High number of private and public entities and/or market sectors relevant to a given scheme taking up certification after the entry into force of the implementing act
6.D Increase trust in ICT products, services and processes	Article 8 and Title III	2025	• Number of certificates issued and published under an EU certification scheme; high utilisation rate in the market	High degree of visibility and utilisation of EU cybersecurity certificates

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
6.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes	• Scheme meets stakeholder requirements, notably of the MSs and the Commission • Take-up of schemes by stakeholders • Timely delivery of all schemes requested in cooperation with the Commission • Statutory bodies and AHWGs actively involved	• AHWGs on certification • ECCG • European Commission	Stakeholder satisfaction	Biennial (survey)	82%	75%
			Number of opinions of stakeholders managed	Annual (report)	n/a	100 opinion items per scheme
			Number of people/ organisations engaged in the preparation of certification schemes	Annual (report)	n/a	At least 20 AHWG members from third-party experts; at least 15 MSs joining AHWGs
6.2 Implementing and maintenance of the established schemes including evaluation of adopted schemes, participation in peer reviews etc. and monitoring the dependencies and vulnerabilities of ICT products and services	• Review of schemes to improve efficiency and effectiveness • Take-up of schemes by stakeholders	AHWGs on certification ECCG European Commission	Stakeholder satisfaction	Biennial	82%	75%
			ENISA response to consolidated monitoring and maintenance requirements of schemes adopted	Triennial (survey)	n/a	75%
			Satisfaction of ENISA's role in NCCA peer reviews	Triennial (survey)	n/a	75%
6.3 Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks		ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			Feedback from statutory bodies including NCCAs on ENISA's role	Annual (survey)	n/a	75%
6.4 Developing and maintaining the necessary provisions, tools and services concerning the EU's cybersecurity certification framework (including the certification website, supporting the Commission in relation to the core stakeholders service platform of the Connecting Europe Facility for collaboration, publication, promotion of the implementation of the cybersecurity certification framework etc.)	• Supporting transparency and trust of ICT products, services and processes • Stakeholders' engagement and promotion of certification	ECCG European Commission SCCG	Stakeholder satisfaction	Biennial	82%	75%
			User satisfaction concerning the certification website services	Annual (survey)	n/a	75%
			Usage of certification website	Annual (report)	n/a	75%

Stakeholders and engagement levels

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

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

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

[57] Carried over into 2023: EUR 277 604 (73) Carried over into 2023: EUR 277 604

ACTIVITY 7: Supporting the European cybersecurity market and industry

Overview of activity

This activity seeks to foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce dependence on external markets, increase the capacity of the EU and reinforce supply chains to the benefit of internal market. It involves measures to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation. Therefore, this activity also seeks to lay the groundwork for a robust role for ENISA in the CRA, notably in terms of market analysis, preparation of market sweeps and reporting of exploited vulnerabilities etc. Measures to support this activity include producing analyses and guidelines as well as good practices on cybersecurity requirements, facilitating the establishment and take-up of European and international standards across applicable areas such as for risk management, and performing regular analysis of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities present therein. Platforms for collaboration among the cybersecurity market players, improve visibility of trustworthy and secure ICT solutions in the digital single market.

Output 7.4 has been absorbed into output 6.2

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

Link to strategic objectives (ENISA STRATEGY)

- High level of trust in secure digital solutions

Indicator for strategic objectives

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

Activity Objectives	CSA article and other EU policy priorities	Timeframe Of Objective	Indicator	Target
7.A Foster a robust European cybersecurity industry and market	Article 8 and Title III CSA CRA proposal	2024	• Stakeholders' satisfaction (survey) • State of the EU cybersecurity industry and market for products and services (index) • Industry perception of the internal market (survey)	Improved ability of ENISA and the EU to analyse the EU cybersecurity market
7.B Improve the conditions for the functioning of the internal market	Article 8 and Title III CSA CRA proposal	2025	• Better informed choices by users of products in market niches analysed	Improve stakeholders' understanding of the cybersecurity market conditions in the EU

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
7.1. Market analysis on the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes	Improved understanding of the market/ industry	• AHWGs cybersecurity market analysis • ECCG (as necessary) • SCCG • Advisory Group • NLO (as necessary)	Stakeholder satisfaction	Biennial (survey))	88%	60%
			Cybersecurity market analysis; cybersecurity product and services analysis; analysis of vulnerabilities and dependencies in ICT products and services as appropriate; analysis of other relevant market areas	Annual (report)	n/a	All reports produced as planned (Y out of Y reports)
7.2. Monitoring developments in related areas of standardisation, analysis of standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification	Alignment with standards	• SCCG • Advisory Group • NLO (as necessary)	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Reports on analysis of standardisation aspects of cybersecurity including cybersecurity certification	Annual (report)	n/a	All reports produced as planned (Y out of Y reports)

Stakeholders and engagement levels

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

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

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

[58] Carried over into 2023: EUR 105 230.

ACTIVITY 8:
Knowledge on emerging cybersecurity challenges and opportunities

Overview of activity

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

These activities leverage on expertise of relevant legal, regulatory, economic and societal trends and data by aggregating and analysing information. The strategic goal is to provide timely, reliable and useful information and knowledge (across the past–present–future timeline) to different target audiences as per their needs and contribute to the improvement of the state of cybersecurity across the EU.

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

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

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

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

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

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

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

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
8.A Knowledge and uptake of future challenges and opportunities by MS and EU actors	Article 9 CSA	2025	• Cybersecurity index indicator 'emerging technology threats are considered by national risk assessments' • Level of the acceptance of the report of the state of cybersecurity in the EU	• European Parliament positive adoption • High take-up of the report by MS and EU actors • All MSs have considered at least 1/3 of the mapped emerging technology threats in assessing risk at the national level
8.B Increase understanding of the state of cybersecurity	Article 9 CSA and eIDAS Article 10	2025	• Use of cybersecurity index by MSs	• All MSs give input to cybersecurity index • 2/3 of MSs are using the index to inform their national cybersecurity strategies
8.C Deliver relevant and timely information	Article 9 CSA	2024	• Usage of knowledge management portals, i.e. index, the cybersecurity incident reporting and analysis system, etc. • Value and usability of knowledge management portals	• 2/3 of targeted stakeholders use the portals regularly • 2/3 of stakeholders are satisfied with the portals

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
8.1. Develop and maintain EU cybersecurity index	• Measuring maturity • Stakeholders can better prepare for future challenges based on indication of maturity	NISD CG, NLO, CSIRTs Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Uptake of the cybersecurity index	Biennial (survey)	n/a	• 20 MS representatives • 60 % satisfaction rate • Agreement by all validating bodies
8.2. Collect and analyse information to report on the cyber threat landscapes	• Mapping threats • Generate recommendations for stakeholders to take up	NLO, Advisory Group and Cybersecurity Threat Landscape AHWG CSIRTs Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357	±5 % compared to 2023
			Uptake of reports generated in activity 8	Annual (report)	n/a	±5% compared to 2023
8.3. Analyse and report on incidents as required by Article 5(6) of the CSA as well as other sectorial legislations (e.g. DORA, Article 10 eIDAS, etc.)	• Analysing incidents • Generate recommendations for stakeholders to take up	Work Stream 3 of the NISD CG, European Competent Authorities for Secure Electronic Communications and Article 19 eIDAS groups	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			EU incident reporting maturity	Annual (survey)	n/a	EU Average >50%
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	n/a	±5 % compared to 2023
			Uptake of reports generated in activity 8	Annual (report)	n/a	±5% compared to 2023
8.4. Foresight on emerging and future cybersecurity challenges and recommendations	• Identifying future challenges and opportunities • Generate recommendations for stakeholders to take up	Foresight AHWG, NLO and AG	Stakeholder satisfaction	Biennial (survey)	91.5%	>5% compared to 2023
			Number of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	357	±5% compared to 2023
			The influence of foresight on the development of ENISA's work programme	Biennial (ENISA SPD)	n/a	>2 emerging areas identified
			Uptake of reports generated in activity 8	Annual (report)	n/a	±5 % compared to 2023

Stakeholders and engagement levels

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

Involve/ Engage: NLO/AG, CSIRTs Network

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

[59] Activity 10 outputs and thus resources were undertaken within activity 8 in 2022.

[60] Carried over into 2023: EUR 81 543.

ACTIVITY 9:
Outreach and education

Overview of activity

The activity seeks to raise the overall awareness of cybersecurity risks and practices. in cooperation with MSs, EU institutions, bodies, offices and agencies and the EU's international partners, it aims to build an empowered European community, with an allied global community which can counter risks in line with the values of the EU. As part of this activity, the agency will organise regular outreach campaigns, provide guidance on best practices and support coordination across MSs on awareness and education. Moreover, the agency will facilitate the exchange of best practices and information on cybersecurity in education between MSs.

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

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

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

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

Link to strategic objectives (ENISA STRATEGY)

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

Indicator for strategic objectives

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

Activity Objectives	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
9.A Increase awareness of cybersecurity risks and improve cyber-secure behaviour	Article 10	2025	• Cybersecurity indicator 'Enterprises: Staff awareness' • Cybersecurity indicator 'SME culture of cybersecurity' • Number of cybersecurity incidents with human error as root cause • Cybersecurity index indicators 'National culture of cybersecurity'	• 1–2 % increase of cybersecurity indicator 'SME culture of cybersecurity' year by year • Number of cybersecurity incidents in critical sectors with human error as root cause decreases year by year in relative percentages • 1–2 % increase of cybersecurity index 'National culture of cybersecurity'
9.B Increase the supply of skilled professionals to meet market demand	Articles 6 and 10 EU priority on skills shortage Commission Communication on Cybersecurity Skills Academy	2025	• Increase in cybersecurity indicator 'Cybersecurity graduates in higher education' • Number of professionals trained under cybersecurity skills academy	• 'Cybersecurity graduates in higher education' • At least 200 000 professionals trained by 2025
9.C Foster EU cybersecurity values and priorities	Article 42	2024	• Ability to support the EU external objectives • Coherence of ENISA international engagement with the agency's strategy	• ENISA is seen as a key contributor to foster EU cybersecurity values and priorities where engaged • ENISA activities are judged to be aligned with its international strategy

Outputs	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2024
9.1 Develop activities to enhance behavioural change by essential entities [61]	• Targeted awareness campaigns to improve behaviour • Take-up of best practices by stakeholders	Awareness raising AHWG, NISD Work stream	Stakeholder satisfaction	Biennial (survey)	91.5%	>1 % increase (from previous year – decrease in duplication)
			Number of activities and participation in awareness-raising initiatives organised by ENISA on cybersecurity topics	Annual (report)		>5% increase
			Total social media impressions		27 278 491	
			Total social media engagement		19 301	
			Total video views		6 602 355	
			Total website visits		300 530	
			Total participation at events		40	
			Number of downloads of materials and overall utilisation of Awareness Raising tools (i.e. Awareness Raising-in-a-box and SME tool)	Annual (ENISA website)	n/a	>4000 per semester

[61] Defined by NIS2

9.2 Promote cybersecurity topics and good practices ([62])	- Recognise threats and risks and how to act cyber secure - Better informed stakeholder	Awareness Raising AHWG, ECSM coordinators group	Stakeholder satisfaction	Biennial (survey)	91%	1 % increase (from previous year – decrease in duplication)
			Number of activities and participation in awareness-raising initiatives organised by ENISA on cybersecurity topics	Annual (report)		>5 % increase
			Total social media impressions	Annual (report)	27 278 491	>5% increase
			Total social media engagement		19 301	
			Total video views		6 602 355	
			Total website visits		300 530	
			Total participation at events		40	
			Number of downloads of materials and overall utilisation of Awareness Raising tools (i.e. AR-in-a-Box and SME tool)	Annual (ENISA website)	n/a	>4000 per semester
9.3 Implement ENISA international strategy and outreach	- EU values recognised by international stakeholders - International cooperation support ENISA objectives	MT, EEAS, COM and (MB as required)	Stakeholder satisfaction	Biennial (survey)	91 %	1% increase (from previous year – decrease in duplication)
			Staff satisfaction with international coordination	Annual (survey)	n/a	>80%
			Number of international engagements	Annual (report)	n/a	
9.4 Support the implementation and uptake of EU cybersecurity skills framework	- Promoting cybersecurity skills courses - Greater number of participants in cybersecurity courses	AHWG on Cybersecurity Skills, ECCC WG on Skills	Stakeholder satisfaction	Biennial (survey)		1% increase (from previous year – decrease in duplication)
			Number of cybersecurity programmes (courses) and participation rates	Annual (cyberhead platform)		1-2% increase
			Total number of students enrolled in the first year of the academic programmes		5 205	
			Student gender distribution (% female: % male)		- 19% female - 81% male	
			Total number of cybersecurity programmes		122	
			Number of postgraduate programmes		5%	
			Number of master's degree programmes		80%	
			Number of bachelor's degree programmes		15%	
			Number of entities included in ECSF registry (i.e. # of MS adopted ECSF, #of ECSF implementations/pledges)	Annual (register of activities)	n/a	30% of MS to adopt ECSF, At least 15 orgisations to have endorsed ECSF

[62] Including based on stakeholder strategy.

9.5 Implement the cybersecurity in education roadmap [63]	• Influence education to include cybersecurity • Greater awareness and interest in cybersecurity as a career path	AR AHWG	Stakeholder satisfaction	Biennial (survey)	91.5%	1 % increase (from previous year – decrease in duplication)

Stakeholders and engagement levels

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

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

RESOURCE FORECAST									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 9.1[64]	NIS	1.75	50 000	0.6	50 000	0	0	2.35	100 000
Output 9.2	INDEX, TREX	1	50 000	0.5	49 315	0	0	1.5	99 315
Output 9.3	SITAW, TREX	1	-	0.75	20 000	0	0	1.75	20 000
Output 9.4	INDEX, TREX, NIS	1.5	70 000	1	30 000	0	0	2.5	100 000
Output 9.5	INDEX	0.5	60 000	0.5	30 000	0	0 0	1	90 000
Activity total	FTE: 9.1 Budget: EUR 409 315								
Actual resources used in previous year (2022)	FTE: 5.22 Budget: EUR 415 122 [65]								

[63] Roadmap developed by ENISA during the course of 2022.

[64] Carried over into 2023: EUR 125 341.

[65] ENISA during the course of 2022.

ACTIVITY 10:
Advise on research and innovation needs and priorities

Overview of activity

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

To prepare this strategic advice, ENISA will take full account of past and ongoing research, development and technology assessment activities, and scan the horizon for emerging and future technological, societal and economic trends that may have an impact on cybersecurity.

ENISA will also conduct regular consultations with relevant user groups, projects (including EU-funded projects), researchers, universities, institutes, industry, start-ups and digital innovation hubs to consolidate information and identify gaps, challenges and opportunities in R & I from the different quadrants of the community.

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

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

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

Link to strategic objectives (ENISA STRATEGY)

- Foresight on emerging and future cybersecurity challenges

Indicator for strategic objectives

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

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

[66] Percentage of funding programmes that address cybersecurity challenges proposed by ENISA.

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

Stakeholders and engagement levels

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

RESOURCE FORECAST									
Outputs	***Service package related to category A***	***A** (reserved for tasks to maintain statutory service)*		***B** (reserved for other regular statutory tasks)*		***C** (reserved for ad hoc statutory tasks)*		***Total***	
		FTE	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**	**FTE**	**EUR**
Output 10.1	NIS	0.6	0	1.15	85 510	0.00	0	1.75	85 510
Output 10.2				1.8	35 490	0.20	5 000	2	40 490
Activity total	FTE: 3.75 Budget: EUR 126 000								
Actual resources used in previous year (2022)	n/a ([67])								

[67] Activity 10 outputs were undertaken under activity 8 in 2022

3.2. CORPORATE ACTIVITIES

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

ACTIVITY 11: Performance and sustainability

Overview of activity

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

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

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

ANNUAL

Activity Objectives	Link To Corporate Objectives	Activity Indicators	Frequency(Data Source)	Latest Result	Target
11.A Maintain corporate performance and coordinate strategic planning	Ensure efficient corporate services	Proportion of SPD KPIs meeting targets	Annual	13 metrics were unchanged, 21 underperformed and 58 outperformed	>80 of indicators out-performed
	Continuous innovation and service excellence	Results of Internal control framework assessment	Annual	Effective (Level 2)	Effective level 1/2
	Developing service propositions with additional external resourcing	High satisfaction with essential corporate services in the area of compliance and coordination	Annual	n/a	>60%
11.B Increase corporate sustainability	Ensure climate neutral ENISA by 2030	EU Eco-Management and Audit Scheme (EMAS) established	Annual	n/a	Adopted by end 2024
	Develop efficient framework for ENISA continuous governance to safeguard high level of IT	• Agency IT strategy aligned with corporate strategy • Proportion of total IT budget allocated to information security proportional to the level of risks across various IT systems within Agency	Annual	• n/a • n/a	• Revised IT strategy by 2024 • 20% by 2024

Outputs	How output expected to contribute to activity objective for the year	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
11.1 Coordinate the implementation of the Agency's performance management framework, including Agency wide budget management and IT management processes, environmental management and regulatory compliance	• Unified day to day practices across the agency upon implementing SPD • Annual risk assessment and internal controls assessment performed and reported • Legal and regulatory compliance are monitored; issues and areas of improvement identified • Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy; reports from ITMC • Streamlined budget management across the Agency; reports from BMC • A plan to reduce CO2 emissions at ENISA's HQ	• MT & relevant committees • External and internal audits • Statutory bodies	Efficiency and effectiveness of project management procedures and tools (survey)	Annual	N/a	>80%
			Number of high risks identified in annual risk assessment		3	≤3
			Percentage of identified internal controls deficiencies addressed within timelines		N/a	100% for critical, 80% for major, 60% for moderate
			Number of complaints filed against ENISA/ number of identified legal or regulatory breaches		3	≤3
			% of revised and up to date corporate rules (MBD, EDD, policies, processes)		N/a	60% corporate rules which have not been reviewed less than 3 years ago; 80% corporate rules which have not been reviewed less than 4 years ago
			MoU with Hellenic authorities for CO2 reduction in ENISA HQ in place		N/a	MoU process initiated by end 2024
			Efficiency and effectiveness of ITMC/ BMC processes (survey)		N/a	> 60%
11.2 Maintain and enhance ENISA's cybersecurity posture	• Compliance with new Regulation on a high common level of cybersecurity within EUIBAs • Timely identification and response to cybersecurity risks • Continuous monitoring of IT systems cybersecurity and timely identification of issues and areas of improvement (first level and second level controls)	• MT and relevant committees • External and internal audits • Statutory bodies	Percentage of identified high risk mitigation measures addressed within timelines	Annual	NA	90%
			Cybersecurity trainings for staff and managers	Annual	NA	At least two trainings per year
11.3 Provide support services in the EU Agencies network and in key areas of the Agency's expertise	• Cybersecurity advisory in implementation of the new Regulation on a high common level of cybersecurity within EUIBAs and in co-operation with CERT-EU • Shared services in the area of data protection, legal services and accounting	• MT, BMC • EUAN (agencies receiving ENISA's support)	Satisfaction within the EU Agency network with ENISA support services	Annual	NA	>80%
11.4 Ensure the implementation of single administration processes across the Agency	Streamlined document management practices	• MT, Staff committee	Percentage of staff considering that the information they need to do their job is easily available/accessible within ENISA	Annual	29%	55%
			Response timeliness to external parties (internal reporting)	Annual	NA	48h

Stakeholders and engagement levels

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

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

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

([69]) In addition 54.604 SLA with the ECCC, see Annex XI for additional information.

([70]) The current SPD activities 11 and 12 were undertaken within activity 11 in 2022.

([71]) Carried over into 2023: EUR 174 087.

ACTIVITY 12:
Reputation and trust

Overview of activity

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

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

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

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

ANNUAL

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

Outputs	How output expected to contribute to activity objective for the year	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
12.1 Implement the multiannual communications and stakeholders' strategies	• Increased transparency and outreach • Engaged communities • Increased impact of ENISA activities • Relevant and easily accessible information is provided to stakeholders	Management Team and agency stakeholders	Number & types of activities at each engagement level (stakeholder strategy implementation)	Annual (Internal report)	N/a	
			Number of social media engagement	Annual (Media monitoring)	75 000	>80 000
			Stakeholder satisfaction with ENISA outreach	Biennial (survey)	N/a	>80%
			Number of total ENISA website visits	Annual (website analytics)	2.03 million	>2.5 million
12.2 Implement internal communications strategy	• Engaged staff	Management Team and staff committee	Staff satisfaction with the quality and timing of ENISA internal communications	Annual (survey)	36%	>50%
12.3 Manage and provide the secretariat for the statutory bodies	• Support the operation and organisation of ENISA statutory bodies • Support the effectiveness of the implementation of the work programme (validation of operational outputs) • Providing administrative support for the day-to-day working of the bodies • MB decisions and recommendations from NLO and AG	Statutory bodies, Management Team and Committees	Number of feedback received per NLO consultation	Annual (Internal report)	NA	>2
			Number of feedback received per AG consultation	Annual (Internal report)	NA	>2
			Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA	Annual (Survey)	NA	>80%
			Satisfaction of statutory bodies with ENISA portals	Annual (Survey)	NA	>80%

Stakeholders and engagement levels

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

Involve / Engage: All ENISA stakeholders

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

[72] Activity 12 outputs were undertaken within activity 11 in 2022.

ACTIVITY 13: Effective and efficient corporate services

Overview of activity

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

The initiatives which will be pursued as part of this activity will focus on making sure that the agency’s HR resources fit the needs and objectives of ENISA, attracting, retaining and developing talent and building ENISA’s reputation as an agile and knowledge-based organisation where staff can evolve personally and professionally, keeping staff engaged, motivated and with a sense of belonging. Emphasis will be placed on competency development and ways to make ENISA an ‘employer of choice’ in order to support ENISA’s objectives The activity will seek to build an attractive workspace by establishing an effective framework enabling teleworking outside the place of assignment, developing and maintaining excellent working conditions (premises, layout of office space) and implementing modern user-centric IT and teleconferencing tools delivering state-of-the-art corporate services and supporting ENISA’s business owners and stakeholders in line with the agency’s objectives.

ENISA will strive to maximise the efficiency of its resources by maintaining its focus on developing a flexible, highly skilled and fit-for-purpose workforce through strategic workforce planning in order to ensure the effective functioning of the agency and maintain a high quality of services in the administrative and operational areas. ENISA will further improve the strategic planning and resource management support to the agency, leading to a constant optimisation of resources under a short- and long-range time frame. This would enable ENISA to enhance its future-readiness capabilities and continue its path towards an agile, knowledge-based and matrix organisational structure. The agency will continue to look into flexible (50/50) working arrangements to better balance work requirements in a pragmatic manner.

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

Activity Objectives	Link To Corporate Objectives	Activity Indicators	Frequency (Data Source)	Latest Result	Target
13.a Enhance people centric services by implementing the Corporate and HR strategy	• Effective workforce planning and management • Efficient talent acquisition, development and retainment • Caring and inclusive modern organisation	• Implementation of SWP/SWR decisions • Implementation of the Corporate and HR strategy • High participation in staff satisfaction survey	• Annual • Annual • Annual	• Fully implemented • N/a • 69 %	• Fully implemented • Actions implemented according to the timelines • 75 %
13.b Ensure sustainable and efficient corporate solutions and promote continuous improvement	• Ensure efficient corporate services • Introduce digital solutions that maximise synergies and collaboration in the agency • Develop service propositions with additional external resourcing • Promote and enhance ecologic sustainability across all agency operations • Develop an efficient framework for ENISA continuous governance to safeguard a high level of IT and physical security	• Understand best practices in sustainable IT solutions • Limited disruption of continuity of corporate services • Handling EUCI at the level of SECRET UE/EU SECRET	• Annual • Annual • By Q2 2024	• N/a • N/a • N/a	• IT strategy updated accordingly • BCP for corporate IT, facilities, financial and HR services ensured • Has been accredited

Outputs	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2024
13.1 Manage and provide horizontal, recurrent, quality support services in the area of resources for ENISA staff and partners	• Implement payroll and recurrent administrative services • Implement annual recruitment plan • Implement annual L&D plan and staff performance • Implement annual procurement plan via PPMT • Implement insource mission service support • Implementation of the ED decision on strategic workforce review [adopted in May 2023] • Follow up on FIA centralisation and implementation of results of external analysis on simplification of ENISA financial procedures • Analyse procurement services and tenders and propose simplifications • Explore further synergies with PMO SLA (e.g. reimbursement of experts)	• Management Team • IT Management Committee • Budget Management Committee • Staff Committee	Turnover rates	Annual	4%	> 3 %
			Establishment plan posts filled		89%	>95%
			Time spent from vacancy announcement to candidate selection		n/a	<300 days
			Percentage of the implementation of approved Recruitment plan		n/a	>90%
			Percentage of the implementation of approved Procurement Plan		n/a	>90%
			Percentage of procurement procedures launched via e-tool (PPMT)		n/a	>90%
			Percentage of budget implementation		100%	>95%
			Average time for initiating a transaction (FIA role)		n/a	<7 days
			Average time for verifying a transaction (FVA role)		n/a	<3 days
			Number of budget transfers		4	<4
			Late payments		n/a	<8%

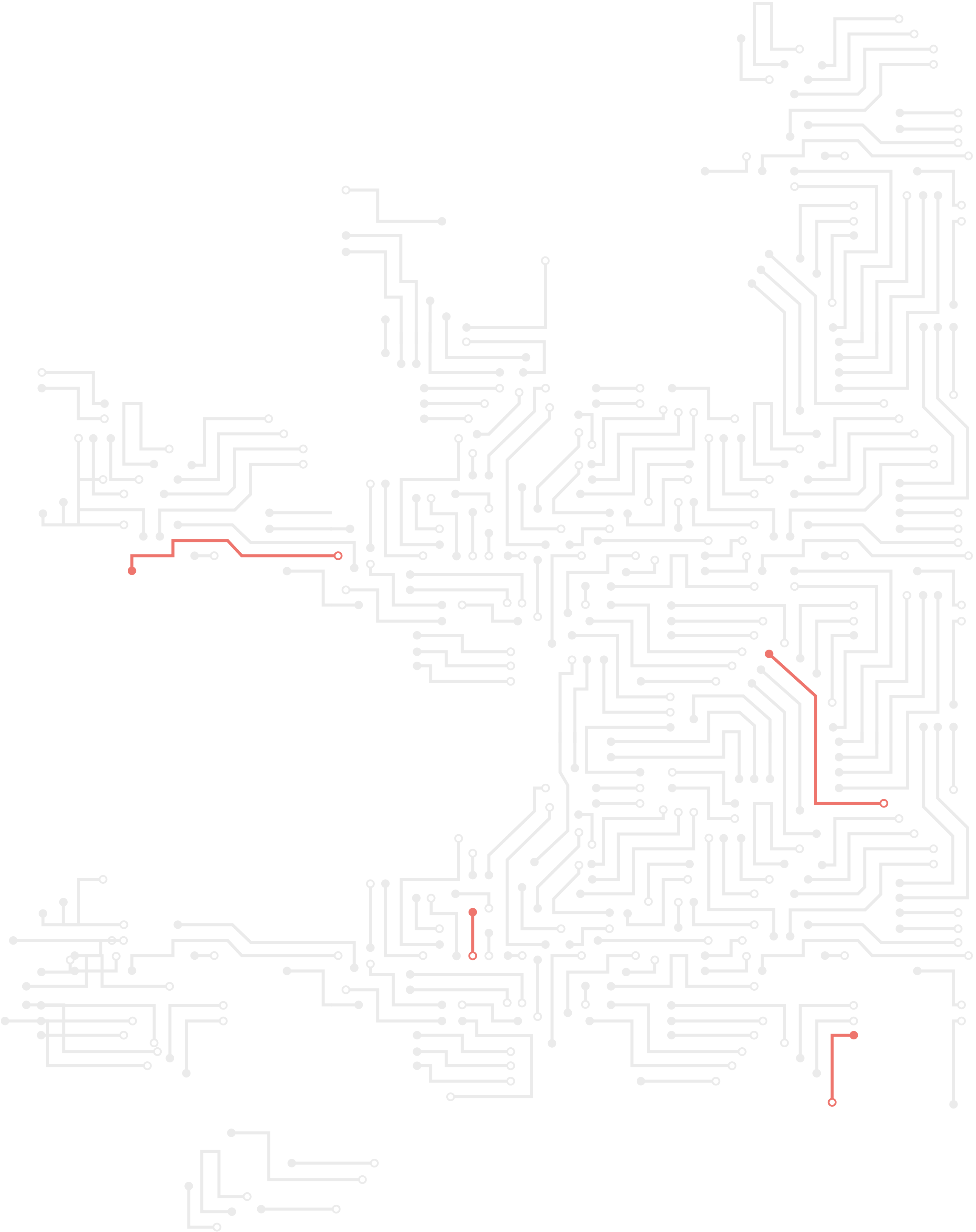
13.2 Implement Agency's Corporate strategy including HR strategy with emphasis on initiatives in talent development, growth and welfare, innovation and inclusiveness areas	• Establish / review corporate costing models and mechanisms to forecast, anticipate and timely manage emerging needs • Revision of HR related MB decisions on middle management staff, on SNEs, on the framework for learning and development, on the appraisal of TA staff and CA staff, on reclassification of TA staff and CA staff indicated in the corporate strategy • Set up of key HR policies in the area of learning and development and review staff welfare and mission policies • Introduce modern digital solutions in managing talent that give real time input to managers • Modernize the selection process by introducing automated IT tool in the process	• Management Board • Management Team • Staff Committee • EUAN • BMC	Number of policies/IR revised or adopted	Annual	n/a	>1
			Number of processes reviewed/redesigned		n/a	>1
			Percentage of staff satisfaction survey with talent development		43%	>50%
			Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time		n/a	>95%
			Number of implemented competency driven training and development activities		n/a	>1
			Number of multisource feedback evaluations implemented and followed up		n/a	>5
13.3 Manage and provide horizontal, recurrent, quality support services in the area of facilities, security and corporate IT for ENISA staff and partners	• Implement annual IT project plan • Implement annual FM plan, maintenance and upgrades, including physical security service provision • Upgrade infrastructure to improve working conditions and create a conducive work environment to ensure sustained productivity and employee satisfaction • Align the lifecycle of IT services and equipment (servers, used equipment) with objectives • Ensure timely implementation of requirements to maintain EUCI at relevant level • Review ENISA's geographically disperse IT solutions and systems and propose cost benefit solutions that would maximise ENISA's corporate resilience • Follow up on the ServiceNow implementation and explore further synergies for integrating further services (HR, FM, EDO, etc) • Follow up on AV implementation and upgrade of meeting rooms	• Management Team • IT Management Committee • Budget Management Committee • Staff Committee	Satisfaction survey for working environment	Annual	n/a	80 %
			Safety and security incidents reported at workplace in any of the 3 ENISA offices		n/a	<3
			Average time for dealing with facilities management requests >1		n/a	<3 days
13.4 Enhance operational excellence and digitalisation through modern, safe and secure and streamlined ways of working and introducing self-service functionalities	• Explore synergies between FM and Security service provision by integrating services via one service provider, hence reducing FWC numbers and provide all-inclusive services • Implementation of an Identity and Access Management Solution to increase the Cybersecurity posture of the organisation • Equipment renewal (laptops/mobiles) to ensure business continuity through updated technology, enhanced security measures and improved equipment performance • Implement an effective backup solution (SAN) to enhance business continuity by safeguarding critical data, mitigating the risk of data loss and ensuring a swift operation recovery in the event of system failures, disasters or cyber-attacks • Implement new A/V and conference equipment to bolster business continuity by facilitating seamless remote collaboration to ensure high-quality communication and collaboration, which is essential to maintain productivity and operational efficiency • Implement of a cloud-based platforms and solutions automate IT delivery services, assure service availability, improve self-service functionalities and provide critical IT-related metrics enabling secure access and sharing of information or device from any location • Upgrade physical security measures to ensure high standards for the other ENISA offices to get EUCI accreditation • Further development of Athens data centre for high availability purposes to ensure the business continuation and minimisation of downtime risks	• Management Team • IT Management Committee	Resilience and quality of ENISA IT systems and services (automated or via surveys) [specific KPIs will be defined for each expected result of the output and will be monitored separately] – as generic indicators – • Critical systems uptime//downtime • Staff satisfaction with resolution	Annual	100 % 84 %	99 % 85 %

Stakeholders and engagement levels

Partners: ENISA staff members and EUIBAs
Involve / Engage: Private sector and international organisations

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

[73] Carried over into 2023: EUR 444 812.



NOTES

NOTES

NOTES

TP-AH-24-002-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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union

ISBN 978-92-9204-547-0