



EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ENISA SINGLE PROGRAMMING DOCUMENT 2025 -2027

Condensed work programme 2025

JANUARY 2025

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 2025–2027 as approved by the Management Board in Decision No MB/2024/16. The Management Board may amend the Work Programme 2022–2024 at any time. ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source. Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2025

This publication is licenced under CC-BY 4.0 “Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated”.

Copyright for the image on the cover and internal pages: © Shutterstock

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

Luxembourg: Publications Office of the European Union, 2025

Linguistic version	Catalogue number	ISBN	ISSN	DOI
PDF Web	TP-01-25-005-EN-N	978-92-9204-692-7	2467-4176	10.2824/3285936



ENISA SINGLE PROGRAMMING DOCUMENT 2025–2027

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

SECTION I	
WORK PROGRAMME FOR 2025	7
1.1. OPERATIONAL ACTIVITIES	9
• ACTIVITY 1: Support for policy monitoring and development	9
• ACTIVITY 2: Cybersecurity and resilience of critical sectors	12
• ACTIVITY 3: Capacity Building	16
• ACTIVITY 4: Enabling operational cooperation	20
• ACTIVITY 5: Provide effective operational cooperation through situational awareness	24
• ACTIVITY 6: Provide services for operational assistance and support	28
• ACTIVITY 7: Supporting Development and maintenance of EU cybersecurity certification framework	31
• ACTIVITY 8: Supporting European cybersecurity market, research & development and industry	34
1.2 CORPORATE ACTIVITIES	38
• ACTIVITY 9: Performance and sustainability	38
• ACTIVITY 10: Reputation and Trust	43
• ACTIVITY 11: Effective and efficient corporate services	46



FOREWORD

This Single Programming Document (SPD) for the years 2025-2027 outlines the steps ENISA will take to enhance the maturity and resilience of cybersecurity in the EU.

Firstly, as the EU took legislative steps to strengthen its cybersecurity framework with the aim of protecting its economy, society and everyday life across Europe, the strategy of the Agency was revised accordingly by the Management Board in 2024 to further clarify and amend the Agency's priorities and focus. This program thus includes the new indicators to measure the success of its strategic objectives. At the same time, the Agency streamlined its operational activities and adjusted its organizational structure to more effectively manage these activities and improve its capacity to deliver more efficiently.

Secondly, approximately half of ENISA's operational resources are allocated towards enabling operational cooperation between Member States, including through dynamic and improved common situational awareness. The contribution agreement of EUR 20 million from the EU budget, for which the European Commission entrusted ENISA to manage in Autumn 2023, will enable the Agency to continue to scale up and expand its support to EU Member States in 2025 and 2026. Furthermore in the end of 2024, the Agency and the European Commission signed another Contribution Agreement, which includes EUR 12 million for the establishment, management of the CRA Single Reporting Platform and EUR 2.55 million for the continuation of the Support Action, which will be implemented by 31st December 2027. The combination of these measures will enable Member States to identify potential cyber risks, assess serious vulnerabilities and take timely action to mitigate attacks and respond effectively to threats.

Thirdly, through this work program ENISA has strengthened its capabilities and capacities to support EU Member States with implementation of the NIS2 Directive, the Cyber Resilience Act and the Cyber Solidarity Act, as well as ensuring the EU cybersecurity certification framework is implemented efficiently.

Through cooperation with Member States and Union bodies, private and public organizations, and various cyber communities as well as through synergies with like-minded international partners, ENISA strives to ensure a secure and trusted digital environment for all businesses and citizens in Europe in the complex geopolitical context and the evolving threat landscape of 2025.

Juhan Lepassaar
Executive Director



SECTION I

WORK PROGRAMME FOR 2025

This is the main body of the Work Programme. It describes what the agency aims to deliver through its operational and corporate activities during the year 2025 towards achieving its strategy and expected results. A total of eight operational activities and three corporate activities have been identified to support the implementation of ENISA's mandate in 2025.

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

Service catalogue

In 2022 the Agency introduced the concept of a service catalogue to allow management to focus efforts and resources in a highly structured and more efficient manner to obtain specific objectives. ENISA's service catalogues are organised into individual service packages. A service package is a collection of cybersecurity products and services that span a number of activities and contribute to the objectives of a discrete service package. A service package is a

means of centralising all services that are important to the stakeholders that use it. The Agency will continue to review and prioritise its actions in order to build and make use of internal synergies and ensure that adequate resources are reserved across the Agency in a transparent manner.

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

- NIS directive (NIS) led by Activity 2 - cybersecurity and resilience of critical sectors;
- Training and exercises (TRES) led by Activity 3 - capacity building;
- Situational Awareness (SITAW) led by Activity 5 - providing effective operational cooperation through situation awareness;
- Certification (CERTI) led by Activity 7 - development and maintenance of EU cybersecurity certification
- Cybersecurity index (INDEX) led by Activity 1 - support for policy monitoring and development.

Stakeholders and engagement level

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

Each activity includes a list of stakeholders and the expected or planned engagement level for each stakeholder. The engagement level refers to the degree of the stakeholder's interest and influence in the activity for stakeholders classified as either partner or involve / engage. Stakeholders classified as 'Partner' refers to stakeholders with high influence and high interest, usually business owners and others with significant decision-making authority. They are typically easy to identify and to engage with actively. Stakeholders classified as 'involve / engage' have high influence but low interest. These are typically stakeholders with a significant decision-making authority but lacking the availability or the interest to be actively engaged.

KPIs / metrics

In 2020 the Agency developed and introduced a new set of key performance indicators and related metrics for measuring the performance of the activities. These metrics are described in the Single Programming Document for each activity and are made up of both quantitative and qualitative metrics. Quantitative metrics are those that measure a specific number through a certain formula, whereas qualitative metrics are those that are more of a subjective opinion based on the information received; however even these are quantified in order to be interpreted and measured. The work programme for 2025 includes indicators for measuring the new strategic objectives from the updated ENISA strategy, indicators and targets for measuring the objectives of activities and indicators at the output level to measure the performance of the outputs.

1.1. OPERATIONAL ACTIVITIES

ACTIVITY 1: Support for policy monitoring and development



Overview of activity



This activity seeks to bolster policy initiatives on novel or emerging areas of technology by providing technical, fact-driven and tailor-made policy analyses and recommendations. ENISA will support EU institutions and MSs on new policy initiatives¹ through evidence-based inputs into the policy development process. ENISA, in coordination with the Union's institutions 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, as well as develop monitoring capabilities and tools to regularly and consistently be able to provide advice on the effectiveness of existing Union policy and law in accordance with the EU's institutional competencies in the area via the "Implementation Check" model, together with Activities 2 and 8 in particular.

This activity delivers on ENISA's strategic objectives 'Cybersecurity as an integral part of EU policies' and 'Efficient and effective cybersecurity knowledge management for Europe'. In particular, work under this Activity shall provide strategic long-term analysis, guidance and advice on current policy challenges and opportunities. In terms of knowledge management, ENISA will work towards consolidating data, information and indicators concerning the status of cybersecurity across MSs, including through input from National Cybersecurity Strategies and the EU average. 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 Union under Article 18 of NIS2 will continue.

This cross cutting activity leads ENISA's efforts towards delivering the cybersecurity index (INDEX) and policy analyses to better map the needs of MSs and their requirements, which can be used for programming activities 2 and 3. The added value of this activity is to support the decision-makers in evidence-based policy-making, 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. Value can also be added by using, among other sources, information from foresight, incident reporting and vulnerabilities in collaboration with Activities 4, 5 and 8.

Activity 1 leads the Index service package and support the NIS, TREX and CERTI service packages.

The legal basis for this activity is Articles 5 and 9 of the CSA and Article 18 of the NIS2.

Link to strategic objective (ENISA strategy)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective and consistent implementation of EU policies for cybersecurity
- Foresight on emerging and future cybersecurity opportunities and challenges

Indicator for strategic objectives



- Uptake of recommendations stemming from NIS2 Article 18 report.
- Number of identified future and emerging areas reflected in the policy initiatives and interventions

¹ - Initiatives on NIS2 sectors such as space, health, AI, data spaces, digital resilience and response to current and future crises.

ACTIVITY 1 OBJECTIVES

Description	Csa Article And Other Eu Policy Priorities	Timeframe Of Objective	Indicator	Target
1.A By end 2026 implement a policy monitoring and analysis framework that delivers relevant and regular as well as ad hoc support and assistance to national and Union policymakers in cybersecurity	Art 5 CSA; Art 9 CSA	2026	Assessment of ENISA advice on EU policy (stakeholder survey, desktop research)	75% stakeholder satisfaction from ENISA's advice (among EU policy makers) By end of 2025 policy analysis framework is endorsed
1.B By Q3 2026 and in collaboration with Activity 2, ensure that two-thirds of policy observations within the first State of Cybersecurity in the Union report have been realised	Art 18 NIS2	2026	Assessment of MSs use of the Art 18 report (stakeholder survey, desktop research)	Two-thirds of MSs are using Art 18 report as input for their cybersecurity strategies All MSs use ENISA support and tools for the work on their NIS Strategies

ACTIVITY 1 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2025
1.1 Assist MSs to implement, assess and review National Cybersecurity Strategies and policies. Enhance a culture of trust and cooperation among MSs, also through peer reviews and by developing a code of conduct.	Stakeholders receive technical advice with the evidence needed for policy-making activities and the definition of implementation measures	Union Institutions (COM, EP, Council) NIS CG, including relevant work streams NLOs, including relevant sub-groups	Develop and pilot peer review framework, including code of conduct		n/a	By end of 2025 both endorsed
1.2. Collect and present relevant evidence by maintaining and developing EU cybersecurity index and State of Cybersecurity in the Union report.			Assessment of ENISA advice on EU policy	Biennial Survey, annual dialogues, and annual desktop research	93%	>90% stakeholder satisfaction
1.3. In coordination with Activities 2, 4 and 8, develop and maintain analyses on time-sensitive observations offering technical advice for policy development.			Assessment of timeliness of advice provided during policy development		n/a	>70% stakeholder satisfaction with timeliness

Stakeholders and Engagement Levels



Partners: Union institutions such as DG CNECT, other DGs, HWPCI, EP ITRE, MSs cybersecurity authorities, NIS Cooperation Group and relevant work streams, ENISA National Liaison Officers and subgroups;

Involve / Engage: Operators of NIS2 and industry associations/representatives

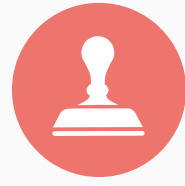
ACTIVITY 1 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 353 037 ²	FTE: 10 ³

2 - of which €59 000 centralised to missions and the budget for large-scale events.

3 - Target FTEs.

ACTIVITY 2: Cybersecurity and resilience of critical sectors⁴



Overview of activity



This activity supports Member States and EU Institutions with the implementation of the NIS2. The objectives of this activity are the rapid and harmonised implementation of NIS2, to increase the maturity of NIS sectors and to ensure NIS2-aligned implementation of sectorial resilience policies, such as DORA for resilience in the finance sector and the Network code for the cybersecurity of cross-border electricity flows. This activity includes an annual check on the implementation of policy, which relies on direct information from companies in the NIS sectors.

Under this activity ENISA provides support to the workstreams of the NIS Cooperation Group and the implementation of the NIS CG work programme. In this period the focus is on supporting the transposition of NIS2, the NIS2 implementing acts and the implementation of new tasks under NIS2 such as the EU registry for digital infrastructure entities. ENISA's goals here are to develop effective NIS2 frameworks for risk management, security measures and incident reporting, which can also be used beyond the NIS2, for example, under DORA, creating a single framework or approach for risk management, security measures and incident reporting in the EU.

Secondly, ENISA supports MSs and the Commission by addressing specific threats and risk scenarios for the Union, such as by supporting the 5G toolbox process and other Union coordinated risk evaluations such as Nevers, the Council Cyber Posture⁵, the Union's coordinated assessments of supply chain risks (under the NIS2), and the Union's coordinated preparedness tests (aka resilience stress tests, under the Cyber Solidarity Act). After supporting the MSs and Commission with developing the necessary frameworks, methodologies and scenarios, in 2026 ENISA will also support the MSs and the Commission with carrying out a Union coordinated preparedness test of resilience and a Union coordinated assessment of supply chain risks. Alignment with Activity 8 will be a priority. It would also support potential work conducted by the EU and Member States on the security and resilience of submarine cables, under existing (NIS2, CERG) or future cooperation bodies.

Thirdly, the activity also addresses sector-specific issues, working with sectorial stakeholders in the NIS sectors, providing targeted service bundles ('sustain', 'build', 'involve', 'prepare') depending on the needs of each sector. For each sector, ENISA will support a working group of relevant national authorities, but also engage with the industry either by supporting EU ISACs or by organising industry events to facilitate public-private dialogue on cybersecurity. Besides supporting the four highly critical sectors, namely telecoms, energy-electricity, finance and the Internet's infrastructure (aka core Internet), ENISA also supports sectors with low to medium levels of maturity, such as health, rail and public administration. This activity provides important sectorial input to other SPD activities, such as cyber exercises and training (Activity 3) and situational awareness (Activity 5).

Finally, there is a dedicated output for checking the implementation of these policies, by directly surveying companies in the NIS sectors to ensure that the NIS2 sectorial rules and other *lex specialis* do not only remain on paper but actually improve the level of security in the NIS sectors, producing the annual NIS investments report, the annual NIS 360 and sectorial cyber risk posture briefs, which give an overview of the posture of different NIS sectors. This output provides important sectorial input to the State of Cybersecurity in the Union report (Activity 1).

This activity leads the NIS service package and contributes to the INDEX, TREX and SITAW service packages. The legal basis for this activity is Articles 5 and 6 (1)(b) of the CSA.

4 - The term critical sectors is used in this context to cover ALL sectors within the scope of NIS2.

5 - [st09364-en22.pdf \(europa.eu\)](#).

Link to strategic objective (ENISA strategy)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective and consistent implementation of EU policies for cybersecurity

Indicator for strategic objectives










Uptake of ENISA recommendations to support Member States and stakeholders in implementing EU legislation

ACTIVITY 2 OBJECTIVES

Description	Csa Article And Other Eu Policy Priorities	Timeframe Of Objective	Indicator	Target
2.A By 2026 pilot and by end 2027 implement common frameworks and joint tools for NIS2 in the areas of (a) risk management, (b) security measures and (c) incident reporting for all EU sectors, and in line with industry best practices and international standards.	CSA Article 5, Article 6 and NIS2	Development of frameworks 2025	Framework's development	2 frameworks developed
		Frameworks pilot by 2026	Implementation of pilot programme (number of sectors piloting the frameworks, feedback scores on the usability)	20 MSs to adopt/use/endorse the frameworks
		Full implementation by 2027		>75% usability score
2.B Provide continuous comprehensive support to MS for implementing Union's regulatory requirements on cybersecurity and raising resilience across critical sectors.	CSA Articles 5 and 6 and NIS2	2027	Requests received by the NIS CG or MSs or other community groups	>80% of requests received have been resolved for a maximum of 20 requests
				>75% satisfaction with ENISA support over period
2.C By end 2027, help to increase the overall maturity level of critical sectors under NIS 2.	CSA Article 5 [possibly NCCS]	2027	Assessment of maturity based on updated NIS360 methodology	>2 sectors improving maturity

ACTIVITY 2 OUTPUTS

 Description	 Expected Results Of Output	 Validation	 Output Indicator	 Frequency (Data Source)	 Latest Results	 Target 2025
2.1 Support Member States in their implementation of the NIS2	NIS2 frameworks for risk management, security measures and incident reporting achieving harmonisation	DG CNECT, NIS CG	Framework usage	Annual (Internal count)	n/a	10 MSs to adopt, use or endorse the frameworks
			EU register for digital entities is used by all MSS	Annual (Report)	n/a	20 MSs to use the registry
			Alignment between DORA and NISD2	Satisfaction survey	n/a	>80%
2.2 Support Member States with EU toolboxes, EU coordinated risk evaluations, and EU coordinated preparedness tests	Support Union-wide risk evaluations and risk scenarios and their follow-up (5G, Nevers) Coordinated risk assessment of critical supply chains	DG CNECT, NIS CG	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Risk assessment framework for critical supply chains	Annual (Internal count)	n/a	One coordinated risk assessment for one domain or sector
			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 CNECT, NIS CG, Sectorial EU ISACS, sectorial EU agencies	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of critical sectors increasing maturity (from build to sustain or involve - NIS360)	Annual (Internal count)	3	5
			Number and frequency of services or workflows delivered to NIS sectors according to the maturity of the sector	Annual (Internal count)	21	24
2.4 Perform an annual check on policy implementation	MSs and EU institutions, both horizontal and sectorial stakeholders, use the NIS investments, the NIS360 and the cyber posture briefs as reference documents for policy-making.	DG CNECT, NIS CG, Sectorial EU ISACS, sectorial EU agencies	Stakeholder satisfaction	Biennial (Survey)	94%	>90%
			Number of critical or essential sectors covered by NIS Investments	Annual (Internal count)	10 subsectors covered	12 subsectors covered
			Number of critical sectors assessed by NIS360 and cyber posture briefs	Annual (Internal count)	10	12
			Implementation tracker	Annual (Internal count)	n/a	Five requests stemming from the implementation of NIS2 in MSS

Stakeholders and engagement levels



Partners: CNECT, NIS CG, National competent authorities, Sectorial DGs, Sectorial EU agencies, National competent authorities, Sectorial ISACs

Involve / Engage: NLOs, essential and important entities in the scope of NIS2 and industry associations/ representatives

ACTIVITY 2 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 468 024⁶	FTE⁷: 12

6 - of which €137,000 centralised to missions and the budget for large-scale events .

7 - Target FTEs.

ACTIVITY 3: Capacity Building



Overview of activity



This activity seeks to improve the capabilities of Member States, Union Institutions, bodies, and agencies, as well as, public and private stakeholders from NIS 2 Sectors. It focuses on improving stakeholders' resilience and response capabilities, enhancing their skills and behavioural change with regards to cyber hygiene, and increasing their preparedness.

Following an integrated approach and on the basis of the European Cyber Security Skills Framework (ECSF), capacity building is achieved by developing and conducting large-scale and/or sectorial exercises and training, designing and executing awareness raising programmes on cybersecurity risks and good practices, and by facilitating gamified Capture the Flag (CTF) competitions at national and EU level.

Secondly, this activity contributes to Agency's reporting duties on the current State of Cybersecurity in the Union (NIS2 Article 18) by providing insights on the cybersecurity capabilities of private and public stakeholders and on the cybersecurity awareness and hygiene of citizens. In that context, the activity will contribute to the INDEX (activity 1) by developing indicators and collecting relevant data to measure the progress towards closing the cyber talent gap, in line with the EC Communication on the Cybersecurity Skills Academy.

Thirdly, this activity will maintain and regularly update the European Cybersecurity Skills Framework (ECSF) by engaging with the relevant communities and stakeholders (in cooperation with activities 1, 2, and 4). On the basis of ECSF, it will develop, deploy, promote and maintain tools, frameworks and material that enable stakeholders, in particular NIS sectors, to independently execute their own cybersecurity capacity building programmes using ENISA's services through a pricing model.

Furthermore, the Agency, in collaboration with relevant EUIBAs and operational communities in Members States, will conduct a limited number of targeted exercises and training sessions focusing on empowering the trainers with the intention to enhance the resilience, maturity and preparedness of NIS sectors (in cooperation with activities 2, 4 and 6). In addition, the Agency will step up its efforts to support the development of new cybersecurity professionals through gamified cybersecurity training sessions (such as Team Europe training) and educational programmes in cooperation with National Competence Centres (NCCs) and other relevant stakeholders.

The plan is to gradually transfer knowledge and empower MSs, in particular NCCs, national operational communities and the ECCC, and to organise and financially support CTF training sessions at national and EU level with ENISA maintaining a facilitating role.

The previous output 9.2 (Promote cybersecurity topics and good practices) from work programme 2024 has been suppressed in 2025 in order for the resources to be re-allocated to higher priority tasks.

This activity leads the TRES service package and supports the INDEX, SITAW and NIS service packages.

The legal basis for this activity is Articles 6, 7(5) and 10 of the CSA, Art 18(1) of NIS2, Article 10 of CRA and Article 10 of REU⁸.

8 - REGULATION (EU, Euratom) 2023/2841

Link to strategic objectives (ENISA STRATEGY)



Empowered communities in an involved and engaged cyber ecosystem
 Strong cybersecurity capacity within the EU

Indicator for strategic objectives










Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, training sessions)
 Percentage of MSs that use the European Cybersecurity Skills Framework

ACTIVITY 3 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
3.A Maintain and regularly update the European Cybersecurity Skills Framework (ECSF)	EU Communication on Cyber Security Skills Academy Article 10 and 6	2027	Number of MSs endorsing the updated ECSF framework	23
			Stakeholder satisfaction rate	95%
3.B Between 2025-2027, enhance the cybersecurity skills and capabilities of at least 100 000 professionals in the EU	CSA Articles 4, 6, 7(5) and 10 CRA Article 10 REU Article 10	2027	Number of professionals whose skills have been directly or indirectly improved by capacity building activities	100 000 professionals
			Satisfaction survey of stakeholders on ENISA's capacity building activities	70%
3.C Between 2025-2027, ensure that ENISA has put in place frameworks to support the development of at least 100 000 additional cybersecurity professionals in EU	CSA Articles 4, 6, 7(5) and 10 CRA Article 10 REU Article 10	2027	Stakeholder satisfaction survey on new frameworks put in place	75%

ACTIVITY 3 OUTPUTS

 Description	 Expected Results Of Output	 Validation	 Output Indicator	 Frequency (Data Source)	 Latest Results	 Target 2025
3.1. Support the adoption and uptake of EU's Cybersecurity Skills Framework	<p>Review and update ECSF in line with the CyberSkills Academy Communication</p> <p>Measure and report on the skills gap, including developing indicators to be used for INDEX and Article 18a</p> <p>Promote the adoption of ECSF in MSs, in training organisations and academia and ensure its regular update.</p>	<p>AHWG on Cybersecurity Skills,</p> <p>ECCC WG 5 on Skills</p>	<p>Stakeholder satisfaction</p> <p>Number of MSs endorsing ECSF</p> <p>Number of training organisations endorsing ECSF in their training programmes</p>	<p>Biennial (Survey)</p> <p>Annual</p> <p>Annual</p>	<p>91%</p> <p>n/a</p> <p>n/a</p>	<p>95%</p> <p>10</p> <p>15</p>
3.2. Organise targeted exercises and support stakeholders to plan, execute their own exercises	<p>Organise a set of limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders</p> <p>Develop, deploy and promote exercises tools and frameworks that enable stakeholders, in particular in NIS2 sectors, to independently execute their own cybersecurity exercises</p> <p>Develop a community of 'train the planners' that leverages the tools, platforms and frameworks developed by ENISA</p>	<p>NLO Network (as necessary)</p> <p>CSIRTs Network (as applicable)</p> <p>EU-CyCLONe members (as applicable)</p> <p>NIS Cooperation Group (as applicable)</p> <p>EU ISACs (as applicable)</p> <p>NLO subgroup of Cyber Europe planners (as applicable)</p> <p>CERT EU</p>	<p>Number of people impacted directly and/or indirectly by exercises organised by ENISA</p> <p>Number of sectorial authorities, including EUIBAS, using ENISAs exercise solutions and frameworks</p> <p>Number of MSs participating in the community of 'train the planners'</p>	<p>Annual (Report)</p> <p>Annual</p> <p>Annual</p>	<p>n/a</p> <p>n/a</p> <p>n/a</p>	<p>>7.000</p> <p>5</p> <p>10</p>
3.3. Organise targeted trainings and awareness programmes and support stakeholders to plan, execute their own trainings / programs	<p>Develop, deploy and promote trainings and awareness raising tools, frameworks and content that enable stakeholders, in particular NIS2 sectors, to independently execute their own training or awareness raising programmes</p> <p>Develop a community of 'train the trainers' that leverages the tools, platforms and frameworks developed by ENISA</p> <p>Harmonise training activities sponsored by Cyber Security Support Action</p>	<p>NLO Network (as necessary)</p> <p>CSIRTs Network (as applicable)</p> <p>EU-CyCLONe members (as applicable)</p> <p>NIS Cooperation Group (as necessary)</p> <p>EU ISACs (as applicable)</p> <p>NLO subgroup of Cyber Europe planners (as necessary)</p>	<p>Number of participants in ENISA online based training sessions</p>	<p>Annual (Report)</p>	<p>3800</p>	<p>4000 (depending on Support Action contribution)</p>

			Number of participants in ENISA's train-the-trainer and train-the-planner events	Annual (Report)	220	> 250
			Number of professionals impacted by ENISA's awareness raising in a box	Annual (Report)	n/a	10 000
3.4 Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)	Deliver the ECSC final Form and train an elite team representing Europe at the ICC Create challenges and a platform (OpenECSC) with access to potentially new cybersecurity professionals	ECSC Steering Committee NLO Subgroup	Number of countries represented in Team Europe cohort	Annual (Report)	24	26
			Number of users participating in OpenECSC and national CTFs, who are potentially new cybersecurity professionals	Annual (Report)	3 000	20 000

Stakeholders and engagement levels



Involve / Engage: Training organisations, private entities of NIS 2 sectors, CSIRTs Network and related operational communities, European ISACs, EU-CyCLONE members, Blueprint stakeholders, SOCs including National and Cross-border SOCs, National Competent Authorities through the NIS Cooperation Group Work Streams, AHWG on Awareness Raising and Education, AHWG on Skills, EEAS, DG NEAR, DG CONNECT, Cybersecurity professionals.

ACTIVITY 3 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 796 409⁹	FTE¹⁰: 12
Other supplementary contributions	EUR 120 000 from Service Level Agreement with EU-LISA to provide support on exercises	Other supplementary contributions

9 - of which €105 000 centralised to missions and the budget for large-scale events.

10 - Target FTEs.

ACTIVITY 4: Enabling operational cooperation



Overview of activity

This activity supports operational cooperation among Member States, Union 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, including the revision of the Blueprint. Under our NIS2 mandate, activity 4 provides expertise, organisational support, tools and infrastructure for both the technical layer (EU CSIRTs Network) and the operational layer (EU CyCLONe - Cyber Crises Liaison Organisation Network) of Union operational cooperation networks.

Secondly, the activity aims to enhance interaction and trust between these two layers, the NIS Cooperation Group, and the HWPCI. ENISA supports operational communities by developing and maintaining secure and highly available networks, IT platforms, and communication channels. This includes developing the EU Vulnerability Database and launching the CRA Single Reporting Platform. The activity is also internally responsible for structured cooperation with CERT-EU and as such to identify and act upon synergies between the Agency and Member States' work and the work of the IICB and CERT-EU.

Thirdly, this activity manages the ENISA Cyber Partnership Programme and information exchange with security vendors and non-EU cybersecurity entities. ENISA will contribute to the next steps in enhancing the EU's cyber crisis management framework following the NIS2 and the 2022 Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, complementing the EU's coordinated response to large-scale cybersecurity incidents and crises. In addition, this activity supports the ENISA Cybersecurity Support Action. This activity will also provide for the delivery of the tasks mandated by the Cyber Solidarity Act within the Cybersecurity Incident Review Mechanism (at the request of the Commission or national authorities - the EU-CyCLONe or the CSIRTs network). ENISA will be responsible for the review of specific significant or large-scale cybersecurity incidents and will be required to deliver a report that includes lessons learned and, where appropriate, recommendations to improve the Union's cyber response.

Fourthly, the activity also maintains IT systems and platforms for all ENISA's operational activities and develops a comprehensive knowledge and stakeholder management system. This activity facilitates synergies with national cybersecurity communities (including civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors, such as CERT-EU, EC3 and EEAS, to exchange knowledge and best practices, provide advice and issue guidance.

Finally, this activity will also seek to contribute to the Union's efforts to cooperate with third countries and international organisations on cybersecurity, including revising ENISA's international strategy and stakeholder strategy.

This activity supports SITAW, INDEX and NIS service packages.

The legal basis for this activity is Articles 9, 10, 11, 12, 14, 15, 16 and 17 of NIS2, Articles 6, 7, 12 and 16 of the CSA and Article 11 of the CSOA (final text pending).

Link to strategic objectives (ENISA STRATEGY)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective Union preparedness and response to cyber incidents, threats and cyber crises
- Consolidated and shared cybersecurity information and knowledge support for Europe

Indicator for strategic objectives



Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks








EU Vulnerability Database is operationalised by ENISA resulting in a high satisfaction rate (by MSs and stakeholders) with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threat

ACTIVITY 4 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
4.A By end 2026, strengthen the interaction and trust within and between key EU operational and cybersecurity communities (CSIRTs Network, EU-CyCLONe, HWPCI and NIS Cooperation Group)	Articles 7, 10, 15 and 16 NIS2 Articles 6 and 7 CSA Article 16 CRA Article 11 CSOA ¹¹	2026	Assessment of high level of operational interaction across CSIRTs Network, EU-CyCLONe, HWPCI and NIS Cooperation Group	>60% of stakeholders agree that ENISA has enabled the functioning of or supported the building of trust within the network
			ENISA is judged as a key enabler of trust within and between CSIRTs Network, CyCLONe, HWPCI and NIS Cooperation Group	>60% of stakeholders agree that ENISA has enabled interaction and trust between the networks and communities
4.B Review and implement both the ENISA stakeholder strategy and ENISA international strategy	Article 12 CSA	2026	Coherence of ENISA international engagement with the Agency's strategy	Updated international strategy
			Comprehensive knowledge management and stakeholder management system is established	Established framework for knowledge management and stakeholder management
4.C Develop and maintain relevant operational IT systems and platforms to support all operational communities and enhance synergies	Articles 7, 10, 12, 15 and 16 NIS2 Article 7 CSA Article 16 CRA	2026	Relevant IT systems are maintained and new mandatory platforms are developed	IT Operations are consolidated and synergy plan designed (2025) and implemented (2026)

11 - Final text pending at time of editing.

ACTIVITY 4 OUTPUTS

 Description	 Expected Results Of Output	 Validation	 Output Indicator	 Frequency (Data Source)	 Latest Results	 Target 2025 ¹²
4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs network and eu-cyclone members HWPCI and NIS cooperation group	Enhanced information sharing and cooperation among the CSIRTs network and eu-cyclone members and enhanced interaction with HWPCI and NIS cooperation group	CSIRTs Network and EU-CyCLONe members, HWPCI and NIS Cooperation Group	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	>60% use of platforms
			Number of joint sessions established	Annual (report)	1 joint session per year.	2 joint sessions per year with operational outcomes
4.2 Maintain, develop and promote the ENISA Cyber Partnership programme to enable the exchange of information to support the Agency's understanding of threats, vulnerabilities, incidents and cybersecurity events	Operationalisation of the Cyber Partnership Programme	CSIRT Network, EU CyCLONe, EUIBAs, HWPCI, MB	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Number of new and total partners in the ENISA partnership programme	Annual (report)	4	6
			Percentage of RFI answered by members of partnership programme	Annual (report)	n/a	65%
4.3 Implement ENISA's international strategy and outreach	EU values recognised by international stakeholders	MT, EEAS, COM (and MB as required)	Stakeholder satisfaction	Biennial (survey)	91%	1% increase (from previous year – decrease in duplication)
	International cooperation supports ENISA objectives		Staff satisfaction with international coordination	Annual (survey)	n/a	>80%
4.4 Develop comprehensive CVD platforms by operationalising the EU Vulnerability Database and designing the CRA Single Reporting Platform	EU VD is deployed	CSIRTs Network.	Stakeholder satisfaction	Biennial (survey)	N/A	66% by 2027
	CRA Single Reporting Platform is being developed					

12 - Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023.

4.5. Develop and maintain IT systems and platforms for operational activities	Consolidation of operational IT with view to supporting ENISA operations	CSIRTs Network and CyCLONe members, HWPCI and NIS Cooperation Group and Business owners for ENISA's Operational IT systems	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			IT architecture for external operational IT services	Biennial update	n/a	Completed by end of 2025
			ENISA operational IT	Annual (report)	n/a	All operational IT systems are consolidated under one IT operational manager by 2025 One third of current systems are updated every year to reach 100% in 2027
			EU Vulnerability Database	Annual (report)	n/a	EU Vulnerability Database is produced and users are trained
			CRA Single Reporting Platform	Annual (report)	n/a	Technical specifications of the CRA Single Reporting Platform are available and the service provider is contracted to start implementation
4.6 Development of stakeholder and knowledge management systems and frameworks			Stakeholder satisfaction with knowledge management and stakeholder management system	Biennial (survey)	n/a	>60% by 2026

Stakeholders and engagement levels



Partners: Blueprint actors, EU decision-makers, institutions, agencies and bodies, CSIRTs Network Members, EU-CyCLONe Members, HWPCI and NIS Cooperation Group SOCs including National and Cross-border SOCs

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

ACTIVITY 4 RESOURCE FORECAST

	Budget	FTEs
Total activity resources	Budget: EUR 1 652 091¹³	FTE¹⁴: 15

13 - of which €115 000 centralised to missions and the budget for large-scale events .

14 - Target FTEs.

ACTIVITY 5: Provide effective operational cooperation through situational awareness



Overview of activity



This activity contributes to cooperative preparedness and responses at the level of the Union and Member States through data driven analyses of threats and risks, operational and strategic recommendations based on the collection of incidents, information on vulnerabilities and threats in order to contribute to the Union's common situational awareness.

ENISA delivers on this activity by collecting and analysing security events, cyber incidents, vulnerability and threats based on its own monitoring, shared by external stakeholders due to legal obligations¹⁵ or voluntary shared. The Agency aggregates and analyses reports, ensuring information flow between the CSIRTs Network, EU-CyCLONE, and other technical, operational and political decision-makers at the Union level to increase situational awareness with the services of other EU entities such as relevant Commission services and in particular DG CNECT, CERT-EU, Europol/EC3, and EEAS including EU INTCEN. This activity actively benefits from ENISA's Cyber Partnership Programme managed under Activity 4 and the Agency's international cooperation frameworks.

Secondly, the activity includes the preparation of the regular in-depth EU Cybersecurity Technical Situation Report in accordance with CSA Article 7(6), also known as the EU Joint Cyber Assessment Report (EU-JCAR), regular weekly OSINT reports, Joint Rapid Reports together with CERT-EU and other ad-hoc reports as needed. Under this activity the Agency prepares threat landscapes and provides topic-specific as well as general assessments on the expected societal, legal, economic, technological and regulatory impact, with targeted recommendations for Member States and Union institutions, bodies, offices and agencies. Under this activity, a semi-annual report in accordance with NIS 2 Article 23(9)¹⁶ is prepared and the work related to the Cyber Solidarity Act – Incident Review Mechanism (Article 18*) - is undertaken.

Thirdly, this activity also supports Member States with respect to operational cooperation within the CSIRTs Network and EU-CyCLONE by providing, at their requests, advice on a specific cyber threat, assisting in the assessment of incidents and vulnerabilities, facilitating the technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities using the EU Vulnerability Database and the Single Reporting Platform established under the Cyber Resilience Act. This activity is also responsible for preparing dedicated reports and threat briefings for the Council, in particular the HWPCI under the Cyber Diplomatic Toolbox.

In addition, this activity implements the agreements between ENISA and DG CONNECT for the contribution to the Commission Situation Centre project.

Finally, under this activity the work that underpins the establishment of the Single Reporting Platform as set up under the Cyber Resilience Act is carried out. In doing so, the Agency takes into account the frameworks for **incident reports** implemented under Article 23 of NIS2 and other relevant EU legislation to ensure alignment and to future proof the architecture for the simplification of reporting at the EU level.

This activity includes the continuous development and maintenance of a 24/7 monitoring and incident support capability in combination with activity 6.

The budget for this activity is partly financed through a contribution agreement between ENISA and the Commission to support the work on the CRA and CSOA (final text pending) as well a contribution to the Commission Situation and Analysis Centre.

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

The legal basis for this activity is Articles 5(6), 7(4)(6)(7) and 9 of the CSA, Article 23(9) of NIS2, Article 18 of the CSOA¹⁷ and Articles 14-17 of the CRA.

15 - NIS2, CRA and Regulation 2023/2841

16 - In 2025 this activity will fulfil the tasks under CSA Article 5(6) a, b and c. These reports will be superseded as provisions in NIS2 Art 23(9) apply.

17 - Final text pending at time of editing

Link to strategic objectives (ENISA STRATEGY)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective Union preparedness and response to cyber incidents, threats and cyber crises
- Consolidated and shared cybersecurity information and knowledge support for Europe

Indicator for strategic objectives



EU Vulnerability Database is operationalised by ENISA and a high satisfaction rate (by MSs and stakeholders) with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats Reporting platform under the CRA is established within 21 months of the entry into force of the Regulation and successfully operated.

ACTIVITY 5 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
5.A By end 2027 build a common situational awareness between Member States based on accurate shared data and underpinned by validated joint analysis	Article 7 of CSA	2025 - 2027	Content of JCAR is contributed and validated by Member States	Produce at least one comprehensive joint analysis report every quarter, contributed and validated by at least 75% of Member States (EU-JCAR)
	Article 23(9) of NIS2		ENISA Data repository is open to and includes also information directly provided by Member States	Data repository is accessible by MSs Percentage of information in the data repository validated or provided by MSs is above 75% and 100% or significant event impacting EU MSs
	Article 18 of CSOA ¹⁸		Establish and test processes and procedures for the Incident Review Mechanism under Article 18 of CSOA ¹⁹	Process for IRM is established and endorsed by MSs
5.B Provide regular and general as well as specific threat landscapes and threat analyses, based on observed data-driven trends in incidents and vulnerabilities	Article 9 of CSA	2025 - 2027	Produce ENISA Threat Landscapes	Maintain the regular publishing schedule for general threat landscape reports (yearly) and specific threat analysis and sectorial reports (e.g. bi-monthly).
	Article 7 of CSA		JCAR includes threat analysis based on incidents and vulnerabilities available within ENISA data repositories (EUVDB, CIRAS, CRA SRP)	Incident analysis is included in JCAR as of Q3 2025 EUVDB vulnerability analysis is included by Q2 2025 CRA SRP AEV and incidents analysis are included by Q4 2026
	Article 23(9) of NIS2		Ability of ENISA to produce accurate threat analyses based on incidents, vulnerabilities and threat information based on the Agency's own monitoring, shared by external stakeholders due to legal obligations ²¹ , or voluntarily shared,	80% of Member States score quality of threat analyses provided by ENISA above 4 (on scale 1-5) 80% of Member States score ability of ENISA to use available information to produce threat analyses and recommendations above 4 (on scale 1-5)
	Article 18 of CSOA ²⁰		CRA SRP is established and operational	CRA SRP is used to carry on tasks under CRA by end of 2026
	Articles 14-17 CRA			


18 - Final text pending at time of editing.

19 - Final text pending at time of editing.

20 - Final text pending at time of editing.

21 - NIS2, CRA and Regulation 2023/2841.

ACTIVITY 5 OUTPUTS

 Description	 Expected Results Of Output	 Validation	 Output Indicator	 Frequency (Data Source)	 Latest Results	 Target 2025
5.1 Collect, organise and consolidate information (including from the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, operational and technical levels ²²	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, Union entities, National Authorities within MSs subscribed to the products	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Timeliness and Accuracy of reports	Annual (survey)	n/a	>85%
5.2 Provide analysis and risk assessment jointly with other operational partners including EUIBAs, Member States, industry partners, and non-EU partners	Union joint assessment and reports, sectorial analysis, threats and risk analysis. ²³ Recipients receive accurate and timely assessment of threat actors and associated risks to the EU Internal Market	CSIRT Network, EU CyCLONE, Union entities, HWPCI, Management Board	Stakeholder satisfaction	Biennial (survey)	84%	>90%
			Number of contributing MSs to EU JCAR	Annual (report)	n/a	>40%
5.3 Collect and analyse information to report on cyber threat landscapes	Mapping threats, Generating recommendations for stakeholders to take up	NLO, AG and Cybersecurity Threat Landscape AhWG CSIRTs Network	Stakeholder satisfaction	Biennial (survey)	91,5%	>5% compared to 2023
			Number of downloads of ETL	Annual (report)		>5% increase year on year
5.4. Analyse and report on incidents as required by Article 5(6) of CSA as well as other sectorial legislation (e.g. DORA, eIDAS Art 10, etc.)	Analysing incidents Generating recommendations for stakeholders to take up	WS3 of the NISD CG, ECASEC and ECATS groups	Stakeholder satisfaction	Biennial (survey)	91,5%	>5% compared to 2023
5.5 Developing the CRA Single Reporting Platform and operationalise EU vulnerability database	CRA SRP platform work is scoped and implementation is initiated Operational and business processes are defined together with primary stakeholder	CSIRT Network	Operational processes expected for 2025 are defined Implementation work is started.	Survey	n/a	80% of the stakeholders agree on the established process and score them >4

22 - Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.

23 - Including JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and CNECT Situation Centre.

Stakeholders and engagement levels



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

Involve / Engage: Other types of CSIRTs and PSIRTs, private sector industry.

ACTIVITY 5 RESOURCE FORECAST

	Budget	FTEs
Total activity resources from direct annual budget	Budget: EUR 1 566 118 ²⁴	FTE ²⁵ : 13 ²⁶
Other supplementary contributions	Budget: TBD (outputs 5.1 and 5.2) ²⁷ and TBD ²⁸ for CRA Platform	2 ²⁹
Other supplementary contributions on-going	Budget: (outputs 5.1 and outputs 5.2) forecast EUR 223 000 from existing contribution agreement signed in 2023	2 ³⁰

24 - Of which €90 000 centralised to missions and the budget for large-scale events.

25 - Target FTEs, Current Staff 12 plus foreseen 2 FTE for CRA SRP and 1 FTE for Incident Review Mechanism.

26 - Including 2 FTE – Contract Agents are hired through the Contribution Agreement signed with Commission in 2023 under Cybersecurity Support Action and Situation Centre.

27 - Allocation depending on the final text of the contribution agreement to be signed with Commission in 2024. Allocation is expected to be 15 000 000 to support cybersecurity actions, situation centre and implementation of CRA single reporting platform. Please refer to annex XI for further details regarding contribution agreements, final text pending. The amount indicated refers to years 2025 to 2027.

28 - Allocation depends on the final text of the Contribution Agreements to be signed with Commission in 2024.

29 - FTE allocation depends on the final text of the Contribution Agreement to be signed with Commission in 2024.

30 - 2 FTEs – Contract Agents are hired through the Contribution Agreement signed with Commission in 2023 under Cybersecurity Support Action and Situation Centre.

ACTIVITY 6: Provide services for operational assistance and support



Overview of activity



The activity contributes to the further development of capabilities to prepare and respond at the level of the Union and Member States for 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 services such as penetration testing, threat hunting, risk monitoring and assessment, customised exercises and training, and supports the Member States in responding to incidents.

The Agency will leverage the lessons learned and the mechanisms that were put in place during the first year of the Cybersecurity Support Action in 2023. This will refocus the service catalogue as the processes and methodologies will be further adapted to better suit the needs of the Member States, allowing for more flexibility and scalability.

The types and level of services have been agreed with a single point of contact within each EU Member State and the final benefiting entities.

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

This activity is resourced through the use of 10 Contract Agents to be absorbed as a direct cost of the programme and financed through the Commission contribution agreement. ENISA would not be able to resource this activity within its current establishment plan. The budget for this activity is to be implemented during 2025 and 2026.

This activity will be adjusted when the Cyber Solidarity Act enters into force. According to the Cyber Solidarity Act, the Commission shall entrust, partly or fully, the administration and operation of the EU Cybersecurity Reserve to ENISA. The Reserve entails delivery of incident response services and it also includes the mapping of the services needed by the users of the Reserve, including the availability of such services for legal entities established and controlled by Member States.

The activity contributes to the SITAW, NIS, INDEX, TREX service packages.

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

Link to strategic objectives (ENISA STRATEGY)



- Empowered communities in an involved and engaged cyber ecosystem
- Effective Union preparedness and response to cyber incidents, threats and cyber crises

Indicator for strategic objectives



Operationalisation of the EU Cybersecurity Reserve of which the administration and operation is to be entrusted fully or partly to ENISA and used by MSs, EUIBAs and on a case-by-case basis by DEP associated third countries

ACTIVITY 6 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
6.A By end Q2 2026, deliver and complete ENISA support actions	Articles 6 and 7 of the CSA	2026	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. (survey) Complete tasks on time and in budget. (survey)	4 (1 to 5 score)
6.B. By end Q2 2026 and onwards, deploy European Cyber Reserve under CSOA.	Articles 6 and 7 of the CSA	2026	Reaching consensus with the EC on European Cyber Reserve. (survey) Timely deliver. (survey)	4 (1 to 5 score)

ACTIVITY 6 OUTPUT



Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2025
6.1 Provide penetration testing (pentest) and threat hunting services towards selected entities within EU Member States ³¹	Pentest and Threat Hunting services are delivered in a timely and accurate manner to MSs	MSS, CNECT, Beneficiaries	Percentage of MSs requesting the service Satisfaction score		n/a	50% >4
6.2 Provide customised exercises and training for selected entities within EU Member States	Customised exercise and training services are delivered in a timely and accurate manner to MSs	MSS, CNECT, Beneficiaries	Percentage of MSs requesting the service Satisfaction score		n/a	50% >4
6.3 Support risk monitoring and assessment for selected entities within EU Member States	ENISA is able to provide regular risk monitoring towards specific targets or at national level, including by leveraging commercial of-the-shelf platforms, as well as providing specific risk assessment and threat landscapes as requested by MSs	MSS, CNECT, Other beneficiaries	Percentage of MSs requesting the service Satisfaction score	Annual	n/a	50% >4
6.4 Support incident response and incident management of selected entities within EU Member States	ENISA provides 24/7 support for incident response to MSs	MSS, CNECT, other beneficiaries	Percentage of MSs requesting the service Support provided in a timely manner Satisfaction Score		n/a	50% >4

31 - The beneficiaries of Activity 5 services are specified in the Contribution Agreement.

Stakeholders and engagement levels



Partners: EU Member States, selected beneficiary entities, Commission

Involve / Engage: EU-CyCLONe, CSIRT Network, DG CONNECT

ACTIVITY 6 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources from direct annual budget	Budget: n/a	FTE: 4
Other supplementary contributions	Budget: TBD ³²	FTEs: TBD
Other supplementary contributions on-going	Budget: forecast EUR 9 773 866.89 from existing contribution agreement signed in 2023	9 FTEs financed from existing Contribution Agreement signed in 2023

³² - Allocation depending on the final text of the contribution agreement to be signed with the Commission in 2024. Allocation is expected to be EUR 15 000 000 to support Cybersecurity action, situation centre and implementation of the CRA single reporting platform. Please refer to annex XI for further details regarding contribution agreements, final text pending. The amount indicated refers to the years 2025 to 2027.

ACTIVITY 7: Supporting Development and maintenance of EU cybersecurity certification framework



Overview of activity



This activity encompasses actions that seek to establish and support the EU cybersecurity certification framework by preparing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commissioner on the basis of the Union Rolling Work Programme (URWP) or, in duly justified cases, at the request of the Commission or the European Cybersecurity Certification Group (ECCG). This also includes in particular the activities related to the certification of ID Wallets (support for national schemes and for the development of an EU scheme) as a priority, and other schemes under development (EUCS, 5G), as well as activities related to upcoming requests in line with the URWP, such as the one related to managed security services following entry into force of an amendment to the CSA. These actions also include supporting the maintenance and review as well as evaluation of the adopted European cybersecurity certification schemes, in particular the adopted scheme from EUCC, as well as capacity building for National Cybersecurity Certification Authorities (NCCAs), and supporting the peer review mechanism in line with the CSA and related regulations on implementation. In addition, in this activity, ENISA assists the Commission with regard to the European Cybersecurity Certification Group (ECCG) and existing ECCG sub-groups (EUCC review and maintenance; peer review; cryptographic mechanisms) as well as with co-chairing and providing a secretariat for the Stakeholder Cybersecurity Certification Group (SCCG).

ENISA has developed a one candidate scheme based on an EC request from 2019, in accordance with Article 49.2, which was adopted as an implementing regulation, the EUCC. ENISA is currently developing two other candidate schemes also based on EC requests, the EUCS and the EU5G, in accordance with Article 49.2. The URWP was adopted in Feb 2024, and a recent request received for the development of an EUDI wallet candidate scheme is in line with Article 49.1. In anticipation of a possible request for an EU scheme on MSS, as foreseen by the URWP and the amendment to the CSA, ENISA is developing a feasibility study. ENISA has also explored the possibility of the certification of AI, which is also highlighted in the URWP but for which no request for a candidate scheme is expected soon.

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 gradually 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 market aspects of certification as well as aspects related to the interplay with existing laws, in particular the Cyber Resilience Act. Other relevant pieces of legislation include NIS2, DGA EUDI Wallet, AI Act, Chips Act, Data Act.

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)



- Empowered communities in an involved and engaged cyber ecosystem
- Building trust in secure digital solutions

Indicator for strategic objectives



Number of EU certification schemes developed and maintained, number of EU regulations making reference to CSA, number of active Member States' NCCAs (e.g. issuing European certificates)

ACTIVITY 7 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe of objective	Indicator	Target
7.A Between 2025-2027, timely development of feasibility studies for future potential schemas	CSA Article 49	2027	Number of feasibility studies concluded in view of upcoming requests, including managed security services (on-going)	3 (pending potential new requests for scheme)
			Elements of feasibility study reflected/ aligned with EC request for new schemes	More than 50%
7.B. Between 2025-2027, timely finalisation of candidate schemes following formal requests for drafting new cybersecurity certification schemas	CSA Article 49	2027	Number of drafts of certification schemas delivered to COM (ID Wallet Certification and, pending formal COM request, Managed Security Services)	2
			ECCG endorsement of draft certification schemes	Positive ECCG endorsement
			SCCG opinion on draft certification schemes (satisfaction survey)	More than 60%
7.C Ensure the maintenance of existing schemes and support their roll-out	CSA Article 49	2027	Number of schemes maintained with active involvement by ENISA	1 (EUCC) + EUCS pending final approval
			Satisfaction by ECCG on ENISA's supporting efforts for documents for maintenance	75%
			Number of certificates issued and published under an EU certification scheme; high rate of use in the market.	Proportionate ³² number of certificates issued migrating to a new EUCC scheme compared to previous framework

ACTIVITY 7 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2025
7.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemas	Scheme meets stakeholder requirements, notably those of Member States and the Commission Take up of schemes by stakeholders Timely delivery by ENISA of all schemes requested in cooperation with the Commission Statutory Bodies and ad hoc working groups actively involved	Ad hoc working groups on certification	Stakeholder satisfaction	Biennial (survey)	82%	75%
		ECCG	Number of opinions of stakeholders managed	Annual (report)	n/a	100 opinion items per scheme
		European Commission	Number of people or organisations engaged in the preparation of certification schemes	Annual (report)	n/a	At least 20 ad hoc Working Group Members from third-party Experts; at least 15 Member States joining ad hoc Working Groups
7.2 Implementation and maintenance of established schemes including evaluation of adopted schemes, participation in peer reviews etc., monitoring the dependencies and vulnerabilities of ICT products and services	Review of schemes to improve efficiency and effectiveness Take up of schemes by stakeholders	ECCG	Stakeholder satisfaction	Biennial	82%	75%
		European Commission	ECCG satisfaction of ENISA efforts on schemes adopted	Triennial (survey)	n/a	75%
			Satisfaction with ENISA's role in NCCA peer reviews	Triennial (survey)	n/a	75%
7.3 Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks		ECCG	Stakeholder satisfaction	Biennial	82%	75%
		European Commission	Feedback from statutory bodies including NCCAs on ENISA's role	Annual (survey)	n/a	75%
		SCCG				

33 - ENISA monitors the certificates issued under SOG-IS and the transition to EU CC will have to be proportional to the number of certificates issued.

7.4 Developing and maintaining the necessary provisions, tools and services concerning the Union's cybersecurity certification framework (incl. certification website, supporting the Commission in relation to the core stakeholders service platform of CEF (Connecting Europe Facility) for collaboration, publication and promotion of the implementation of the cybersecurity certification framework etc.)	Transparency and trust in supporting ICT products, services and processes	ECCG	Stakeholder satisfaction	Biennial	82%	75%
		European Commission	User satisfaction with the services on the certification website	Annual (survey)	n/a	75%
	Stakeholders engagement in promotion of certification	SCCG	Use of the certification website	Annual (report)	n/a	75%

Stakeholders and engagement levels



Partners: EU Member States (including National Cybersecurity Certification Authorities, ECCG), European Commission, EU Institutions, Bodies and Agencies, selected stakeholders as represented in the SCCG.

Involve/ Engage: Private sector stakeholders with an interest in cybersecurity certification, Conformity Assessment Bodies, National Accreditation Bodies Consumer Organisations

ACTIVITY 7 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 697 089³⁴	FTE³⁵: 10

34 - of which €127 000 is centralised to missions and the budget for large-scale events.

35 - Target FTEs.

ACTIVITY 8: Supporting European cybersecurity market, research & development 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 for SMEs and start-ups, to reduce dependence from outside and increase the capacity of the Union and to reinforce supply chains to the benefit of the internal market. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation and the adoption of relevant codes of conduct. As such, this activity also seeks to lay the ground for an effective role for ENISA in the CRA, notably in terms of market analysis, the preparation of market sweeps, and the collection and analysis of information for the identification of emerging cybersecurity risks in products with digital elements, etc.

Secondly, the actions to support this activity include producing analyses and guidelines as well as good practices on cybersecurity and data protection requirements, including eIDAS2 and trust services, facilitating the establishment and take up of European and international standards across applicable areas such as risk management as well as performing regular analyses of cybersecurity market trends on both the demand and supply side including monitoring, collecting and identifying dependencies among ICT products, services and processes and vulnerabilities as well as incidents that have occurred. The activity aims at strengthening and reinforcing ties with the private sector and promoting collaboration among cybersecurity market players, in order to improve the visibility and uptake of trustworthy and secure ICT solutions in the digital single market.

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

To prepare this strategic advice, ENISA will take full account of past and ongoing research, the development and assessment of technology, outputs of other statutory bodies in the cybersecurity landscape such as the NIS Cooperation Group, ECCG, CSIRTs Network, EU-CyCloNe. The Agency will also scan the horizon for emerging and future technological, societal and economic trends that may have an impact on cybersecurity. In this respect, lessons learned and trends from reported incidents and vulnerabilities will also be used.

ENISA will also conduct regular consultations with relevant user groups, projects (including EU funded projects), researchers, universities, institutes, industry, start-ups and digital innovation hubs to consolidate information and identify gaps, challenges and opportunities in research and innovation from the various quadrants of the community. The ecosystem of the ECCC and the National Coordination Centres (NCCs) will be involved in these consultations. A strong collaboration with, and the mapping of the relevant requirements of, the market authorities as defined in the CRA will also take place in the context of this activity.

Finally, this activity supports cybersecurity certification and the assessment of the conformity of products with digital elements by monitoring the standards being used by European cybersecurity certification schemes and digital products, and by recommending appropriate technical specifications where such standards are not available.

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

The legal basis for this activity is Articles 8 and 11 and Title III of the CSA, as well as the CRA, the eIDAS2 Regulation, the AI Act (Article 67) and the Data Governance Act (Article 29).

Link to strategic objectives (ENISA STRATEGY)

- Empowered communities in an involved and engaged cyber ecosystem
- Building trust in secure digital solutions
- Foresight on emerging and future cybersecurity opportunities and challenges



Indicator for strategic objectives



Rate of satisfaction with ENISA's support for the implementation of the CRA (Market Supervisory Authorities MSAs) and European cybersecurity certification framework (ECCG), number of advisories and the level of support given on Research and Innovation Needs and Priorities for the ECCC and its uptake by the ECCC

ACTIVITY 8 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
8.A By end 2026, implement a 'market' monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, reports on the trustworthiness of critical products and services with digital elements under the CRA	CRA (final text pending)	2026	Timeliness of ENISA reports	Reports delivered on time
			Acceptance of ENISA reports by MSs	2/3rds of MSs endorsing ENISA reports
			Validity of ENISA framework	All MSs validating and endorsing ENISA framework
8.B Provide continuous comprehensive support to MSs' market supervisory authorities and to the COM for implementing CRA requirements	CRA (final text pending)	2026	MSs and COM stakeholder satisfaction survey	More than 70%
8.C. Create a technology and innovation radar, to understand the level of impact that new technologies are having on cybersecurity	CSA Article 9 and CRA (final text pending)	2026	Number of cybersecurity trends and patterns accurately identified through an evidence-based methodological approach	5% increase over reference data
			Assessment of impact of EU cybersecurity R&I	5% increase over reference data

ACTIVITY 8 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2025
8.1 Collect and analyse information on new and emerging information and communications technologies and provide strategic advice to ECCC on the EU agenda on cybersecurity research, innovation and deployment	Identifying current and emerging ICT gaps, trends, opportunities and threats Advising EU Funding programmes including the ECCC and its Strategic Agenda and Action Plan	Academia, Industry and National R&I, MSs market authorities, Entities (including NCCs) and EUIBAs EC including CNECT and JRC, ECCC and NCCs, as appropriate	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Findings endorsed by MSs (NCCs and market authorities)	Annual	n/a	> 60%
			Alignment with ECCC Strategic Agenda and Action Plan	Annual (survey with ECCC GB)	n/a	> 60%

8.2. Market analysis of the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes and prepare biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements	Improved understanding of the market and industry	Ad hoc working groups for cybersecurity market analysis ECCG (as necessary) SCCG Advisory Group NLO (as necessary) MSs Market authorities	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Cybersecurity market analysis; cybersecurity products and services	Annual (report)	n/a	All reports produced as planned (Y out of Y reports)
			Endorsement by MSs of report on emerging trends regarding cybersecurity risks in products with digital elements	Biennial (report)	n/a	27 MSs endorse report
8.3 Support activities of market surveillance authorities and identification of categories of products for simultaneous coordinated control actions and, upon request, conduct evaluations of products that present a significant cybersecurity risk	Produce a catalogue of market surveillance authorities; survey requirements of market surveillance authorities; identify categories of products; produce a methodology on market sweeps; carry out market sweeps Evaluations to be carried out ideally on the basis of input from market sweeps; rely on external expertise. This output should be carried out under A7 Certification	NLO / NCCA Commission SCCG (as appropriate)	Collection of requirements Matching requirements with deliverables Time to carry out market sweeps Methodology for evaluations Profiles of experts	Catalogue, survey and categories of products in 2025-26 Market sweeps as from 2027 (3-year transition) or earlier if requested Method to evaluate products Guidance and criteria to accept evaluation results	n/a	Stakeholder satisfaction above 60%
8.4 Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification	Alignment with standards	SCCG Advisory Group NLO (as necessary)	Stakeholder satisfaction	Biennial (survey)	88%	60%
			Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification	Annual (report)	n/a	All reports produced as planned (Y out of Y reports)

Stakeholders and engagement levels



Partners: EU Member States (including market authorities and entities with an interest in cybersecurity market monitoring, e.g. NCCA, National Standardisation Organisations), European Commission, EU Institutions, Bodies and Agencies, European Standardisation Organisations (CEN, CENELEC, ETSI), Private sector or ad hoc Standards Setting Organisation, EC-Joint research centre, National and EU R&I Entities, Academia and Industry, European Cybersecurity Competence Centre and National Cybersecurity Coordination Centres.

Involve / Engage: Private sector stakeholders (entrepreneurs, start-ups and investors) with an interest in cybersecurity market and/or standardisation, International Organisation for Standardisation / International Electrotechnical Committee, Consumer Organisations.

ACTIVITY 8 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 697 887³⁶	FTE³⁷: 10

36 - Of which €134 200 centralised to missions and the budget for large-scale events.

37 - Target FTEs.

1.2. CORPORATE ACTIVITIES

Activities 9, 10 and 11 encompass enabling actions that support the operational activities of the agency.

ACTIVITY 9: Performance and sustainability



Overview of activity



This 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 inter alia an efficient performance and risk management framework and the development of single administrative practices as well as the promotion of sustainability across all the Agency's operations. In addition in line with Article 4(2) of the CSA this activity includes contributions to gains in efficiency, e.g. via shared services in the EU Agencies network and in key areas by relying on the Agency's own expertise (e.g. cybersecurity risk management).








Under this activity ENISA seeks to deliver, as a service-centric and sustainable organisation, key objectives of the Agency's Corporate Strategy by establishing a framework for the thorough assessment of quality, ensuring proper and functioning internal controls and compliance checks, as well as maintaining a high level of cybersecurity across all the Agency's corporate and operational activities. In terms of resource management, the Budget Management Committee coordinates the Agency's adherence to the principles of financial management. In the area of IT systems and services, the IT Management Committee coordinates and monitors the comprehensive application of the Agency's IT strategy and adherence to applicable 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, Article 41 and Articles 32 to 33 (re ENISA's financial rules and combatting fraud).

ACTIVITY 9 ANNUAL OBJECTIVES

Description	Link To Corporate Objectives	Activity Indicators	Frequency (Data Source)	Latest Result	Target
9.A Enhance corporate performance and strategic planning	Ensure efficient corporate services	Proportion of SPD KPIs meeting targets	Annual	13 metrics were unchanged, 21 underperformed and 58 overperformed	>80 of indicators overperformed
	Continuous innovation and service excellence	Results of assessment of Internal control framework	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%
9.B Increase corporate sustainability	Ensure climate neutral ENISA by 2030	Maintain EU Eco-Management and Audit Scheme (EMAS)	Annual	n/a	Implement follow up actions to ensure EMAS certification is maintained
	Develop efficient framework for ENISA's continuous governance to safeguard a 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 identified across IT systems within Agency	Annual	n/a n/a	70% implementation (ITMC reporting) 20%

ACTIVITY 9 OUTPUTS

						
Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2025
<p>9.1 Coordinate the implementation of the Agency's performance management framework, including Agency wide budget management and IT management processes, environmental management and regulatory compliance</p>	Unified day-to-day practices across the agency upon implementing SPD	MT, ITMC & BMC External and internal audits Statutory bodies	Number of high risks identified in annual risk assessment	Annual	3	<= 3
	Annual assessments of risk and internal controls performed and reported		Effective monitoring of high risks and critical recommendations to follow up on timely implementation of mitigation measures by business owners		n/a	Quarterly status reporting to the MT Internal controls assessment including reporting on implementation for year N-1 Risk assessment
	Legal and regulatory compliance monitored; issues and areas for improvement identified		Percentage of identified deficiencies in internal controls addressed within timelines		n/a	100% for critical, 80% for major, 60% for moderate
	Outcomes are included in the annual assessments of risk and internal controls		Timely follow-up and resolution of internal and external audits (in particular from IAS and ECA) recommendations and findings			Monitoring audit action plans Results of corrective actions taken during year N-1 are reported in the current year AAR
	Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy under ITMC		Number of identified regulatory breaches		3	<=3
	Streamlined budget management across the Agency, under BMC		Percentage of revised and up to date corporate rules (MBD, EDD, policies, processes)		n/a	Review 50% of corporate rules which have not been reviewed in the last 4 years; 60% of corporate rules which have not been reviewed in the last 5 years. Provide or confirm motivation for non-revision, as baseline requirement
	A plan to reduce CO2 emissions at ENISA's HQ		Annual report on ARES maintenance and actions		n/a	80% resolution of identified open issues, incorporating lessons learned
			Reduction of CO2 emissions in ENISA HQ		n/a	By >5%; provide motivation if expected rate is unattainable, as baseline provision
			Efficiency and effectiveness of ITMC & BMC (survey)		n/a	> 60%

9.2 Maintain and enhance ENISA's cybersecurity posture	Compliance with new regulations on a high common level of cybersecurity within Union entities Timely identification and response to cybersecurity risks Continuous monitoring of cybersecurity of IT systems and timely identification of issues and areas for 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	n/a	90%
			Annual risk assessment (RA) and risk treatment plan with the relevant business owners	annual	n/a	Implement annual risk assessment follow up actions.
			Implement action plan for implementation of cybersecurity risk management measures in line with Regulation (EU) 2023/2841	annual	n/a	Report on the level of accomplishment of action plan
			Address all potential cybersecurity incidents	annual	n/a	Respond to >90% of tickets submitted to ServiceNow
			Cybersecurity training for staff and managers	annual	n/a	At least two training sessions a year
9.3 Provide support services to the EU Agencies network and in key areas of the Agency's expertise and chair EUAN in 2025	Cybersecurity advisory on implementation of the new regulation on a high common level of cybersecurity within Union entities 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	n/a	>80%
9.4 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 or accessible within ENISA	Annual	29%	55%
			Response timeliness to external parties (internal reporting)	Annual	n/a	48h

Stakeholders and engagement levels



Partners: EU Agencies Network, relevant Union entities and European Commission, Staff Committee, Management Team.

ACTIVITY 9 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 743 000	FTE: 14 ³⁸
Other supplementary contributions	Budget: EUR 54 604 SLA with ECCC, see annex XI for additional information	FTE: 0

38 - Including ED, COO, advisor and accounting officer.

ACTIVITY 10: Reputation and Trust



Overview of activity



This activity seeks to meet the requirements set out in 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 that a transparent and proactive approach is taken to maximise the quality and value provided to stakeholders. It also includes contributing to efficiency gains by optimising the way it engages with stakeholders and offering on demand services in addition to 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.







In this activity, ENISA will deliver essential and demand driven communications services as described in ENISA's Corporate Strategy.

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

ACTIVITY 10 ANNUAL OBJECTIVES

Description	Link to corporate objectives	Activity indicators	Frequency (Data source)	Latest result	Target
10.A Protect and grow the Agency's brand	Ensure efficient corporate services	Level of trust in ENISA (as per Biannual Stakeholder Survey)	Biennial	95%	95%
		ENISA brand management	Annual	n/a	Target set in crisis communications playbook by 2025
10.B Improve outreach of ENISA's mandate	Ensure efficient corporate services	Corporate satisfaction with essential communication and administrative assistants services	Annual (MT survey)	n/a	60%
		Corporate satisfaction with demand driven communication and assistants services	Annual (MT survey)	n/a	60%
		Stakeholder satisfaction with ENISA events	Annual	n/a	>60%
		Number of unique visitors	Annual		>10% increase year on year

ACTIVITY 10 OUTPUTS

						
Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2025
10.1 Review and implement the multiannual communications strategy and support stakeholders' strategy including corporate outreach	Enhanced transparency and outreach	Management Team and agency stakeholders	Number and types of activities at each engagement level (stakeholder strategy implementation)	Annual (Internal report)	n/a	Stakeholder strategy under review
	Engaged communities		Number of social media engagements	Annual (Media monitoring)	75k	>80k
	Increased impact of ENISA activities		Stakeholder satisfaction with ENISA outreach	Biennial (survey)	n/a	>80%
	Relevant and easily accessible information is provided to stakeholders		Number of total ENISA website visits	Annual (website analytics)	2.03 million	>2.5 million
	Successful EUAN leadership, communications and EUAN yearly meetings		Website availability	Annual (website analytics)	97%	>97%
10.2 Implement internal communications strategy	Engaged staff	Management Team and staff committee	Staff satisfaction with ENISA internal communications	Annual (survey)	39%	>60%
10.3 Manage and provide the secretariat for statutory bodies, i.e. EB, MB, AG, NLO (excluding certification)	Support for the operation and organisation of ENISA statutory bodies	Statutory bodies, Management Team and Committees	Number of feedback instances received per NLO consultation	Annual (Internal report)	n/a	>6
	Support the effectiveness of implementation of work programmes (validation of operational outputs)		Number of feedback instances received per AG consultation	Annual (Internal report)	n/a	>8
	Provision of administrative support for the day to day workings of the Management board's decisions and recommendations from NLO & AG		Satisfaction of statutory bodies with ENISA's support to fulfil their tasks as described in CSA	Annual (Survey)	n/a	>80%
			Satisfaction of statutory bodies with ENISA portals	Annual (Survey)	n/a	>80%

Stakeholders and engagement levels



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

Involve / Engage: All ENISA stakeholders

ACTIVITY 10 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 760 000	FTE: 8.5

ACTIVITY 11:

Effective and efficient corporate services



Overview of activity



This activity seeks to meet Article 3(4) of the Cybersecurity Act which calls upon the Agency to ‘develop its own resources, including /.../ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation’.

ENISA aims to develop its human resources to align them with the Agency’s goals and needs, by attracting, retaining and nurturing talent while enhancing its reputation as an agile, knowledge-driven organisation where staff can grow, stay motivated and remain engaged. A key priority is the development of competency, positioning ENISA as an ‘employer of choice’ and a rewarding place to work for all.








The Agency strives to maximise resource efficiency by building a flexible, skilled and fit-for-purpose workforce through strategic workforce planning. ENISA is committed to maintaining the effective functioning of the Agency and delivering high-quality services across both administrative and operational areas. Additionally, the Agency recognizes that flexible working arrangements support a healthy balance between work and personal life for its staff.

At the same time, ENISA will continue to strengthen its secure operational environment to the highest standards. It will also explore cloud-based services that meet European and international standards in line with the ENISA’s IT strategy.

ACTIVITY 11 ANNUAL OBJECTIVES

Description	Link to corporate objectives	Activity indicators	Frequency (Data source)	Latest result	Target
11.A Enhance people centric services by implementing the Corporate and HR strategy	Effective workforce planning and management	Implementation of Strategic Workforce Planning and Review decisions	Annual	Fully implemented	Fully implemented
	Efficient talent acquisition, development and retention	Implementation of the Corporate and HR strategy		n/a	Actions implemented according to the timelines
	Caring and inclusive modern organisation	High participation in staff satisfaction survey		64%	75% participation rate
11.B Ensure sustainable and efficient corporate solutions and promote continuous improvement	Ensure efficient corporate services	Implement best practices in sustainable IT solutions	Annual	n/a	IT strategy updated accordingly
	Introduce digital solutions that maximise synergies and collaboration in the Agency	Limited disruption of continuity of corporate services	Annual	n/a	BCP for corporate IT facilities, financial and HR services in 2025
	Developing service propositions with additional external resourcing	Handling EU/CI at the level of SECRET UE/EU SECRET	Annual	n/a	Operational for the first full year in 2025
	Promote and enhance ecologic sustainability across all Agency's operations				
	Develop efficient framework for ENISA's continuous governance to safeguard high level of IT and to ensure physical security services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently				

ACTIVITY 11 OUTPUTS

						
Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2025 ³⁹
11.1 Manage and provide horizontal, recurrent administrative services in the area of resources for ENISA staff and partners	Services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently. Implementation of the ED decision on annual workforce review [adopted in April 2024]	Management Team IT Management Committee Budget Management Committee Staff Committee	Turnover rates	Annual	4.9%	<5 %
			Establishment plan posts filled		98%	>95%
			Lag between vacancy announcement to candidate selection		n/a	<300 days median across all posts
			Percentage implementation of approved Recruitment plan		n/a	>90%
			Percentage implementation of approved Procurement Plan		n/a	>90%
			Percentage procurement procedures launched via e-tool (PPMT)		100%	>90%
			Percentage 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		2	<4
Late payments resulting in interest payments		9%	<10%			

39 - Targets will be updated during the course of 2024 after the review of the annual activity report on work programme 2023.

11.2 Implement Agency's Corporate strategy including HR strategy with emphasis on talent development, growth and welfare	Objectives and goals set out in the corporate and HR strategy are met.	Management Board Management Team Staff Committee EUAN BMC	Number of policies/IR reviewed	Annual	n/a	>1
			Number of processes revised		n/a	>1
			Percentage of staff satisfaction with talent development		58%	>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
11.3 Manage and provide horizontal, recurrent support services in the area of facilities, security and corporate IT for ENISA staff and partners	Services such as corporate IT, facilities and security are performed efficiently with minimal disruption. Upgrade of meeting rooms	Management Team IT Management Committee Budget Management Committee Staff Committee	Staff satisfaction with working environment	Annual	74%	>70 %
			Time to respond to safety and security incidents.		n/a	<1 to acknowledge and <3 to respond
			Average time to respond to facilities management requests		n/a	<1 to acknowledge and <3 to respond
11.4 Enhance operational excellence and digitalisation through modern, safe, secure and streamlined ways of working, and introducing self-service functionalities	Services such as access management, meeting room facilities, equipment renewals, cloud-based solutions and data availability are efficient.	Management Team IT Management Committee	Critical systems uptime and downtime	Annual	100%	99%
			Staff satisfaction with IT resolution		84%	85%

Stakeholders and engagement levels



Partners: ENISA staff members and EU Institutions, Bodies and Agencies.

Involve / Engage: Private sector and international organisations.

ACTIVITY 11 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	Budget: EUR 4 631 348	FTE: 21.25



NOTES





ABOUT ENISA

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

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

