EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA Single Programming Document 2026 - 2028

Condensed work programme 2026

JANUARY 2026

CONTACT

For contacting ENISA please use the following details:
info@enisa.europa.eu
website: www.enisa.europa.eu

LEGAL NOTICE

COPYRIGHT NOTICE

Luxembourg: Publications Office of the European Union, 2026

Language version	Output format	Catalogue number	ISBN	ISSN	DOI
English	PDF Web	TP-01-26-003-EN-N	978-92-9204-784-9	2467-4176	10.2824/4993923

ENISA Single Programming Document 2026 - 2028

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

Foreword

As we embark on the next phase of our journey to enhance the maturity and resilience of cybersecurity in the European Union, I am pleased to introduce the Single Programming Document (SPD) for 2026-2028.

This SPD outlines the steps that the European Union Agency for Cybersecurity (ENISA) will take to support the implementation of key EU cybersecurity policies, including the Cybersecurity Act, the NIS2 Directive, the Cyber Resilience Act, EU Blueprint for Cyber Crisis Management, the Cyber Solidarity Act, the EU Action Plan for the Cybersecurity of Hospitals and Health Providers and the Digital Omnibus. These will shape and inform the actions that will be undertaken in 2026 and thereafter.

Firstly, this SPD outlines our commitment to continue working to support EU Member States in their pursuit of enhanced cybersecurity. ENISA will focus its effort on supporting EU Member States in their implementation of key legislation such as the NIS2 Directive, the Cyber Resilience Act and EU policies by serving as a centre of expertise in both collecting and providing independent, high quality technical advice and assistance.

Secondly, ENISA will build on our existing capabilities and capacities, leveraging our expertise and partnerships to drive progress in areas where the Agency itself needs to implement key priorities — in cybersecurity certification, vulnerability reporting and management, and crisis management to name but a few. The launch of the Single Reporting Platform in September 2026 will be a significant deliverable from the Agency, a global first for vulnerability management. Moreover, the administration and operation of the EU Cybersecurity Reserve puts ENISA in the limelight as a dependable partner for the cybersecurity community in the EU.

Finally, the Agency welcomes the recently proposed Digital Omnibus and the revision of the Cybersecurity Act. In 2026, the Agency will work with our partners to ensure the final provisions will contribute to a trusted and secure single market. I am proud of the progress we have made so far and I am confident that the work outlined in this SPD will help us achieve our goals.

I would like to thank our partners, stakeholders and team members for their hard work and dedication to our mission. Together, we can break new ground towards an even more cyber-secure single digital market that meets the challenges of today and tomorrow.

Juhan Lepassaar
Executive Director

Section I

WORK PROGRAMME 2026

This is the main body of the Work Programme; It describes what the Agency's operational and corporate activities aim to deliver in 2026 towards achieving its strategic objectives based on ENISA's strategy and to fulfil its mandate. A total of eight operational activities and three corporate activities have been identified to support the implementation of ENISA's mandate in 2026.

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

1. 2026 WORK PROGRAMME PRIORITIES

The agency's work programme for 2026 focuses on key priorities that align with ENISA's strategy. These priorities include implementation of the cyber reserve and the CRA single reporting platform, as well as the publication of the second report on the state of cybersecurity in the EU and assisting MSs in enhancing cybersecurity maturity. By prioritising the areas described below, ENISA will ensure effective implementation of its strategic objectives while addressing critical challenges and opportunities.

1.1. Policy Monitoring & Resilience of Critical Sectors

State of Cybersecurity in the EU Report (NIS2 Article 18). ENISA will publish the second edition in cooperation with the NIS Cooperation Group and the European Commission and will ensure follow-up on the recommendations.

Critical Sector Resilience. ENISA will assist Member States in enhancing cybersecurity maturity through a study of NIS Investments, the NIS360 service catalogue and the EU action plan for hospitals and healthcare providers under NIS2.

Union Risk Assessments. ENISA conduct coordinated stress tests on resilience and assess supply chain risks to evaluate and strengthen critical infrastructure.

Sectorial & Horizontal Working Groups. ENISA will support NIS2 workstreams to refine policies and address emerging threats.

Strategic Alignment: Support for effective and consistent implementation of EU cybersecurity policies.

1.2. Capacity Building

Cyber Europe 2026. ENISA will host the 8th edition of Europe's largest cybersecurity exercise, testing the revised Cyber Crisis Management Blueprint in response to evolving geopolitical threats.

European Cybersecurity Skills Framework (ECSF). ENISA will assist Member States in adopting ECSF to standardise cybersecurity training and workforce development.

Strategic Alignment: Strong cybersecurity capacity within the EU.

1.3. Operational Cooperation, Support Services & Situational Awareness

Strengthen cooperation. ENISA will strengthen CSIRTs Network and EU-CyCLONe cooperation by providing threat assessments, vulnerability analysis and cross-border incident response.

Threat Intelligence & Preparedness. ENISA will ensure that stakeholders are informed about cyber threats, vulnerabilities and crises to improve EU-wide resilience.

EU Cybersecurity Reserve (Cyber Solidarity Act). ENISA will operationalise the reserve to enhance large-scale incident response capabilities (financed via contribution agreement).

EU Cybersecurity Networks & Platforms. ENISA will develop and upgrade IT systems for operational support, including the EU Vulnerability Database and CRA Single Reporting Platform (financed via contribution agreement).

Strategic Alignment: Effective Union preparedness and response to cyber incidents, threats and crises.

1.4. Certification & Market Support

EU Certification Schemes. ENISA will develop candidate schemes for EU Managed Security Services (EUMSS) and EU Digital Wallet (EUDIW) in line with EU Cybersecurity Certification Framework.

Support implementation. ENISA will support CRA implementation with technical guidance, market surveillance and analysis, and the assessment of harmonised standards to help relevant stakeholders, SMEs in particular.

Strategic Alignment: Building trust in secure digital solutions.

In addition, each of the priorities align with the horizontal objectives of empowering communities in an involved and engaged cyber ecosystem, by providing foresight on emerging and future cybersecurity opportunities and challenges as well as supporting consolidated and shared cybersecurity information and knowledge for Europe.

1.5. Strengthening ENISA's IT infrastructure

ENISA will prioritise IT infrastructure to support its evolving mandate, with two critical initiatives:

Data Centre Migration. ENISA will complete the transition of its data centre from Heraklion by the end of 2026.

Cybersecurity maturity plan. ENISA will implement a comprehensive framework for cybersecurity maturity aligned with Regulation (EU) 2023/2841 that will support expanded legislative tasks under the CRA, the EU Vulnerability Database and other regulations.

The following graphs provide insights into the allocation of resources for each of the operational activities in the 2026 work programme.

Table 1 presents the budget allocated to each of ENISA's operational activities financed from the Title 3 EU subsidy budget. Please note that activity 4 manages the IT platforms and systems on behalf of the all-operational activity business owners. Actions under Activity 6 are financed via contribution agreements; see table 3 for further information on contribution agreements and annex 11.

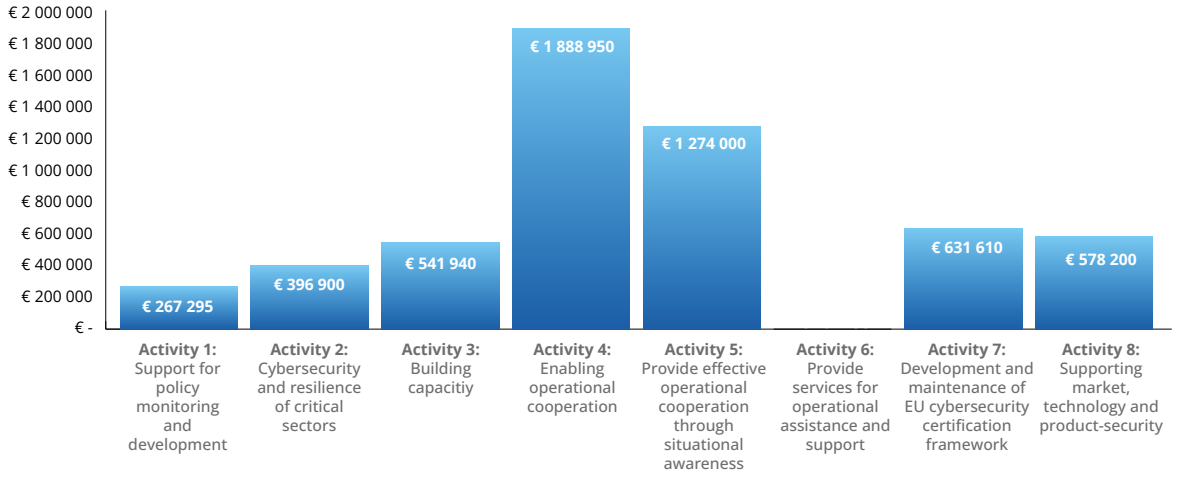


Table 2 presents the allocated number of target FTEs for each of ENISA's operational activities financed from Title 1 EU subsidy budget.

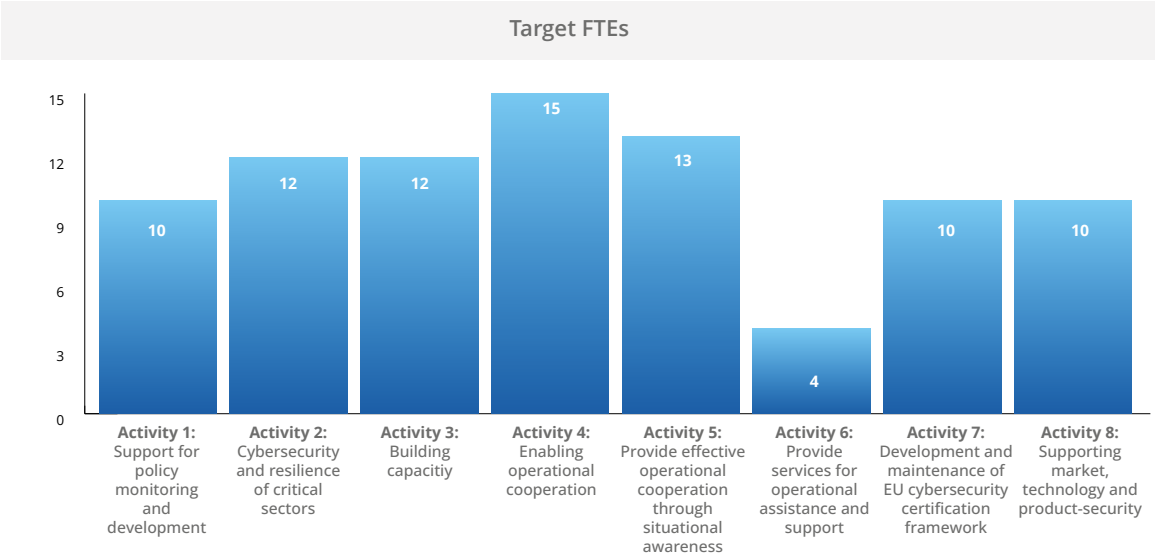


Table 3 presents the 2026 forecast appropriations for commitment in the contribution agreements in the Title 4 budget.

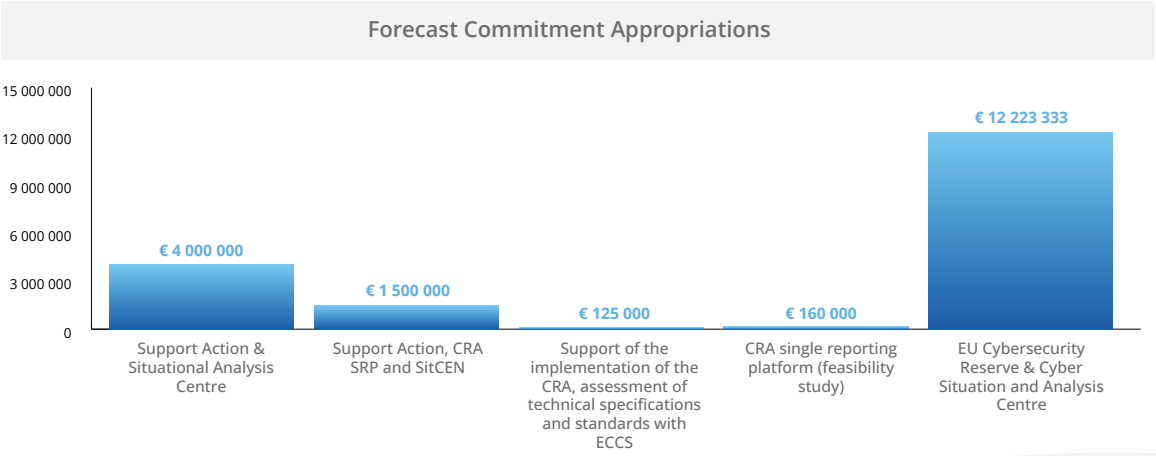
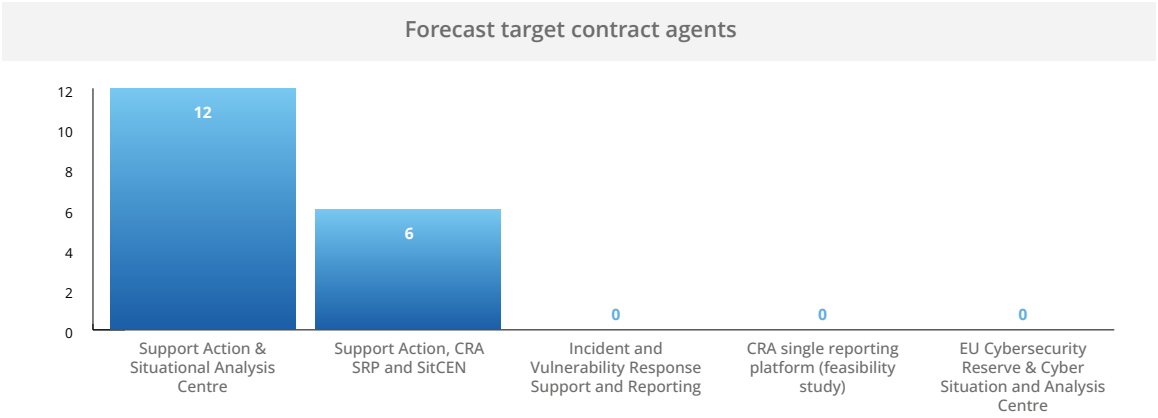


Table 4 presents the forecast number of FTE contract agents financed via the contribution agreements in the Title 4 budget.

Please note that a number of FTEs from the Support Action contribution agreement signed in 2023 will be transposed during the course of 2026 to the Cyber Reserve.



Service packages

In 2022 the Agency introduced the concept of service packages to allow management to focus efforts and resources in a highly structured and more efficient manner for achieving specific objectives. The ENISA service packages 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:

- NIS2 led by activity 2 cybersecurity and resilience of critical sectors;
- Training and exercises (TREX) led by activity 3 capacity building;
- Situational Awareness (SITAW) led by activity 5 provide effective operational cooperation through awareness of the cyber situation;
- Certification (CERTI) led by activity 7, the development and maintenance of EU cybersecurity certification;
- Cybersecurity index (INDEX) led by activity 1, support for policy monitoring and development.

Stakeholders and engagement level

Stakeholder strategy is expected to the reviewed towards the end of 2025. As a result this section will be reviewed and updated according to the outcome of the strategy during the drafting of the 2027-2029 work programme.

KPIs / metrics

The work programme for 2026 includes indicators for measuring the new strategic objectives in the updated ENISA strategy, and indicators and targets for measuring the objectives of activities as well as indicators at the output level to measure the performance of the outputs. The implementation of Strategic KPIs is expected to be reviewed and the requirements for achieving them to be drawn up during the course of 2026; these will be reflected in the draft work programme 2027-2029.

2. OPERATIONAL ACTIVITIES

ACTIVITY 1: Support for policy monitoring and development

Overview of activity

This activity delivers on ENISA's strategic objectives 'support for effective and consistent implementation of EU cybersecurity policies' and 'consolidated and shared cybersecurity information and knowledge support for Europe'. In particular, work under this Activity shall provide strategic long-term analysis, guidance and advice on current policy challenges and opportunities with the aim of supporting informed decision-making. In terms of knowledge management, ENISA will work towards consolidating information on cybersecurity posture across MSs, including via input from national cybersecurity strategies in conjunction with the EU cybersecurity index, peer-reviews, as well as from other ENISA activities. Efforts in developing and maintaining the EU cybersecurity index and developing and following up on the biennial 'Report on the State of Cybersecurity in the Union' mandated by Art.18 of NIS2 will continue. The highlight for 2026 is the biannual report on the State of Cybersecurity in the Union (Art.18 NIS2 directive).

As such, under this activity, ENISA will support Union institutions and MSs on new policy initiatives[6] through evidence-based inputs into the policy development process. ENISA will also conduct policy monitoring in coordination with and in support of other EU institutions, bodies and MSs. Such monitoring will facilitate the identification of potential areas for policy development and measures for policy implementation. This will also be supported by the development of in-house capabilities to provide timely, regular, and consistent advice on the effectiveness of existing Union policy and law, in accordance with the EU's institutional competencies using the 'Implementation Check' model and together with Activities 2 and 8 in particular.

This cross-cutting activity leads ENISA's efforts towards delivering the cybersecurity index (INDEX) and policy analyses to better map MSs needs and 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. Value is also added by informing them about developments at the technological, societal and economic market levels which might affect the cybersecurity policy framework and also by using, among other sources, information from the Threat Landscape report, situational awareness, foresight, incident reporting and vulnerabilities disclosure in collaboration with Activities 4, 5 and 8.

Activity 1 leads the Index service package and supports the NIS, TREX and CERTI service packages. The Activity supports the European Commission (COM) and European External Action Service (EEAS) initiatives for Eastern partnerships or similar.

The full list of statutory tasks that the activity undertakes based on EU legislation is presented in annex 15.

Link to strategic objective (ENISA strategy)

- Empowered communities in an involved and engaged cyber ecosystem.
- Consolidated and shared cybersecurity information and knowledge support for Europe.
- Effective and consistent implementation of EU policies for cyber resilience.

Indicator for strategic objectives

Uptake of recommendations stemming from NIS2 Art.18 report.

Number of identified future and emerging areas adopted for policy interventions.

6 Horizontal initiatives on NIS2 sectors and CRAs.1

ACTIVITY 1 OBJECTIVES

Description	CSA article and other EU policy priorities	Timeframe Of Objective	Indicator	Target
1.A By the end of 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 and continuous thereafter	Assessment of ENISA advice on EU policy (stakeholder survey, desktop research)	75% stakeholder satisfaction from ENISA's advice (among EU policy makers)
1.B By Q3 2026 and in collaboration with Activity 2, aim to ensure that two-thirds of policy observations within the first State of Cybersecurity in the Union report have been followed up by MSs and COM.	Art.18 NIS2	2026 and continuous thereafter	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 work on their NIS Strategies

ACTIVITY 1 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
1.1 Assist MSs to implement, assess, review National Cybersecurity Strategies and policies. Enhance a culture of trust and cooperation among MSs, also through peer reviews.	Stakeholders receive technical advice with the evidence needed for policy-making activities and the definition of implementation measures	NIS CG, including relevant work streams; National Liaison Officers (NLOs), including relevant subgroups, Advisory Group	Rate of use by MSs of the National Capabilities assessment framework or the peer review framework, including the code of conduct.	Biennial (Survey), Annual dialogues, and annual desktop research	NA	Two thirds of MSs are using Art.18 report as input for their cybersecurity strategies and policy-making. All MSs use ENISA support and tools for the work on their NIS Strategies and policy-making
1.2. Collect relevant evidence by maintaining and enhancing the EU cybersecurity index and use such evidence to inform ENISA's support on strategies, as per output 1.1. Present collected knowledge in the Report on the State of Cybersecurity in the Union, further contextualising it with other ENISA sources, e.g. the CRA Market Analysis (Activity 8).			Rate of contribution to State of the Cybersecurity in the Union Report by CSIRT N and NIS CG.		Contribution by all MSs	100%
1.3. Maintain analyses of time-sensitive policy observations offering technical advice for policy development and implementation by mapping gaps, challenges and needs in implementing NIS2 and other EU legislative acts.			Assessment of timeliness, regularity and consistency of advice provided during policy development.		NA	75% stakeholder satisfaction from ENISA's advice (among EU policy-makers)

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
Activity resources from EU subsidy	**Budget: EUR €267 295**	**FTE: 10**[7]

7 Target FTEs.

ACTIVITY 2:
Cybersecurity and resilience of critical sectors[8]

Overview of activity

This activity supports Member States with increasing cybersecurity maturity in critical sectors, not only through policy implementation but also by measuring the needs of each sector and offering tailor made recommendations. The objectives of this activity are to ensure efficient measurement of the maturity of the sectors (through the NIS Investments study and NIS360), to promote actions that increase cybersecurity posture and increase collaboration, and to support alignment and integration of sector specific resilience policies (such as DORA for resilience in the finance sector, the Network code for cybersecurity of cross-border electricity flows, part-information security of Aviation, etc). This activity includes an annual check on policy implementation (through the NIS Investments study and the NIS360), which relies on direct information from companies in the NIS sectors.

Under this activity ENISA provides support to sector-related and sector-focused working groups such as the NIS Cooperation Group (NIS CG) workstreams implementing the NIS CG work programme. ENISA's goal here is to monitor the implementation of the adopted horizontal frameworks for risk management, security measures and incident reporting across all policy files, which can also be used beyond NIS2 (for example, under DORA and the Aviation Part-IS when relevant), creating a common approach. Similarly, other related sector-specific files (such as the Healthcare Cybersecurity Action Plan or the Electricity Code) will be coordinated under this activity to support MSs, depending on the resources allocated.

Secondly, under this activity, ENISA supports MSs and the Commission in addressing specific threats and risk scenarios for the Union related to critical sectors (supply chains), by considering technology or market developments such as Open Radio Access Networks (O-RAN) and other Union coordinated risk evaluations (such as Nevers call in 2024, Cyber risk posture for telecoms and energy in 2024), the Council Cyber Posture[9] , the Union coordinated supply-chain risk assessments (under NIS2), and Union coordinated preparedness tests (aka resilience stress tests, under the Cyber Solidarity Act). Based on the stress tests methodology developed by ENISA, this activity supports the implementation of the cables security[10] toolbox.

In 2026 ENISA will also support the MSs and the Commission by carrying out Union coordinated tests of resilience preparedness and Union coordinated assessments of supply-chain risks. Resilience stress tests are part of the services catalogue ENISA has developed for critical sectors to increase their maturity. This activity is tightly linked with Activity 8 on market, technologies and product security.

Thirdly this activity also addresses sector-specific issues, working with sectorial stakeholders in the NIS sectors, providing a service catalogue based on their criticality and maturity posture (NIS360). For each sector, ENISA will support (if created) an NIS Cooperation Group workstream for relevant national authorities, and also engage with the industry either by supporting EU ISACs, or by co-organising industry events together with Member States or relevant authorities to facilitate public-private dialogue on cybersecurity. This activity provides important sectorial input to other SPD activities, such as the cybersecurity posture of the Union (Activity 1), cyber exercises and training (Activity 3) and situational awareness reports for particular sectors (Activity 5).

Finally, there is a dedicated output for checking the implementation of these policies and the efficiency of the services catalogue in the longer term. This is done by collecting data from the public sector and industry directly to ensure that NIS2, sectorial rules and other lex specialis do not only remain on paper but actually improve the level of security in NIS sectors. This can be seen in the annual NIS investments report and 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).

The full list of statutory tasks that the activity undertakes based on EU legislation is presented in annex 15.

8 The term critical sectors is used in this context to cover ALL sectors within the scope of the NIS2 Directive.
9 https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.
10 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009.

Link to strategic objective (ENISA strategy)

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

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
2.1. 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 good practices and international standards.	CSA Art.5 and Art.6 NIS2 Directive	Frameworks pilot by 2026	Implementation of pilot programme (number of sectors piloting the frameworks, feedback scores on usability)	20MSs to adopt, use or endorse the frameworks
		Full implementation by 2027		>75% usability score
2.2. Provide continuous comprehensive support to MSs for implementing Union's regulatory cybersecurity requirements and raising resilience across critical sectors.	CSA Art.5 and Art.6 NIS2 Directive	Full implementation by 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
2.3. Help increase the overall maturity level of critical sectors under the NIS2 Directive.	CSA Art.5 [possibly NCCS] NIS2 Directive	End of 2027	Maturity assessment based on the updated NIS360 methodology	>2 sectors improving maturity

ACTIVITY 2 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
2.1. Support Member States with implementation of policy files (such as NIS2, DORA, etc)	NIS2 frameworks for risk management, security measures and incident reporting	DG CNECT NIS CG	Framework usage	Annual (Internal count)	N/A	to be mapped against national frameworks from 3 MS
			EU register for digital entities is used by all MSs	Annual (Report)	(2025) 5 MSs use EUDIR	at least 10 MS to use EU Digital Infrastructure Registry (EUDIR)
			Coherence in the level of implementation between NIS2 and other frameworks, e.g. DORA, NCCS	Satisfaction survey	N/A	60%
2.2. Support Member States with union coordinated risk evaluations, and union coordinated preparedness tests	Support Union-wide risk evaluations and risk scenarios (health, transport, vehicles) and their follow-up (5G, Nevers) Coordinated risk assessment of critical supply chains	DG CNECT NIS CG	Stakeholder satisfaction	Biennial (Survey)	94%	70%
			Number of sectorial situational awareness reports	Annual (Internal count)	6	6
2.3. Improve cybersecurity and resilience in the NIS sectors	Stakeholders use the NIS service packages to improve the security and resilience of the sectors	DG CNECT, NIS CG, Sectorial EU ISACS, Sectorial EU agencies	Number of critical sectors increasing maturity based on NIS360	Annual (Internal count)	3	3
			Number and frequency of services or workflows delivered to NIS sectors	Annual (Internal count)	21	10
			Stakeholder satisfaction	Biennial (Survey)	94%	70%
2.4. Perform an annual check on policy implementation and improve maturity of sectors	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, AG as necessary	Number of critical sectors assessed by NIS360 and cyber posture briefs	Annual (Internal count)	10	at least 6

Stakeholders and engagement levels

Partners: CNECT, NIS CG, National competent authorities, Sectorial DGs, Sectorial Union Entities, Sectorial competent authority groups, sectorial ISACs.
Involve / Engage: NLOs, essential and important entities in the scope of NIS2 and industry associations/ representatives, ENISA Cybersecurity Directors Group.

ACTIVITY 2 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: €396 900**	**FTE[11]: 12**

11 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 NIS2 Sectors. It focuses on improving stakeholders' resilience and response capabilities and increasing their preparedness.

It also aims at enhancing their skills and causing behavioural changes with regards to cyber hygiene. Furthermore it seeks to reduce the cyber skills gap, maintaining the European Cybersecurity Skills Framework (ECSF) by engaging with the relevant communities and stakeholders. ENISA will support Member States in adopting the ECSF by providing practical guidance, promoting a coherent approach to the development of cybersecurity skills across the Union including the development of attestation schemes for the cybersecurity skills of European individuals. The 'train the trainers' concept will empower stakeholders to autonomously deploy ENISA's services, share good practices and lessons learnt as well as materials to increase their preparedness and ability to respond to emerging cybersecurity threats and risks (CSA art.6).

In line with CRA art.10, activity 3 will also support market surveillance authorities, conformity assessment bodies and SMEs liable under the CRA regulation to develop appropriate cybersecurity skills following ENISA's ECSF and facilitate collaboration among relevant public and private stakeholders to ensure the re-skilling or up-skilling of targeted professionals.

The Agency, in collaboration with relevant Union Entities, Members States' operational communities and NIS2 sectors, will conduct a limited number of targeted exercises (CSA Art.6(1)h) and accompanying training sessions (CSA Art.6(1)(i) focusing on empowering the trainers and enhancing the resilience, maturity and preparedness of the NIS sectors (in cooperation with activities 2, 4 and 6). In cooperation with CERT-EU, it will devise and deliver a targeted capacity building programme to assist Union Entities in implementing Regulation (EU) 2023/2841. In addition, ENISA will support the Cybersecurity Blueprint in the context of Cyber Europe. Given the advanced planning stage of Cyber Europe, ENISA will integrate the strategic and political layers and their scope in accordance with the resources available.

The activity will contribute to the INDEX service package by developing indicators and collecting data to measure progress in closing the cyber talent gap in line with the EC Communication on the Cybersecurity Skills Academy. It will provide analytical insights on EU cybersecurity capacity and the awareness and cyber hygiene of citizens and SMEs in the EU in the context of the State of Cybersecurity in the Union (NIS2 Art.18).

This activity seeks to develop strong ties with stakeholders and build on the work established by the ENISA cybersecurity Support Action, as well as the forthcoming ECCC's funded projects on capacity building.

Finally, this activity will assist non-EU stakeholders (e.g. from the Western Balkans or Ukraine to improve their capacity building mechanisms and will participate in EU US strategic dialogue by exchanging good practices on capacity building.

The full list of statutory tasks that the activity undertakes from EU legislation is presented in annex 15.

Link to strategic objectives (ENISA STRATEGY)

- Empowered communities in an involved and engaged cyber ecosystem
- Strong cybersecurity capacity within 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
3.1. Maintain and regularly update the European Cybersecurity Skills Framework (ECSF).	EU Communication on Cyber Security Skills Academy Arts.10 and 6	2027	Number of MSs endorsing the ECSF framework	18
			Stakeholder satisfaction rate	95%
3.2. Community empowerment through maintaining and evolving relevant toolkits, methodologies and standards.	CSA Arts.4, 6, 7(5) and 10 REU Art.10	2027	Number of MSs and Union institutions, bodies, offices and agencies using ENISA's toolkits, methodologies and frameworks	20

ACTIVITY 3 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
3.1. Support the adoption and uptake of EU's Cybersecurity Skills Framework	Measure and report on the skills gap including developing indicators to be used for Cybersecurity IndexArt.18a Map the skills arising from new policy instruments Promote the adoption of ECSF in MSs, in training organisations and academia and ensure its regular update in line with the Cyber Skills Academy Communication, to include skills attestation schemes.	Ad hoc Working Group (AHWG) on Cybersecurity Skills, ECCC WG 5 on Skills	Stakeholder satisfaction	Biennial (Survey)	91%	93%
			Number of MSs endorsing ECSF	Annual	N/A	17
			Number of training organisations endorsing ECSF in their training programmes	Biennial	N/A	3
			Number of Training Organisations endorsing ECSF in their training programmes	Annual	N/A	8
3.2. Organise targeted exercises and support stakeholders to plan and execute their own exercises	Organise a set of limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders (e.g. Cyclone, CSIRTs Network, Union Entities). Orchestrate the execution of exercises for specific target audiences including those defined in Cooperation Agreements with other EU entities providing tools such as methodologies, templates and providing them access to a community of peers. Follow up on the findings of previous exercises and ensure timely and appropriate implementation of lessons learned. Assist Union Entities in implementing Regulation (EU) 2023/2841 (mostly arts.4 and 11) by providing tools such as methodologies, templates as well as access to a community of peers.	NLO Network (as necessary) CSIRTs Network (as applicable) EU-CyCLONe members (as applicable) NIS Cooperation Group (as applicable) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as applicable) CERT-EU	Number of people impacted directly and/or indirectly by exercises organised by ENISA	Annual (Report)	N/A	10 000
			Satisfaction of entities or communities participating in the capacity building activities organised by ENISA	Annual	N/A	93%

3.3. empowering communities to execute their own capacity building programmes using ENISA's relevant tools and methodologies	Develop and support communities that will facilitate and multiply the sharing of frameworks, good practices and lessons learnt, covering all Activity 3 initiatives and services. Develop strong ties to stakeholders and the work of Support Action as well as the forthcoming ECCC's funded projects on capacity building, and develop synergies with ENISA's services and results	NLO Network (as necessary) CSIRTs Network (as applicable) EU-CyCLONe members (as applicable) NIS Cooperation Group (as necessary) EU ISACs (as applicable) NLO subgroup of Cyber Europe planners (as necessary) Key private stakeholders (as applicable and in line with ENISA's international and stakeholder engagement strategies)	Number of participants in ENISA's communities, multiplying the sharing of frameworks, good practices and lessons learnt.	Biannual (Report)	N/A	100
			Engagement rate, the percentage of active members who are contributing to these communities.	Biannual (Report)	N/A	40
			Community retention rate as percentage of members who remain in the community over a long period	Biannual (Report)	N/A	>70%
3.4. Support stakeholders in organising and delivering successful and trustworthy Cyber Security Challenge competitions by helping to ensure trust, transparency and fairness in the competitions.	By being involved in key governance and oversight activities involving the Jury, Watchdogs and ECSC governance structures. This includes, as well as on-site operations during the ECSC Final, critical reinforcing of ethical standards, managing disputes, aligning operational protocols, and maintaining the credibility of the competition. Providing guidance and connecting the community, especially the ECSC Steering Committee, with EU entities and especially the ECCC, thus supporting them to undertake the organisation and execution of ECSC finals and form an elite team to represent Europe in the next ICCs.	ECCC staff European Cyber Security Challenges (ECSC) executive committee and Steering Committee NLO Subgroup	Stakeholders' satisfaction with ENISA's support to ensure trust, transparency and fairness in cybersecurity challenges (survey).	Annual (Report)	N/A	60%

Stakeholders and engagement levels

Involve / Engage: Training organisations, private entities in NIS2 sectors, CSIRTs Network and related operational communities, European ISACs, EU-CyCLONe members, Blueprint, 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, the Horizontal Working Party on Cyber Issues (HWPCI), the European Digital Infrastructure Consortium (EDIC), ECCC Working Group 5, European Digital Infrastructure Consortium.

ACTIVITY 3 RESOURCE FORECASTS

	Budget		FTEs
Activity resources from EU subsidy	**Budget: €541 940**		**FTE[12]: 12**

12 Target FTEs.

ACTIVITY 4:
Enabling operational cooperation

Overview of activity

This activity supports operational cooperation among Member States, EU entities and the internal coordination between ENISA operational activities.

The main goal of the activity is to provide operations support and assistance in order to ensure efficient functioning of the EU's operational networks and the cyber crisis management framework outlined in the 2025 EU blueprint. Under the mandate of NIS2, Activity 4 provides daily operations, expertise, organisational support, tools and infrastructure for both the technical layer and the operational layer, as well as the EU CSIRTs Network, the EU CyCLONe (Cyber Crises Liaison Organisation Network), the Union's operational cooperation networks, including activities stemming from the healthcare cybersecurity action plan.

Secondly, the activity aims to enhance interaction and trust between these two layers and the overall ecosystem as well as with the NIS Cooperation Group and the Council of the EU with the goal of bringing all networks and communities closer in order to form an informed, empowered and organised EU cyber crisis management ecosystem.

ENISA further supports operational communities by operating, developing and maintaining secure and highly available networks, interoperable IT platforms and communication channels. This includes providing operational and maintenance support for EU platforms such as the EU Vulnerability Database and, when established, the CRA Single Reporting Platform as well as other tools used by EU operational networks. Enhanced investment in IT infrastructure is crucial to strengthen business continuity, supply chain management, incident response and change management, while at the same time elevating the maturity of operational IT to ensure resilience and adaptability in an increasingly complex environment.

The 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, best practices, provide advice and issue guidance. 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 the work of Member States and the work of the Interinstitutional Cybersecurity Board (IICB) and CERT-EU. It equally drives internal cooperation with law enforcement and collaboration with Europol/EC3.

This activity equally manages the ENISA Cyber Partnership Programme and information exchange with security vendors and non-EU cybersecurity entities.

Finally, this activity will also seek to contribute to the Union's efforts to cooperate with third countries and international organisations on cybersecurity, including implementing the revised ENISA international strategy[13] and to contribute to the ENISA stakeholder strategy.

This activity supports SITAW, INDEX and NIS service packages.

The full list of statutory tasks that the activity undertakes arising from EU legislation is presented in annex 15.

13 Inline where applicable with the EU International Digital Strategy adopted in June 2025.

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 standard operating procedures coordinated by ENISA

EU Vulnerability Database is operationalised by ENISA and used by MSs

Reporting platform under CRA is operationalised and used by stakeholders

ACTIVITY 4 OBJECTIVES

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

ACTIVITY 4 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
4.1. Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs Network and EU-CyCLONe members HWPCI and the NIS Cooperation Group.	Enhanced Information Sharing and cooperation among the CSIRTs Network and EU-CyCLONe members and enhanced interaction with HWPCI and the NIS Cooperation Group.	CSIRTs Network and EU-CyCLONe members, HWPCI and NIS Cooperation Groups.	Stakeholder satisfaction	Biennial (survey)	89%	89%
			Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)	N/A	Core platforms remain operational during at least one large-scale cyber exercise annually
			Number of joint sessions established	Annual (report)	1 joint session per year	1 joint session per year.
4.2. Maintain, develop and promote ENISA Cyber Partnership programme aiming at information exchange to support the Agency's understanding of threats, incidents involving vulnerabilities and cyber security events	Operationalisation of the Cyber Partnership Programme	CSIRT Network, EU CyCLONe, Union Entities, HWPCI, MB	Stakeholder satisfaction	Biennial (survey)	84%	80%
			Number of new and total partners in the ENISA partnership programme	Annual (report)	4	4
			Percentage of RFI answered by members of partnership programme	Annual (report)	N/A	50%
4.3. Implement the revised ENISA international strategy and outreach programme	EU values recognised by international stakeholders International cooperation that supports ENISA objectives	MT, EEAS, COM and (MB as required)	Stakeholder satisfaction	Biennial (survey)	91%	>90%
			Internal satisfaction with international coordination	Annual (survey)	N/A	>70
4.4. Develop, maintain and upgrade IT systems and platforms for operational activities	Consolidation of operational IT with view to supporting ENISA operations	CSIRTs Network, CyCLONe members, NIS Cooperation Group and Business owners for ENISA Operational IT systems.	Stakeholder satisfaction	Biennial (survey)	89%	>90%
			IT architecture for external operational IT services	Biennial update	N/A	One IT architecture for Operational IT services
			ENISA operational IT	Annual (report)	N/A	Key deliverables included in ENISA annual report
4.5 Development of stakeholder and knowledge management systems and frameworks	Implementation of stakeholder strategy	MT and MB as required	Stakeholder satisfaction with knowledge management and stakeholder management system.	Biennial (survey)	N/A	Phase 1: assessment of operational needs achieved

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 (Security Operation Centres) including National and Cross-border SOCs.

Involve / Engage: NISD Cooperation Group, operators of essential services (OESs) and digital service providers (DSPs), Information Sharing and Analysis Centres (ISACs).

ACTIVITY 4 RESOURCE FORECAST

	Budget	FTEs
Activity resources from EU subsidy	**Budget: €1 888 950**	**FTE[14]: 15**

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 threat analysis, operational and strategic recommendations based on collections of incidents, and vulnerability and threat information to contribute to the Union's common situational awareness.

ENISA delivers on this activity by collecting and analysing security events, cyber incidents, vulnerabilities and threats based on its own monitoring, information shared by external stakeholders due to legal obligations[15] or voluntarily, by aggregating and analysing reports, ensuring information flow between the CSIRTs Network, EU-CyCLONe, and other technical, operational and political decision-makers at Union level and including cooperation finalised to increase situational awareness with other Union entities services such as relevant Commission services and in particular DG CNECT, CERT-EU, Europol/EC3, and EEAS including European Union Intelligence and Situation Centre (INTCEN) This activity benefits from ENISA's Cyber Partnership Programme managed under Activity 4 and the Agency's international cooperation frameworks.

Moreover, this activity includes the preparation of the regular in-depth EU Cybersecurity Technical Situation Report in accordance with CSA art.7(6), also known as the EU Joint Cyber Assessment Report (EU-JCAR), regular weekly OSINT reports, joint 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 NIS2 Art.23(9) is prepared and the work related to the Cyber Solidarity Act – Incident Review Mechanism (Art.21) is undertaken.

This activity also supports Member States with respect to operational cooperation within the CSIRTs Network and EU-CyCLONe by providing at their request advice on a specific cyber threat, assisting in the assessment of incidents and vulnerability, facilitating the technical handling of incidents, supporting cross-border information sharing and analysing vulnerabilities, including through the EU Vulnerability Database (EUVD) established under NIS2 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 Diplomacy Toolbox.

The work on the EUVD and CRA Single Reporting platform is complemented through the delivery of vulnerability services for EU stakeholders. This activity manages participation in the Common Vulnerabilities and Exposures (CVE) Programme, namely the work related to the CVE Root and participation in CVE governance structures.

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

Finally, this activity includes the work underpinning the establishment of the Single Reporting Platform (SRP) as established under the Cyber Resilience Act. In doing so, the Agency takes into account incident reporting frameworks implemented under Art.23 of the NIS2 Directive and other relevant EU laws to ensure alignment and future proof architecture for reporting simplification at EU level. Possible developments of the SRP to accommodate other legislation could also be part of this activity.

15 NIS2, CRA and Regulation (EU) 2023/2841.

This activity includes the continuous development and maintenance of a 24/7 monitoring system for situational awareness.

The budget of this activity is partially financed through a contribution agreement between ENISA and the Commission to support the work on the CRA and CSOA as well as contributions to the Commission's Situation and Analysis Centre.

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

The full list of statutory tasks that the activity undertakes arising from EU legislation is presented in annex 15.

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 crises
- Consolidated and shared cybersecurity information and knowledge support for Europe

Indicator for strategic objectives

EU Vulnerability Database is operationalised by ENISA and a 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 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
5.1. Build a common situational awareness between Member States based on shared accurate data and underpinned by validated joint analysis	CSA Art.7 NIS2 Art.23(9) CSOA Art.21	2025 to end of 2027	EU MSs contribute to and validate EU JCAR.	Cyber Security Assessment Tool (CSAT) for Joint Cyber Assessment Report (JCAR) >4 75% of EU MSs contribute to JCAR
			ENISA knowledge base is open to Member States and the leverage of information provided by EU MSs	Knowledge base is used by 40% of EU MSs.
				Feedback provided by EU MSs pertaining to missing or inaccurate entries is less than 10% of the total of incidents taken into account.
			Establish and test processes and procedures for the Incident Review Mechanism under Art.21 of CSOA	Process for Interoperable EU Risk Management (IRM) is endorsed by EU MSs by Feb 2026 CSAT on IRM report is > 4
5.2. Regularly provide general as well as specific threat landscapes and threat analysis, based on observed and data-driven trends in incidents and vulnerabilities	CSA Arts.7 and 9 NIS2 Art.23(9) CSOA Art.21 CRA Arts.14-17	2025 - 2027	Publish ENISA Threat Landscapes	Publish an annual Threat Landscape CSAT on ETL is >4 from selected communities
			JCAR includes threat analysis based on incidents and vulnerabilities available within ENISA data repositories (EUVD, Cybersecurity Incident Reporting and Analysis System (CIRAS), CRA SRP)	Incident analysis is included in JCAR as of Q4 2025.
				CRA SRP, Adversarial Exposure Validation, (AEV) and Incidents analysis is included by Q4 2026
			Ability of ENISA to publish accurate threat analyses based on incidents, vulnerabilities and on the Agency's own monitoring, shared by external stakeholders voluntarily or due to legal obligations[16]	80% of recipients score quality of threat analysis provided by ENISA above 4 (1-5)
				80% of recipients score ability of ENISA to use information available to produce threat analyses and recommendations above 4 (1-5)
			CRA SRP is established and operational	CRA SRP is used to carry on tasks under CRA by Q4 2026

16 - NIS2, CRA and Regulation 2023/2841.

ACTIVITY 5 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
5.1. Collect, organise and consolidate information (including for the general public) on common cyber situational awareness, threat analysis, technical situational reports, incident reports and support consolidation as well as exchange of information on strategic, operational and technical levels[17]	Establishment of a Threat Information Management Platform Publication of situational awareness and threat analysis reports, production of briefings and summaries of incidents 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 reports	Overall stakeholder satisfaction	Biennial (survey)	84%	85%
			Timeliness and Accuracy of reports	Biannual (survey)	84,2%	85%
5.2. Provide analysis and risk assessment (such as JCAR and ETL) jointly with other operational partners including Union Entities, Member States, industry partners, and non-EU partners	Union joint reports and briefings, sectorial analysis, threat analysis[18] Recipients receive accurate and timely assessment of threats faced by the EU Internal Market	CSIRT Network, EU CyCLONe, Union entities, HWPCI, Management Board	Stakeholder satisfaction	Biennial (survey)	84,2%	85%
			Number of contributing EU MSs to EU JCAR	Annual (report)	10	15
5.3. Collect and analyse information to report on the cyber threat landscapes	Mapping threats Generate recommendations for stakeholders to take up	NLO, CSIRTs Network / CyCLONe ISACs Advisory Group	Overall stakeholder satisfaction	Biennial (survey)	91.5%	90%
			Number of downloads of ETL	Annual (report)		+10%
5.4. Analyse and report on incidents as required by Art.5(6) of CSA as well as other sectorial legislations (e.g. DORA, eIDAS Art.10, etc.)	Analysis of incidents Generate recommendations for stakeholders to take up	Workstream 3 the NISD CG, CSIRT Network	Stakeholder satisfaction	Biennial (survey)	91.5%	>91%
5.5. Establish the CRA Single Reporting Platform and operationalise the EU Vulnerability Database (EUVD) Services	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 CRA Platform is operational EU vulnerability database	Biennial (survey)	N/A	by 11 Sept 2026 Key enhancement validated by stakeholders

17 Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.
18 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, EU-CyCLONe and NIS Cooperation Group), EU Entities, 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
Activity resources from EU subsidy	**Budget: €1 274 000**	**FTE[19]: 13**
Other supplementary contributions	**Budget planned for 2026: €263 806 (outputs 5.1 and 5.2) SitCen Budget, €5 754 460 (output 5.5) to implement CRA SRP tasks + €100 000 CRA preparatory work** **Total contribution Budget: €447 973 (outputs 5.1 and 5.2) for SitCen Budget €11 947 620 (output 5.5) to implement CRA SRP tasks[20] + €400 000 prep work for CRA SRP[21]**	**FTE: 7[22]**

19 Target FTEs.

20 Please refer to annex 11 for further details regarding contribution agreements. The amount indicated refers to years 2026 to 2027.

21 Contribution Agreements signed with Commission in 2024, applicable until July 2026.

22 Additional FTE financed via contribution agreements (SitCen and CRA SRP). Please refer to annex 11 for further details regarding contribution agreements.

ACTIVITY 6:
Provide services for operational assistance and support

Overview of activity

This activity contributes to the further development of response capabilities and preparedness 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. Following the entry into force of the Cyber Solidarity Act, this activity is tasked with the administration and operationalisation of the EU Cybersecurity Reserve, whose administration and operation has been entrusted by the Commission to ENISA. The Reserve requires the delivery of incident response services. 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 Reserve may also involve the provision of preparedness services closely related to incident prevention and response in the form of the conversion of pre-committed incident response services, in cases where the latter have not been consumed in full.

This activity also implements Cybersecurity Support Action, through which the Agency provides services such as pentesting, threat hunting, risk monitoring and assessment, customised exercises and training sessions, and supports Member States with incident response. Following the establishment of the Reserve, the Cybersecurity Support Action will be phased out in 2026, with service delivery expected to end in all MSs by the end of Q2.

In developing the service delivery framework for the services mentioned above, the Agency worked together with the Commission and the users of the Reserve and Support Action in order to tailor the service catalogue to the needs of the users, while maintaining scalability and flexibility. The Agency also maintains the contractual framework with trusted providers, in accordance with the relevant provisions of the Cyber Solidarity Act, in order to ensure availability of all required services for all types of users, including users outside the MSs, such as CERT-EU/Union entities and DEP-associated third countries. In order to strengthen the service delivery framework, the Agency has also implemented a framework to assess the impact of services delivered and has introduced a 24/7 incident support capability.

These activities are resourced through the use of 10 Contract Agents recruited as a direct cost of the programme and financed through the Commission contribution agreements. ENISA will not be able to resource this activity with its current establishment plan; it follows that the conditions of recruitment and employment of these resources will differ from those applying to staff under the establishment plan of the Agency. The budget for this activity is provided from three individual contribution agreements that extend to mid-2028.

In addition to the activities mentioned above, ENISA will, in collaboration with CERT-EU, work towards operationalising a virtual CISO (vCISO) service to provide advisory services to three agencies conducting risk assessment, or full risk assessment services depending on the case.

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

The full list of statutory tasks that the activity undertakes arising from EU legislation is presented in annex 15.

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 administration and operation is to be entrusted fully or partly to ENISA and used by MS, Union Entities and on a case by case basis DEP associated third countries

ACTIVITY 6 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
Deliver and complete ENISA's Cybersecurity Support Action by the end of Q2 2026	CSA Arts.6 and 7	Q2 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 (survey) Complete tasks on time and in budget (survey)	4 (1 to 5 score)
By the end of Q2 2026 and thereafter, deploy the European Cyber Reserve under CSOA.	CSA Arts.6 and 7	Q2 2026	Reaching consensus on actions and their prioritisation with the EC on the European Cyber Reserve. (survey) Timely deliver. (survey)	4 (1 to 5 score)

ACTIVITY 6 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
6.1. EU Cybersecurity Reserve	Operationalisation of the Reserve and delivery of incident response services to the users of the Reserve, with the possibility of conversion of pre-committed services to incident preparedness and response services	MSs CNECT CERT-EU	Percentage of MSs for which the Reserve is operational Satisfaction score	Annual (survey)	N/A	90% of MSs 4 (1 to 5 score)
6.2. Cybersecurity Support Action	Delivery of ex-ante and ex-post services until completion of the programme	MSs CNECT Beneficiaries	Percentage of MSs receiving service under Support Action Satisfaction score		N/A	80% of MSs 4 (1 to 5 score)

Stakeholders and engagement levels

Partners: EU Member States, Selected Beneficiary Entities, Commission, Union Entities, CERT EU

Involve / Engage: EU-CyCLONe, CSIRT Network, DG CONNECT, NIS Cooperation Group (CG), private sector providers[23]

23 ENISA cybersecurity support action services.

ACTIVITY 6 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: N/A**	**FTEs: 4**
Other supplementary contributions	**This activity is funded by contribution agreements between ENISA and the Commission. The figures below reflect the direct costs related to the implementation of the contribution agreements[24].** **Budget planned for 2026:** • **€4 562 434 contribution agreement signed in 2023[25]** • **€380 977 contribution agreement signed 2024** • **€10 835 869 contribution agreement signed in 2025**	**5 FTEs financed from the Contribution Agreement signed in 2023 and 3 FTEs financed from the Contribution Agreement signed in 2025**

24 An additional 7% of the contribution agreements budget is reserved for indirect costs incurred by ENISA for implementing the respective actions. This amount is managed by Activities 9, 10 and 11.

25 Please refer to annex 11 for further details regarding contribution agreements.

ACTIVITY 7:
Development and maintenance of EU cybersecurity certification framework

Overview of activity

In line with the political priorities of the new EC established in 2024, the development, maintenance and promotion of the EU cybersecurity certification framework is crucial given its impact on promoting the EU cybersecurity digital market and overall resilience. The work on certification expands not only in developing new candidate certification schemes but, as of 2025, EUCC and other schemes will be in force. These too will require the maintenance, promotion and support of National Cybersecurity Certification Authorities (NCCAs) with capacity building and uptake initiatives. It is essential therefore to ensure that this activity is adequately resourced to cater for the additional streams of work.

This activity encompasses actions that seek to establish and support the EU cybersecurity certification framework by preparing candidate cybersecurity certification schemes in accordance with Art.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, activities related to requests for the ID Wallet certification scheme as a priority and other schemes under development (EUCS, 5G) as well as additional activities for requested Managed Security Services (MSSs) in 2025 following the entry into force of the amendment to the CSA. These actions also include supporting maintenance and review, as well as the evaluation of adopted European cybersecurity certification schemes, in particular the adopted 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 reviews, cryptographic mechanisms) as well as with co-chairing and providing a secretariat for the Stakeholder Cybersecurity Certification Group (SCCG).

ENISA has developed one candidate scheme, based on an EC request from 2019, in accordance with Art.49.2, which was adopted as an Implementing Regulation, the EUCC. ENISA is currently developing four other candidate schemes also based on EC requests, the EU Cloud Certification Scheme (EUCS), the EU Managed Security Services (EUMSS), the EU Digital Wallet (EUDIW) and the EU Certification Scheme for 5G Networks (EU5G), in accordance with Art.49.2. The URWP was adopted in February 2024, and the most recent request received for the development of an EUDI wallet candidate scheme is in line with Art.49.1. The request for an EU scheme on MSs is in line with Art.48.2, as foreseen by the URWP and the amendment to the CSA, based on a feasibility study by ENISA. ENISA also explores feasibility studies on other topics listed in the URWP but for which no candidate scheme request is formally issued in order to facilitate the delivery of the candidate schemes once the request has been received.

As certification schemes become adopted, with EUCC being the first one in 2024, maintenance of these schemes will require continuous efforts by ENISA in addition to the resources to be allocated to newly requested schemes. Given ENISA's finite resources, conducting both actions (development and maintenance) would impose a strain on ENISA's resources and as a consequence efforts to compensate by deprioritising actions might be needed.

ENISA also makes available and maintains a dedicated European cybersecurity certification website according to Art.50 of the CSA. Since 2024, ENISA has been seeking 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 laws include the NIS2 Directive, DGA EUDI Wallet, AI Act, Chips Act and Data Act.

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

The full list of statutory tasks that this activity undertakes as required by EU legislation is presented in annex 15.

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
Between 2025-2027, timely development of feasibility studies for future potential schemas	CSA Art.49	2027	Number of feasibility studies concluded in view of upcoming requests	Three (pending potential new requests for scheme)
			Elements of feasibility study reflected or aligned in EC request for new schemes	More than 50%
Between 2025-2027, timely finalisation of candidate schemes following formal requests for drafting new cybersecurity certification schemes	CSA Art.49	2027	Number of drafts of certification schemes delivered to COM (ID Wallet Certification and Managed Security Services	2
			ECCG endorsement of draft certification schemes	Positive ECCG endorsement
			SCCG satisfaction on draft certification schemes (satisfaction survey)	More than 60%
Ensure the maintenance of existing schemes and support their roll-out	CSA Art.49	2027	Number of schemes maintained with ENISA active involvement	1 (EUCC)
			Satisfaction by ECCG with ENISA's supporting efforts for documents for maintenance	75%
			Number of certificates issued and published under an EU certification scheme; high usage rate in the market.	Proportionate[26] number of certificates issued migrating to a new EUCC scheme compared to a previous framework

26 ENISA monitors the certificates issued under SOG-IS and the transition to EUCC will have to be proportional to the number of certificates issued.

ACTIVITY 7 OUTPUTS

Description	Expected Results Of Output	Validation	Output Indicator	Frequency (Data Source)	Latest Results	Target 2026
7.1. Drafting and contributing to the preparation (via feasibility studies *inter alia*) and establishment of candidate cybersecurity certification schemes[27]	Scheme meets stakeholder requirements, notably those of the 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 ECCG European Commission	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			Number of opinions of stakeholders managed	Annual (report)	27 MSs and the Commission delivered through ECCG	5% increase compared to latest results
			Number of people or organisations engaged in the preparation of certification schemes	Annual (report)	EUCS scheme: 17 EU5G: 25 EUDI Wallet: 25 MSs: 15	5% increase compared to latest results
7.2. Implementing and maintaining the established schemes including evaluating adopted schemes, reviewing and updating state-of-the-art documents, 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 European Commission	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			ECCG satisfaction with ENISA's efforts on schemes adopted	Triennial (survey)	N/A	5% increase compared to latest results
7.3. Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks; supporting peer reviews and capacity building of NCCAs		ECCG European Commission SCCG NCCAs	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			Feedback from statutory bodies including NCCAs on ENISA's role	Annual (survey)	72%	5% increase compared to latest results
			Satisfaction with ENISA's role in NCCA peer reviews	Triennial (survey)	n/a	5% increase compared to latest results
7.4. Developing and maintaining necessary provisions, tools and services concerning the Union's cybersecurity certification framework (including certification website, supporting the Commission in relation to the core stakeholders service platform of CEF (Connecting Europe Facility) for collaboration, and the publication and promotion of the implementation of the cybersecurity certification framework, etc.)	Supporting with transparency and trust ICT products, services and processes Stakeholders engagement and promotion of certification	ECCG European Commission SCCG	Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results
			Users' satisfaction concerning the certification services on the website	Annual (survey)	N/A	5% increase compared to latest results
			Usage of certification website	Annual (report)	N/A	75%
7.5. Promoting and monitoring the uptake of certification and the interplay with other legislative files (e.g. CRA, AI Act, etc.)	Increase in uptake of certification Increase in NCCAs maturity	ECCG European Commission NCCAs	Composite indicator on number of issued certificates and their use	Annual (survey)	N/A	TBD
			Stakeholder satisfaction	Biennial (survey)	72%	5% increase compared to latest results

27 Notably on the EU Digital Identification Wallets (EUDIW) and Managed Security Services (MSS).

Stakeholders and engagement levels

Partners: EU Member States (including National Cybersecurity Certification Authorities, ECCG, European Commission, Union institutions, bodies, offices 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
Activity resources from EU subsidy	**Budget: € 631 610**	**FTE[28]: 10**

28 Target FTEs.

ACTIVITY 8:
Supporting market, technology and product-security

Overview of activity

This activity seeks to foster the cybersecurity of technologies, products and services in the European Union along with the development of the cybersecurity market, industry and services, in particular SMEs and start-ups, to foster cybersecurity competitiveness, strengthen the EU single market and increase the capacity of the Union 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 (a) new emerging technologies (including supporting MSs and the COM in tackling challenges regarding AI and post-quantum cryptography and 6G) and in (b) ICT products, services and processes, including through the development and assessment of technical guidance and specifications, standardisation and the adoption of relevant codes of conduct. As such, this activity will support the development of good cybersecurity engineering practices for products, services and technologies. In doing so, the activity will also build an effective role for ENISA in supporting the implementation of the CRA, notably in terms of the assessment of draft European harmonised standards, the assessment and the development of technical guidance, market analysis, preparation of conformity assessments and market surveillance activities and the collection and analysis of information for the identification of emerging cybersecurity risks in products with digital elements, etc. Preparatory and support actions arising from the CRA will continue to increase in the coming years, particularly in support of markets in MSs and the notification of authorities on behalf of the Commission and the provision of technical advice on implementation to manufacturers including SMEs.

The actions to support this activity encompass producing analyses of standardisation procedures, landscape and gap analysis, and guidelines as well as good practices on cybersecurity and data protection requirements, facilitating the assessment, establishment and take up of European and international standards across applicable areas such as risk management. These actions also include performing regular analyses of cybersecurity market trends on both the demand and supply sides including monitoring, collecting and identifying dependencies among ICT products, services and processes and the vulnerabilities present therein as well as reported incidents. This activity aims at strengthening and reinforcing ties with the private sector and promoting collaboration among the players in the cybersecurity market in order to improve the visibility and uptake of trustworthy and secure ICT solutions in the digital single market.

In parallel, this activity aims to provide advice to EU Member States (MSs), EU institutes, bodies and agencies (Union Entities) on research needs and priorities in the field of cybersecurity, thereby contributing to the EU's strategic research and innovation agenda, notably the ECCC. The ecosystem of the ECCC and the National Coordination Centres (NCCs) will be consulted for these actions. A strong collaboration and mapping of relevant requirements of the market authorities as defined in the CRA will also take place in the context of this activity. To prepare this strategic advice, ENISA will take full account of past and ongoing research, development and technology assessments, outputs of other statutory bodies in the cybersecurity landscape such as the NIS Cooperation Group, the CRA Administrative Cooperation Groups (Market surveillance authorities), ECCG, CSIRTs Network, EU-CyCloNe, and 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 establish a technology and innovation radar to support these activities.

This activity also encompasses ENISA's support to the European Digital Identity Regulation and the European Digital Identity Cooperation Network, by providing advice and, upon request, targeted guidelines in order to ensure deployment and uptake of secure digital wallet solutions, as well as foster the trusted services ecosystem.

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

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

The full list of statutory tasks that the activity undertakes based on EU legislation is presented in annex 15.

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 to the implementation of the CRA Market Supervisory Authorities (MSAs) and the European cybersecurity certification framework (ECCG)

Amount of advice and level of support given on Research and Innovation Needs and Priorities to the ECCC and its uptake by ECCC

ACTIVITY 8 OBJECTIVES

Description	CSA Article And Other EU Policy Priorities	Timeframe Of Objective	Indicator	Target
Implement a 'market' monitoring and analysis framework that delivers relevant and regular, as well as ad hoc, reports on the trustworthiness of products with digital elements under the CRA, including important critical products	CSA Arts.8, 52, 59 and 60	End of 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	2/3rds of MSs validating and endorsing the ENISA framework
Provide continuous comprehensive support to market surveillance by MSs and notify authorities and the COM as well as manufacturers including SMEs that they should implement CRA requirements	CRA Arts.29, 52, 59 and 60	2026	MSs and COM stakeholder satisfaction survey	More than 70%
Create a technology and innovation radar to understand the level of impact that new technologies have on cybersecurity	CSA Arts.9 and 11	2026	Number of cybersecurity trends and patterns accurately identified through an evidence-based methodological approach	5% increase over reference data
			Impact of assessment 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 2026
8.1. Collect and analyse information on new and emerging information and communications technologies (notably AI and PQC), support the COM and MSs with appropriate technical guidelines as necessary, 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 and providing guidelines on them Advising EU funding programmes including the ECCC and its Strategic Agenda and Action Plan.	Academia, Industry and National R&I bodies, MSs' market authorities (including NCCs) and Union Entities NIS CG, EC including CNECT and JRC, ECCC and NCCs, as appropriate	Stakeholder satisfaction	Biennial (survey)	91%	5% increase over reference data
			Findings endorsed by MSs (NCCs and market authorities)	Annual (survey)	N/A	5% increase over reference data
			Guidelines issued and endorsed by NIS CG	as relevant	N/A	5% increase over reference data
			ECCC Strategic Agenda and Action Plan alignment	Annual (survey with ECCC GB)	N/A	5% increase over reference data
8.2. Market analyses on the main trends in the cybersecurity market on both the demand and supply sides, and prepare the framework for the biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements[29]	Improved understanding of the market and industry Framework for the ENISA biennial technical report under the CRA	Cybersecurity market analysis by ad hoc working groups Advisory Group NLO (as necessary) MSs' Market surveillance authorities (as necessary)	Stakeholder satisfaction	Biennial (survey)	88%	5% increase over reference data
			Cybersecurity market analysis; cybersecurity products and services	Annual (framework and reports) (survey)	N/A	5% increase over reference data
			Endorsement by MSs of report on emerging trends regarding cybersecurity risks in products with digital elements	Biennial (report)	N/A	5% increase over reference data
8.3. Support for the implementation of the CRA, including assessment of standards, technical guidance and the activities of market surveillance authorities as well as the identification of categories of products for simultaneous coordinated control actions and, upon request, conducting evaluations of products that present a significant cybersecurity risk.	Assessment of 41 vertical and horizontal standards (CRA standardisation request) Monitoring and following-up on requirements of market surveillance authorities Identify categories of products; produce a methodology for market surveillance and product testing, including in view of market sweeps; carry out market sweeps Technical recommendations on conformity assessment, including in view of notification of CABs under the CRA Technical guidance for the security-by-design and security-by-default principles including for SMEs Evaluations to be carried out ideally on the basis of input from market sweeps; rely on external expertise.	MSs' Market Surveillance Authorities NLOs Commission MSs Notifying authorities CRA Expert group	Collection of requirements Matching requirements with deliverables Time to carry out market sweeps Methodology for evaluations Profiles of experts	Assessment of standards on continuous basis starting in 2025 Security-by-design and security-by-default technical guidelines (reports, checklists) to be issued in 2026 and updated on a continuous basis ENISA SME strategy for the CRA in 2026 and updated on a continuous basis Technical support and recommendations on conformity assessment to be issued in 2026 and updated on a continuous basis	N/A	5% increase over reference data

29 The biennial report is a statutory task for ENISA as per Art.14 of the CRA; the first report is expected two years after the CRA enters into force.

				Market sweeps as of 2027 (3-years transition) or earlier if requested Method to evaluate products in 2026, to be updated regularly Guidance and criteria to accept evaluation results in 2026 to be updated on regular basis		
8.4. Monitoring developments in related areas of standardisation, analysis of standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification	Monitoring of cybersecurity standardisation activities Input to the EU standardisation agenda	CEN/CENELEC/ETSI European Commission Ad hoc working groups (as necessary) Advisory Group NLO (as necessary)	Stakeholder satisfaction	Biennial (survey)	88%	5% increase over reference data
			Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification.	Annual (report)	N/A	5% increase over reference data
8.5. Supporting the implementation of eIDAS2 Regulation and the deployment and uptake of European Digital Identity Wallets	Best practices and guidelines to support implementation of eIDAS2 Monitoring of the uptake of Digital Wallets	European Digital Identity Cooperation Network EC	Stakeholder satisfaction	Annual (survey)		5% increase over reference data

Stakeholders and engagement levels

Partners: EU Member States (including market surveillance authorities and entities with an interest in cybersecurity market monitoring e.g. NCCA, National Standardisation Organisations, European Commission, Union institutions, bodies, offices and agencies, European Standardisation Organisations (CEN, CENELEC, ETSI), private sector or ad hoc standards setting organisations, EC Joint research centre, National and EU R&I entities, academia and industry, European Cybersecurity Competence Centre and National Cybersecurity Coordination Centres, EC AI Office, European Digital Identity Cooperation Group, European Data Innovation Board

Involve / Engage: Private Sector stakeholders via ad hoc working groups, International Organisation for Standardisation, International Electrotechnical Committee, Consumer Organisations, EDPS, EDPB

ACTIVITY 8 RESOURCE FORECASTS

	Budget	FTEs
Activity resources from EU subsidy	**Budget: € 578 200**	**FTE: 10**

3. 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 Art.4(1) of the CSA that sets an objective for the Agency to: 'be a centre of expertise on cybersecurity by virtue of its **independence**, the scientific and technical **quality of the advice and assistance it delivers**, the information it provides, the **transparency of its operating procedures**, its 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 individual administrative practices as well as the promotion of sustainability across all the Agency's operations. In addition, and in line with Art.4(2) of the CSA, this activity includes contributing to efficiency gains, e.g. via shared services in the EU Agencies network by relying on the Agency's own expertise (e.g. cybersecurity risk management).

Under this activity ENISA seeks to deliver against key objectives of the Agency's Corporate Strategy (service-centric and sustainable organisation), including by establishing a thorough quality assessment framework, ensuring proper and functioning internal controls and compliance checks, as well as maintaining a high level of cybersecurity across all the Agency's corporate and operational activities. Enhancing and maintaining the cybersecurity posture of the Agency requires the execution of a cybersecurity maturity plan in order to reach the maturity level required by the Agency for the legislative tasks assigned to it, such as the EU Vulnerability Database, the CRA and DORA platforms and to be in compliance with Regulation (EU) 2023/2841.

In terms of resource management, the Budget Management Committee coordinates the Agency's adherence to financial management principles. 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 Arts.4(1) and 4(2) of the CSA, as well as Arts.24-28, Art.41 and Arts.32 - 33 (ENISA financial rules on 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	73%	>80% of indicators outperformed
	Continuous innovation and service excellence	Results of Internal control framework assessment	Annual	Effective (Level 2)	Effective level 1 or 2
	Developing service propositions with additional external resourcing	High satisfaction with essential corporate services in the area of compliance and coordination	Annual	75%	>60%
9.B. Increase corporate sustainability	Ensure ENISA is climate neutral by 2030	Maintain EU Eco-Management and Audit Scheme (EMAS)	Annual	EMAS audit conducted on 27/2/25	Timely implementation of follow up actions to ensure EMAS certification is maintained
	Develop efficient framework for ENISA's continuous governance to safeguard high level of IT	Agency IT strategy aligned with corporate strategy Proportion of total IT budget allocated to information security proportional to the level of risks identified across IT systems within Agency	Annual	Revised IT strategy proposal submitted end 2024; strategy to be adopted by Q2 2025 18% of total IT costs	70% implementation (ITMC reporting) 20%

ACTIVITY 9 OUTPUTS

Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2026
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	Unified day-to-day practices across the Agency upon implementing SPD Annual risk assessment and internal controls assessment performed and reported Legal and regulatory compliance are monitored; issues and areas of improvement identified. Streamlined IT system management across the Agency and in accordance with ENISA's IT strategy; under ITMC Streamlined budget management across the Agency; under BMC Maintenance of EMAS Certificate	MT, ITMC & BMC External and internal audits Statutory bodies	Number of high risks identified in annual risk assessment	Annual (survey, internal reports)	3	<3 30% reduction in high risks identified in previous year
			Effective monitoring of high risks and critical recommendations to follow up on timely implementation of mitigation measures by business owners		N/A	Risk plans are generated in a timely manner, agreed with risk owners and reported to MT (on a quarterly basis at least)
			Percentage of identified deficiencies in internal controls addressed within timelines		No critical recommendation issued in 2023 ICF assessment. Out of 3 moderate and 2 major – the recommendations remain valid as the deficiencies have not been fully mitigated	100% for critical, 80% for major, 60% for moderate
			Timely follow-up and resolution of internal and external audits (in particular from IAS and ECA) recommendations and findings			<180 days
			Number of identified regulatory breaches		3	0 for critical/ major, <=3 for moderate
			Percentage of revised and up to date corporate rules (MBD, EDD, policies, processes)		23 MBDs on corporate rules from before 2019	60% corporate rules which have not been reviewed less than three years ago; 80% corporate rules which have not been reviewed less than four years ago
			Annual report on ARES maintenance and actions		N/A	Follow up of maintenance and actions
			Reduction of CO2 emissions in ENISA HQ		N/A	Timely submission of report with actions and recommendations
			Efficiency and effectiveness of ITMC & BMC (survey)		TMC: 75% BMC: 63%	> 60%

9.2. Maintain and enhance ENISA's cybersecurity posture in line with the Agency's multiannual cybersecurity maturity plan (2026 – 2028)	Compliance with Regulation (EU) 2023/2841 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) Coordination and implementation of the cybersecurity maturity plan of the Agency for 2026	MT and relevant committees Statutory bodies Interinstitution-al Cybersecurity Board (IICB) External and internal audits	Percentage of identified high risk mitigation measures addressed within timelines	Annual	All high risks addressed within timelines and/ or accordingly reported and planned	>90%
			Annual risk assessment (RA) and risk treatment plan with the relevant business owners	Annual	N/A	RA and risk treatment plans conducted timely and in line with Regulation (EU) 2023/2841
			Cybersecurity measures implemented according to maturity plan and for set timelines	Annual	N/A	Measures and timelines in accordance with the cybersecuri-ty masterplan
			Address all potential cybersecurity incidents	Annual	N/A	All cybersecurity incidents addressed in a timely way
			Cybersecurity training for staff and managers	Annual	Two training sessions by ISO; training programme and phishing exercise (via dedicated training platform)	>2 training sessions by ISO
9.3. Provide support services to the EU Agencies network and in key areas of the Agency's expertise	Shared services in the area of data protection, legal services and accounting EUAN troika shared services pilot	MT, BMC EUAN (Agencies receiving ENISA's support)	Satisfaction within the EU Agency network with ENISA support services	Annual	High satisfaction expressed by the agencies that received ENISA's services	70% satisfaction for the services offered under the EUAN Shared Services Pilot (survey)
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 (survey)	66% of staff survey respondents agree that ENISA's internal communication is timely and clear (last year's survey showed 39%)	50%
			Response timeliness to external parties (internal reporting)	Annual	High response rates in accordance with ENISA's code of conduct	High response rates in accordance with ENISA's code of conduct

Stakeholders and engagement levels

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

ACTIVITY 9 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	**Budget: €432 000**	**FTE: 15**[30]
Other supplementary contributions	**Budget: €54 604 SLA with ECCC, see annex 11 for additional information** **Budget: €1 269 100**[31]	**FTE: N/A**

30 Target FTEs Including ED, COO, ACOO and accounting officer.

31 Budget from contribution agreements forecasted for implementation of cybersecurity maturity plan led by activity 9 with support from activities 4 and 11. Please see annex 11 for further information.

ACTIVITY 10:
Reputation and Trust

Overview of activity

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

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

The legal basis for this activity is Art.4(1), Section 1 and 2 as well as Arts.21, 23 and 26 of the CSA; 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
10a. Protect and grow the Agency's brand	Ensure efficient corporate services	Level of trust in ENISA (as per Biannual Stakeholder Survey)	Biennial	95%	95%
10b. Improve the outreach of ENISA's mandate	Ensure efficient corporate services				
		Stakeholder satisfaction with ENISA events	Annual (Survey)	88%	>80%
		Number of unique website visitors	Annual	N/A	>5% increase year on year

ACTIVITY 10 OUTPUTS

Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2026
10.1. Review and implement the multiannual communications strategy and support stakeholders' strategy including corporate outreach	Enhanced transparency and outreach Engaged communities Increased impact of ENISA activities Relevant and easily accessible information is provided to stakeholders	Management Team and Agency stakeholders	Number of social media engagements	Annual (Media monitoring)	66.3k	68k
			Stakeholder satisfaction with ENISA outreach	Biennial (survey)	96%	>80%
			Number of total ENISA website visits	Annual (website analytics)	2.3 million	1.5 million[32]
10.2. Implement internal communications strategy	Engaged staff	Management Team and staff committee	Staff satisfaction with ENISA internal communications	Annual (survey)	65%	>70%
10.3. Manage and provide the secretariat for statutory bodies, i.e. EB, MB, AG, NLO (excluding certification)	Support the operation and organisation of ENISA statutory bodies Support effectiveness of implementation of work programmes (validation of operational outputs) Provide administrative support for the day-to-day working of the Management board's decisions and recommendations from NLO & AG	Statutory bodies, Management Team and Committees	Number of times feedback is received per NLO consultation	Annual (Internal report)	27 for NLO subgroups (3.6 is average for validations in NLO Network	>6
			Number of times feedback is received per AG consultation	Annual (Internal report)	11.3 on average	>8
			Satisfaction of statutory bodies with ENISA's support to fulfil their tasks as described in CSA	Annual (survey)	97%	>80%

Stakeholders and engagement levels

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

Involve / Engage: All ENISA stakeholders

ACTIVITY 10 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	**Budget: €1 270 815**[33]	**FTE :7.5**[34]

32 New website and analytics have impacted measurement.

33 Including the budget centralised for operational missions and large-scale events.

34 Target FTEs.

ACTIVITY 11:
Effective and efficient corporate services

Overview of activity

This activity seeks to fulfil the requirements of Art.3(4) of the Cybersecurity Act which calls on 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 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 workplace 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 recognises 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 ENISA's IT strategy.

The activity is responsible for decommissioning the Heraklion data centre before the end of Q2 2026 and its migration.

ACTIVITY 11 ANNUAL OBJECTIVES

Description	Link to corporate objectives	Activity indicators	Frequency (Data source)	Latest result	Target
11a. Enhance people-centric services by implementing the Corporate and HR strategy	Effective workforce planning and management Efficient talent acquisition, development and retention Caring and inclusive modern organisation	Implementation of Strategic Workforce Planning and Review decisions	Annual	Fully implemented	Fully implemented
		Implementation of the Corporate and HR strategies		Vacated staff posts in 2024 were fulfilled within 143 days. The indicated KPI was to fulfil posts within 300 days	Proposal new KPI: Vacated post are fulfilled within 200 days Provide updates on new and revisions of: Policies introduced Policies updated Related MB decisions Related ED decisions
		High participation in staff satisfaction survey		80%	75% participation rate

11b. Ensure sustainable and efficient corporate solutions and promote continuous improvement	Ensure efficient corporate services Introduce digital solutions that maximise synergies and collaboration within the Agency Developing service propositions with additional external resourcing Promote and enhance ecologic sustainability across all the Agency's operations Develop efficient framework for ENISA's continuous governance to safeguard high level of IT and physical security	Implement best practices in sustainable IT solutions	Annual	Fully implemented according to plan	IT strategy updated accordingly
		Limited disruption of continuity of corporate services	Annual	Effective disaster recovery is in place to ensure business continuity of its core services.	On demand corporate IT facilities, financial and HR services in 2025
		Handling EUCI at the level of SECRET UE/EU SECRET	Annual	EU Classified Information (EUCI) inspection took place and the report will be sent in 2025.	Operational for the first full year in 2025

ACTIVITY 11 OUTPUTS

Description	Expected results of output	Validation	Output indicator	Frequency (data source)	Latest results	Target 2026[46]
11.1. Manage and provide horizontal, recurrent, administrative services in the area of HR, Finance and Procurement for ENISA staff and partners	Services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently. Implementation of the Unit's annual plan in procurement, L&D and recruitment Set up Service Level Agreements in areas such as HR, Finance, Procurement and Contract Management Establish reporting capabilities in areas such as HR, Finance and Procurement (monthly Heads of Unit (HoUs), quarterly Introduce MS planner to all Corporate Support Services Unit (CSS) to capture workload indicators Introduce Service Now as main ticketing system across all CSS services Expand Service Catalogue to Paymaster Office (PMO) and DG HR Review ENISA CSS intranet page	Management Team IT Management Committee Budget Management Committee Staff Committee	Turnover rates	Annual (internal reports)	4.1%	<5%
			Posts in Establishment Plan filled		98%	>95%
			Percentage of the approved Recruitment plan that is implemented		94%	>90%
			Percentage of the approved Procurement Plan that is imple-mented		63.63%	>90%
			Percentage of the budget that is implemented		100%	>95%
			Average time for initiating a transaction Financial Initiating Agent (FIA) role		7.51%	<7 days
			Average time for verifying a transaction Financial Verification Agency (FVA) role)		0.19	<3 days

11.2. Implement the 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 strategies are met Launch and evaluation of Staff Satisfaction Survey Implementation of the ED decision on annual workforce review [adopted in April 2024] Revision of following policies: 1/ Recruitment & External Mobility 2/ Staffing 3/ Wellbeing and Medical 4/ Probation 5/ MB Seconded National expert (SNE) rules 6/ Amendment of Financial Regulations 7/ Management of Indirect costs 8/ Reimbursement of Experts 9/ Physical Security and Access Control 10/ Incident Reporting and Facility Fault Response 11/ Evacuation and Preparedness (Priority 2025) 12/ Learning & development (L&D) policy 13/ Trainee policy 14/ Stand-by duty policy	Management Board Management Team Staff Committee EUAN Budget Management Committee (BMC)	Number of policies/ IR reviewed/ processes revised	Annual (internal report)	10	> 10
			Percentage of staff satisfaction with talent development		52%	>50%
			Percentage of actions implemented as follow up on results of staff satisfaction survey and implemented on time		N/A	>80%
			Number of competency-driven training and development activities implemented		<10	< 10
			Number of multisource feedback evaluations implemented and followed up		16	> 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. Decommission data centre in Heraklion and programme manage new data centre Programme manage EC tools of budget & HRT transition Expand Service Now (Finance, Procurement, HR, Reporting) Improve Physical security services	Management Team IT Management Committee Budget Management Committee Staff Committee	Staff satisfaction with working environment	Annual	80%	>70%
			Time to respond to IT, safety and security incidents.		n/a	<3 days to respond
			Average time to respond to facilities management requests		2 days	<1 day to acknowledge and <3 days to respond
11.4. Enhance operational excellence and digitalisation through modern, safe, secure and streamlined ways of working and the introduction of self-service functionalities	Services such as access management, meeting room facilities, equipment renewal, cloud-based solutions and data availability are efficient.	Management Team IT Management Committee	Critical systems uptime/downtime	Annual	100%	99%
			Staff satisfaction with IT resolution		82.53%	85%

Stakeholders and engagement levels

Partners: ENISA staff members and EU Entities

Involve / Engage: Private Sector and International Organisations

ACTIVITY 11 RESOURCE FORECASTS

	Budget	FTEs
Total activity resources	**Budget: €4 495 624**[35]	**FTE : 21.5**[37]
Other supplementary agreements	**Budget: €320 900**[36]	

35 Excluding staff in active employment and recruitment expenditure including €414 500 from C1 for data centre migration.

36 Target FTEs.

37 Budget from contribution agreements forecasted for date centre migration; please see annex 11 for further information.

TP-01-26-003-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union