EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2025 Consolidated Annual Activity Report

JUNE 2026

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONTACT

To contact the authors, use info@enisa.europa.eu

For media enquiries about this paper, use press@enisa.europa.eu.

LEGAL NOTICE

This publication presents the annual activity report of ENISA for 2025. The report is based on the 2025 work programme as approved by the ENISA Management Board Decision No MB 2026/08. The ENISA Programming Document 2025–2027 was adopted as set out in Annex 1 to that decision.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that may be made of the information contained in this publication.

Luxembourg: Publications Office of the European Union, 2026

COPYRIGHT NOTICE

English PDF Web TP-01-26-013-EN-N ISBN 978-92-9204-798-6 ISSN 2314-9434 DOI 10.2824/6318192

2025 Consolidated Annual Activity Report

ABOUT ENISA

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

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

FOREWORD

by the Executive Director

June 2026

The 2025 Annual Activity Report of the European Union Agency for Cybersecurity (ENISA) sets out the achievements and progress in delivering the Agency's 2025 work programme and strategy reflecting the dedication, excellence and strong collaboration required to achieve a high common level of cybersecurity across the Union.

Throughout the year ENISA remained committed to its revised strategy focused on vertical and horizontal objectives to enhance cooperation and anticipate threats. The Management Board adopted key governance documents that reinforced ENISA's commitment to strengthening its collaboration with stakeholders with a revised international strategy and new stakeholder strategy.

Key achievements were the implementation of the European Vulnerability Database - a requirement from the NIS2 Directive - an essential tool designed to substantially improve the management of vulnerabilities and the risks associated with it. Additionally, the Agency became a Common Vulnerabilities and Exposures (CVE) Program-Root thus taking a step to further improve the development and capacity of the Agency to support vulnerability management in the EU. Moreover, the contribution agreement signed with the European Commission through which ENISA is entrusted with the administration and operation of the EU Cybersecurity Reserve allowed ENISA to build on the years of extensive experience managing the ENISA Cybersecurity Support Action successfully.

ENISA continued its support to Member States by responding to individual requests and thereby contributing to the transposition of the NIS 2 Directive towards completion. At the same time, the agency supported the NIS sectors through the establishment of sectoral communities, notably by coordinating working groups bringing together national authorities to foster cooperation, knowledge sharing, in the pursuit of raising the maturity of NIS sectors and ENISA played a pivotal role in delivering the ICT supply chain toolbox, establishing a methodology and a roadmap for conducting EU-level risk evaluations.

In terms of skills development the agency made significant strides in narrowing the skills gap by improving the skills of over 75 000 professionals in through dedicated cyber exercises, challenges and awareness-raising actions.

The role of chair of the EU Agencies Network (EUAN) gave ENISA the opportunity to support the 52 EU Agencies and Joint Undertakings by prioritising and strengthening cybersecurity across the Network and to extend cooperation with the sharing of services among its members, to best serve the interests of EU citizens.

I would like to extend my gratitude to all statutory and non-statutory experts, partners, and especially ENISA staff and the Management Board members for their steadfast support towards a trusted and cyber secure Europe.

Juhan Lepassaar
Executive Director

ENISA MANAGEMENT BOARD ASSESSMENT

The Management Board (MB) congratulates the European Union Agency for Cybersecurity (ENISA) for its performance in 2025 and for its commitment to the EU and the EU Member States in their pursuit of a high common level of cybersecurity across Europe. The agency is widely recognised as a leader in cybersecurity that is relied upon by its peers and the wider industry for setting and steering direction; therefore, it is paramount that ENISA stay ahead of emerging trends and remain committed to pursuing excellence at both the operational and corporate levels. Finally, the MB commends ENISA for initiating its cybersecurity maturity plan and on its updated international and stakeholder strategies that were adopted in 2025, which will guide its engagement with stakeholders over the coming years.

Please find below the MB assessment of the 2025 annual activity report (AAR).

1. The MB congratulates ENISA on its support to Member States' cybersecurity policy implementation through the update of the national capabilities assessment framework. By updating the framework to align with the requirements of the NIS 2 Directive, the agency has contributed to harmonising the implementation of national cybersecurity strategies across the EU. The MB looks forward to the agency integrating the framework with the Cybersecurity Index and peer reviews, as the framework's greatest value lies in providing improvement-oriented guidance to support the development and refinement of national cybersecurity strategies.
2. The MB acknowledges the increase in the number of mature network and information security sectors and the support ENISA provides to sectoral communities. The agency's stakeholder engagement efforts via numerous events are much appreciated.
3. The MB commends ENISA on the support of the NIS Cooperation Group in publishing the ICT supply chain toolbox which will lead to the first Union risk assessment roadmap.
4. The MB commends ENISA on the added value it has brought to capacity-building communities through coordination with and support for the European Cybersecurity Competence Centre. The MB also congratulates the agency on its efforts to narrow the skills gap by improving the skills of over 75 000 professionals in 2025 through dedicated cyber exercises, challenges and awareness-raising actions. In addition, the MB congratulates the agency on its execution of BlueOLEx, as it encourages coordinated efforts to maintain a high level of crisis preparedness and capabilities among Member States.
5. The MB recognises ENISA's effort to seek alignment between operational communities and acknowledges that specialised expertise with an operational link to Member States is required to reinforce the agency. In this regard, the MB also acknowledges the agency's efforts to improve stakeholder management by introducing priority-setting through the introduction of a stakeholder strategy that prioritizes cooperation with EU Member States and EUIBAS among its 6 stakeholder groups.

6. In support of its stakeholder strategy, the agency updated its international strategy that gives direction to agency's cooperation with international stakeholders, both of which were adopted by the MB. The MB recommends that ENISA leverage existing systems and frameworks for engaging with stakeholders going forward.

7. The MB concurs with ENISA's proposal to consolidate corporate and operational information technology into a single activity under the guidance of a chief information and technology officer from 2027 onwards.

8. The MB commends the agency on becoming a common vulnerabilities and exposures program root and operationalising the EU Vulnerability Database, as provided for in the NIS 2 Directive, thus enhancing the EU's ability to manage and coordinate cybersecurity vulnerabilities, and reinforcing Europe's security and resilience and it calls the agency to intensify its efforts in relation to its tasks under Cyber Resilience Act (CRA), notably on open-source software.

9. The MB congratulates the agency on the increase in cooperation with Member States on situational awareness and threat analysis. Without the support of Member States in this endeavour, there would be no common situational awareness.

10. The MB acknowledges the efforts made by the agency regarding preparing for the Cyber Resilience Act (CRA) Single Reporting Platform and looks forward to its launch before 11 September 2026.

11. The MB congratulates the agency on its transition from the support action programme to the operational model of the EU Cybersecurity Reserve, including the streamlining of its services catalogue to better reflect Member States' demand for services as demonstrated by the significant number of services delivered in 2025.

12. The MB recognises the work undertaken by ENISA in certification, such as the agency's support for the drafting of the candidate scheme for the EU Digital Identity Wallet, the amendment of the act implementing the EU cybersecurity certification scheme on common criteria and its maintenance activities, and the finalisation of a candidate 5G network equipment security assurance certification scheme submitted to the European Commission.

13. The MB acknowledges the significance of the conformity assessment ecosystem in the success and uptake of both the European cybersecurity certification framework and CRA. The MB calls on ENISA, the European Commission and Member States to ensure these are implemented in a consistent and harmonised manner.

14. The MB congratulates ENISA on the support provided for the implementation of the CRA in the area of product security and the updated cybersecurity market analysis framework. The MB looks forward to the agency's support for Member States' CRA implementation.

15. The MB acknowledges the significance of strengthening the agency's cybersecurity stance in view of the new responsibilities entrusted to ENISA, and calls on the agency to prioritise the cybersecurity maturity plan for 2025–2028.

16. The MB congratulates the agency on its successful coordination of the EU Agencies Network as chair in 2025 and for the support provided to EU entities to improve their cybersecurity stance.

17. The MB commends the agency on its effective resource management, with 98 % of establishment plan posts implemented and an overall budget commitment rate of 99.96 %, which has improved over the past five years from 97.35 %.

18. The MB also acknowledges ENISA's excellent efforts to implement activities under various contribution agreements that amount to a total of EUR 28.1 million signed with the Directorate-General for Communications Networks, Content and Technology in 2025. The MB calls on the agency to ensure the efficient and effective execution of such funds according to the principles of sound financial management as laid out by the EU's financial regulations.

19. During 2025, ENISA committed a total of EUR 26 704 584, representing 99.96 % of the total budget for the year. Payments made during the year amounted to EUR 22 609 962, representing 84.64 % of the total budget. Overall payment execution improved slightly to 84.64 % (from 83.05 % in 2024). The target of a 95 % commitment rate set by the European Commission (specifically, the Directorate-General for Budget) was reached.

20. The agency cancelled a total of EUR 110 160, which represents 2.39 % of the total amount carried forward. Compared with 2024, there is an increase in payment execution for implementation of the C8 funds: 97.61 % in 2025 compared with 96.19 % in 2024. The MB calls on the agency to take measures to lower the amount of cancelled budget from the C8 budget carried forward.

21. The MB welcomes the 21 new staff members who joined the agency in 2025 and notes that the staff turnover increased slightly from 4.49 % in 2024 to 6.42 % in 2025. The MB calls on the agency to monitor turnover to ensure that it is lowered (below 5 %).

22. The 2025 AAR provides extensive information on the 2025 assessment of the internal control framework. Whereas improvements and further fine-tuning are needed in certain areas to increase effectiveness, the assessment confirmed that the internal controls at ENISA provide sufficient and reasonable assurance that the agency's policies, processes, tasks and behaviours, taken together, facilitate its effective and efficient operation, help ensure the quality of internal and external reporting, and help ensure compliance with its regulations. In particular, no critical risks and weaknesses were identified in 2025. Moreover, 21 non-compliant events (i.e. exceptions) were identified in 2025 through internal checks. Only four exceptions were deemed materially relevant, of which one was assessed as high risk. This exception is related to ENISA's participation (financially and physically) in a conference held in an Eastern neighbourhood country, for which an explicit financing decision is missing. This was an *ex ante* exception that was endorsed in order to support the security of the neighbouring country. Regarding the three other material risks identified and reported as exceptions to ENISA's legal frameworks, two relate to the erroneous use of budget carried forward from 2024 to 2025, and one relates to an ineligible cost reimbursement, which was granted in an exceptional context. Based on the above, the MB concludes that necessary actions were undertaken in 2025 to ensure the overall efficiency of the internal controls at the agency in order to comply with ENISA's legal and regulatory framework. The MB further congratulates ENISA for all its efforts engaged to this end.

23. The annexes complete the AAR with the Executive Director's declaration of assurance as well as additional information on human and financial resources, draft annual accounts and financial reports, and performance information. Overall, the MB takes note of ENISA's successful achievements in 2025.

24. The MB expresses its deep appreciation to the staff of ENISA and to the Executive Director for their commitment and excellent overall performance throughout the year. In light of the above assessment, the MB requests the MB Secretariat to forward the AAR, together with this assessment, to the European Parliament, the Council of the European Union, the European Commission, the European Court of Auditors and the permanent representations of the Member States.

EXECUTIVE SUMMARY

Implementation of the agency's annual work programme and highlights of the year

In 2025, the European Union Agency for Cybersecurity (ENISA) continued actively supporting EU Member States and EU institutions, bodies, offices and agencies in improving cybersecurity for the purpose of achieving a high common level of cybersecurity across the EU.

The agency was able to efficiently and effectively deliver the objectives set out in its annual work programme. The 2025 annual work programme, published in the 2025–2027 ENISA single programming document, was drawn up and aligned with ENISA's revised strategy.

Presented below are highlights of the year's key achievements.

The agency stepped up its operational cooperation efforts with a number of important milestones, such as becoming a central point of contact within the common vulnerabilities and exposures programme for national and EU authorities, EU computer security incident response teams network members and cooperative partners. ENISA's new role is part of the EU investment in strengthening vulnerability coordination and management in the EU.

In addition, ENISA launched the European Vulnerability Database as provided for by the NIS 2 Directive. The database provides aggregated, reliable and actionable information, such as mitigation measures and exploitation status, on cybersecurity vulnerabilities affecting information and communication technology products and services.

The EU blueprint for cybersecurity crisis management was adopted in 2025, providing guidelines for Member States to enhance their preparedness, detection capabilities and response to cybersecurity incidents.

In 2025, ENISA initiated the development of a candidate certification scheme for managed security services after a request from the European Commission. Certifying managed security services is essential to ensure a certain level of quality and security of services offered in the single market. Taking this step will not only foster confidence and trust within the EU but also significantly facilitate the selection of trusted providers for the EU Cybersecurity Reserve.

A contribution agreement was signed between ENISA and the European Commission in 2025 for the administration and operation of the EU Cybersecurity Reserve as provided for in Article 14 of the Cyber Solidarity Act. Procured by ENISA, services offered will be contracted from trusted managed service providers. The services are intended for users representing critical sectors in Member States, as described in the NIS 2 Directive, as well as EU institutions, bodies, offices and agencies.

The agency made some significant strides in its stakeholder engagement practices in 2025, with the introduction of a new stakeholder strategy, a revised international strategy and the formation of a new advisory group.

The new stakeholder strategy sets out ENISA's approach to identifying and engaging stakeholders in a value-driven, coordinated and transparent way.

The revised international strategy strengthened the agency's alignment with the EU's international cybersecurity policies and the promotion of EU values. The new advisory group was set up to support the agency's strategic objectives for a term of 2.5 years, ending 31 July 2028.

The agency led inter-agency cooperation as Chair of the EU Agencies Network in 2025. ENISA pursued key priorities in implementing the network's new governance framework, asserting the role of agencies as key institutional partners. It also strengthened cybersecurity within EU agencies and joint undertakings, leading to greater efficiency through sharing services.

2025 was the first year of implementation of the revised ENISA strategy and organisational structure. The organisation was restructured as of January 2025 to support the revised ENISA strategy and the implementation of not only the Cybersecurity Act but also other key legislation, including the NIS 2 Directive, the Cyber Resilience Act and the Cyber Solidarity Act.

I

PART I

ACHIEVEMENTS OF THE YEAR

The following sections of the annual activity report (AAR) are based on the structure of the 2025–2027 European Union Agency for Cybersecurity (ENISA) single programming document (SPD). The achievements of each activity are described, including details of the outcome of each output undertaken during 2025.

ACTIVITY 1:

Support for policy monitoring and development

Activity 1 was reorganised as part of the restructuring of the agency in 2025, focusing on supporting the EU Member States to better understand the challenges of policy implementation. Activity 1 provided technical, fact-driven and tailored recommendations in support of challenges stemming from policy initiatives. The activity was structured into three pillars: (a) building a comprehensive knowledge base on the status of cybersecurity in Member States through the systematic collection of relevant information, (b) analysis through dedicated tools and methodologies and (c) technical advice feeding back to the ENISA SPD and Member States. The results of the data analysis feeds into the work priorities of other ENISA activities – namely Activities 2, 3, 4 and 5 – based on the Member States' needs. Thus Activity 1 contributed to fulfilling the strategic objectives of supporting effective and consistent implementation of EU cybersecurity policies and consolidating and sharing cybersecurity information and knowledge support for Europe. For 2025, the focus was actioning the NIS 2 Directive and to achieve this numerous projects were implemented.

Outlined below are the key accomplishments of the activity in 2025.

- Updated the national capabilities assessment framework (NCAF). ENISA significantly strengthened support to Member States' cybersecurity policy implementation through the update of the NCAF to align with the requirements of the NIS 2 Directive. The revised framework was piloted by four Member States, where the framework served as input for the revision of their national cybersecurity strategies. The framework has been also used as a basis for the peer review process outlined in Article 19 of the NIS 2 Directive, which is a mechanism that allows three (or more) Member States to learn from shared experiences, strengthening mutual trust and enhancing cybersecurity capabilities. Specifically, ENISA has supported the first pilot peer review and used the NCAF as a common basis to describe cybersecurity capabilities. Together with enhancements to the interactive map of national cybersecurity strategies, these activities improved transparency, supported evidence-based policy development and contributed to greater alignment in the implementation of national cybersecurity strategies across the EU.
- Revised the EU cybersecurity index (EU-CSI) framework. ENISA revised the EU-CSI framework in view of the 2026 cycle and successfully collected data from all the Member States, preparing the ground for the 2026 EU-CSI results and the 2026 *State of Cybersecurity in the Union* report, which will give valuable input to the Member States and the EU stakeholders. This was achieved thanks to close cooperation with and the engagement of the national liaison officer (NLO) subgroup for the EU-CSI, including three Member States volunteering to be part of a task force that discussed in depth the details of the revised framework.
- Supported the effective implementation of the NIS 2 Directive. ENISA held structured interviews with representatives from all the Member States through the NLOs. The interviews involved nearly 100 national experts in identifying common challenges, priorities and support needs across key

cybersecurity policy and operational areas covering 26 Member States. The key priorities identified were supervision, incident reporting, capacity building and security measures. By systematically analysing and consolidating this input, ENISA provided a clear, evidence-based picture of shared implementation challenges, informing the 2026–2028 Network and Information Security Cooperation Group (NIS CG) work programme and helping to shape ENISA's strategic priorities and actions for the coming years. The data collected were extensively discussed in the joint MB–NLO meeting and are utilised as the basis for priority setting within ENISA's 2026–2027 work, supporting Member States in implementing the NIS 2 Directive and the priorities of the NIS CG work programme.

The work undertaken as part of this activity received positive feedback and recognition from beyond the EU. For example, the NCAF is referred to as a useful tool in the International Communications Union's *Guide to Developing a National Cybersecurity Strategy*.

Presented below are the key lessons identified during 2025 that will guide future implementation.

- The activity's key performance indicators (KPIs) in the forthcoming SPD will need to be revised to reflect the activity's outcomes, such as the publication of the first *State of Cybersecurity in the Union* report (Article 18 of the NIS 2 Directive), and ensure that the KPIs are able to measure the take-up of the recommendations.
- In the area of peer reviews, the most effective outcomes were observed when the process was clearly positioned as a collaborative exercise centred on mutual learning and the exchange of good practices rather than on formal evaluation. Consolidating this approach can further strengthen trust, openness and practical knowledge sharing among participants.
- Integrating the NCAF in the EU-CSI and the peer reviews should be prioritised, as its greatest value lies in providing improvement-oriented guidance to support the development and refinement of national cybersecurity strategies.
- Regarding the EU-CSI, 2025 was characterised by stronger Member State involvement through the establishment of the abovementioned task force. The experience was extremely positive and led to a solid and shared 2026 EU-CSI framework. This practice should be continued for the next iterations of the EU-CSI. In addition, ENISA recorded positive feedback about the proposal to facilitate the exchange of good practices for analysing the results of the index, thus allowing Member States to process and utilise index-related information more efficiently.
- The consultation with Member States and the open bilateral dialogues with national experts – conducted by ENISA for the first time in 2025 – provided a solid, evidence-based understanding of the challenges of and support needs for implementing the NIS 2 Directive, enabling more targeted prioritisation of activities. Building on these lessons, ENISA will continue and further systematise the dialogue going forward, with focused thematic deep dives into the most challenging areas to ensure stronger follow-up and more tailored support.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Effective and consistent implementation of EU policies for cybersecurity • Foresight on emerging and future cybersecurity opportunities and challenges	• Uptake of recommendations stemming from NIS2 Article 18 report • Number of identified future and emerging areas reflected in the policy initiatives and intervention

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET
1A. By the end 2026, implement a policy monitoring and analysis framework that delivers ad hoc as well as relevant and regular support and assistance to national and EU cybersecurity policymakers.	CSA, Articles 5 and 9	2026	Assessment of ENISA advice on EU policy (stakeholder survey, desktop research).	75 % stakeholder satisfaction with ENISA's advice among EU policymakers. By the end of 2025, the policy analysis framework was endorsed.
1B. By Q3 2026 and in collaboration with Activity 2, ensure that two thirds of policy observations within the first *State of Cybersecurity in the Union* report have been realised.	NIS 2 Directive, Article 18	2026	Assessment of the Member States' use of the *State of Cybersecurity in the Union* (Article 18) report (stakeholder survey, desktop research).	Two thirds of Member States use the *State of Cybersecurity in the Union* (Article 18) report as input for their cybersecurity strategies. All Member States use ENISA support and tools for the work on their network and information security (NIS) strategies.

OUTPUTS	OUTCOME
1.1. Assist Member States to implement, assess and review their national cybersecurity strategies and policies. Enhance a culture of trust and cooperation among Member States through peer reviews and by developing a code of conduct.	**In 2025, ENISA achieved the following.** • Coordinated activities as secretariat of the NIS CG workstream 9, ensuring a smooth transition from having two groups of Member States working on strategies (the NLO subgroup on national cybersecurity strategies and the workstream 9 group on national cybersecurity strategies and peer reviews) into a single group (i.e. the NIS CG workstream 9). In parallel, the scope and priorities of workstream 9 were further structured, including the development of a new work plan and the definition of the terms of reference. • Developed documentation to support the first pilot peer review under Article 19 of the NIS 2 Directive, including the identifying peer reviewers and cybersecurity experts, with a defined code of conduct, the planning and execution framework for peer reviews, the establishment of evaluation metrics and the creation of a peer review reporting template. In addition to this documentation, further deliverables included supporting the participants in the planning and execution of the pilot peer review and assisting in drafting the final report. • Updated the NCAF to reflect the requirements of the NIS 2 Directive and to serve as a structured basis for the implementation, assessment and review of national cybersecurity strategies and policies. The framework also provided the foundation for the peer reviews. • Assisted four Member States in the revision of their national security strategies. The Member States used the draft revised NCAF as a source of actionable information for the assessment and review of their strategies, while generating feedback to further refine the framework. These assessments were conducted through three complementary approaches: self-assessment by Member States, assessments delivered as a service by ENISA and the use of the framework as guidance for improvements in the drafting of the next generation of national cybersecurity strategies. • In parallel, ENISA updated and enhanced the national cybersecurity strategies interactive map, which provides a comprehensive overview of all the national cybersecurity strategies across the EU, including their strategic objectives, implementation measures and good practices. The map highlights how Member States translate policy into action through national implementation efforts and the work of national cybersecurity stakeholders, such as competent authorities, computer security incident response team (CSIRTs) and other coordinating bodies. Through these activities, ENISA continues to develop a central information hub that showcases Member States' progress in strengthening national cybersecurity, while fostering transparency, knowledge sharing and alignment with EU cybersecurity legislation. The link to the map is **here**.

1.2. Collect and present relevant evidence by maintaining and developing the EU-CSI and *State of Cybersecurity in the Union* report.	**In 2025, ENISA achieved the following.** • In collaboration with a task force assembled from three Member States and part of the EU-CSI NLO subgroup, the agency maintained and revised the EU-CSI. This resulted in an updated 2026 EU-CSI framework, which will also be used for the upcoming 2026 *State of Cybersecurity in the Union*. The framework was endorsed by all relevant Member States groups (NLOs, CSIRTs network (CNW) and the NIS CG). • Kicked off the 2026 EU-CSI cycle: following the 2026 EU-CSI methodology, ENISA collected the information needed from all Member States, in collaboration with the EU-CSI NLO subgroup, through the EU-CSI Member State survey and external sources. • Prepared for the 2026 *State of Cybersecurity in the Union* by conducting a preliminary analysis of the potential content and the set-up of an internal network within ENISA.
1.3. In coordination with Activities 2, 4 and 8, develop and maintain analyses on time-sensitive observations offering technical advice for policy development.	**In 2025, ENISA achieved the following.** • Launched a consultation process with all Member States, in collaboration with the National Liaison Officers (NLOs), to identify challenges and needs related to the implementation of the NIS 2 Directive, a cornerstone of EU cybersecurity legislation. The exercise covered a broad range of topics, including supervision, scope, security measures, operational cooperation, incident response, cyber crisis management, information sharing, incident reporting, coordinated vulnerability disclosure, certification and capacity building. • Engaged 97 national experts from 26 Member States in this process. Evidence was gathered through a dedicated survey, bilateral expert-level dialogue and discussions with Member States during several meetings held in October, November and December 2025. The findings were presented to the CNW, the European cyber crisis liaison organisation network (EU-CyCLONe) and the NIS CG, with several needs reflected in the NIS CG's 2026–2028 work programme. • Analysed and aggregated input to identify recurring themes and shared challenges across policy areas, focusing on common patterns rather than individual national positions. While national approaches to transposition and governance differ, Member States reported largely similar implementation challenges. Mapping this shared landscape enables targeted EU-level support where it can have the greatest impact. • Shared the results with ENISA's Management Board (MB) and the NLOs, which informed discussions in early 2026 and shape the agency's priority areas and key actions for the coming years.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
1.1	Stakeholders receive technical advice with the evidence needed for policymaking activities and the definition of implementation measures.	EU institutions (European Commission, European Parliament, Council of the European Union) NIS CG, including relevant workstreams NLOs, including relevant subgroups	Develop and pilot a peer review framework, including a code of conduct.	Biennial survey, annual dialogue and annual desktop research	By the end of 2025, both endorsed.	ENISA developed all peer review documentation and guidance, including the code of conduct, and all were endorsed by workstream 9.
1.2			Assessment of ENISA advice on EU policy.		> 90 % stakeholder satisfaction	Survey planned for 2026.
1.3			Assessment of timeliness of advice provided during policy development.		> 70 % stakeholder satisfaction with timeliness	100 % – fully achieved, as all Member States and the various EU networks have agreed with the consolidated findings. ENISA has also reviewed and validated them as part of its activities.

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. EU institutions, including the European Parliament's Committee on Industry, Research and Energy; directorates-general such as the Directorate-General for Communications Networks, Content and Technology; the Horizontal Working Party on Cyber Issues (HWPCI); Member States' cybersecurity authorities; the NIS CG and relevant workstreams, ENISA NLOs and subgroups.

Involve/engage. Those directly impacted by the NIS 2 Directive and industry associations/representatives.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	9	**NUMBER OF FTES ACTUALLY USED [1]**	5.1
PLANNED BUDGET (EUR)	306 136.50	**BUDGET CONSUMED (EUR)**	341 665.45
AMENDED BUDGET (EUR)	345 079.20	**OF WHICH CARRIED OVER TO 2026 (EUR)**	91 129.10

[1] FTEs available for the activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

ACTIVITY 2

Cybersecurity and the resilience of critical sectors

Activity 2 supported Member States' implementation of the EU cybersecurity policy to enhance the cybersecurity and resilience of critical sectors across the EU. In particular, Activity 2 supported the implementation of the NIS 2 Directive, but it also aimed to support sectoral legislation, such as the Digital Operational Resilience Act (DORA) (*lex specialis*), and sectoral rules like the Network Code on Cybersecurity for Cross-border Electricity Flows. The activity contributed to the fulfilment of the strategic objectives of providing 'support for effective and consistent implementation of EU cybersecurity policies' and fostering 'empowered 'communities in an involved and engaged cyber ecosystem'.

Outlined below are the key accomplishments of the activity in 2025.

- Increased the number of NIS sectors with high maturity. An important KPI for this activity is the number of sectors with high maturity (currently there are six such sectors) based on the *NIS360* report. ENISA assesses maturity to have increased in the rail and health sectors, particularly in the area of information sharing and collaboration (this will be visible in the next edition of the *NIS360*).

- Supported NIS sectors by building sectoral communities, through coordinating working groups of national authorities and engaging with sectoral EU information-sharing and analysis centres (ISACs). ENISA also organised four large conferences to facilitate public–private dialogue: the ENISA Telecom Security Forum in Amsterdam, the Health Cybersecurity Conference in Bucharest, the Rail Conference in Tallinn and the Energy Forum in Brussels. The satisfaction rating among participants was on average 85 %. The annual EU ISACs Summit was also organised to connect and promote the EU ISACs.

- Published the *NIS360* report for the first time. It assesses the cybersecurity maturity and criticality of 22 NIS 2 (sub)sectors. The *NIS360* serves as reference for policymakers at both the EU and national levels. The European Commission, for example, referenced *NIS360* data in the health action plan. ENISA also published the sixth edition of the *NIS Investments* report, which surveys and analyses cybersecurity investments by companies across the EU. Both the *NIS360* and *NIS Investments* provide crucial sector data for the EU-CSI, which is the basis for the biennial *State of Cybersecurity in the Union* report (next edition due in 2026, as part of Activity 1).

- Brought the transposition of the NIS 2 Directive closer to completion. In the last few years, the NIS 2 Directive has developed into the main cybersecurity framework in Europe. At the time of writing, 18 Member States had notified of full or partial transposition, and transposition is

ongoing in the others. The ambitious deadline of October 2024 was too soon for many Member States, as the NIS 2 Directive is extremely broad, covering 19 different critical sectors. In many Member States, new authorities were needed and competences were reallocated. In almost every sector, there have been issues with scope and the registration of entities.

- Developed a better understanding of NIS 2 Directive implementation challenges. An element missing in supporting Member States implementing cybersecurity regulation was the actual gap in implementation. The Member States' dialogues from Activity 1 shed light on this, offering better structure, Member State endorsement and support, and internal coordination.

- Delivered the NIS 2 security measures framework, by means of a detailed technical guideline for NIS 2 security measures for the digital infrastructure sector, working with the Member States and the European Commission. This technical guideline complements Commission Implementing Regulation (EU) 2024/2690 (the NIS 2 Implementation Regulation) and supports both national authorities and companies in this sector. This guideline was the second most-downloaded deliverable on ENISA's website.

- Published the *Handbook for Cyber Stress Tests*. It was used by the Commission, which made conducting cyber stress tests the main recommendation for Member States in its cable security risk assessment report. ENISA also developed detailed stress test scenarios for coordinated preparedness testing under the Cyber Solidarity Act (CSOA), steering last year's EUR 10 million digital Europe programme (DEP) funding towards ransomware for the health sector and cyber-physical systems for the telecom sector. In addition, ENISA supported several EU risk assessments and helped the Commission update the methodology and draft an EU risk assessments roadmap. The information and communications technology (ICT) supply chain toolbox was published, as were the connected and automated vehicles risk assessment and the detection equipment risk assessment. The proposal for the revised CSA formalises the process further, and therefore this area is expected to grow in political importance.

Presented below are the key lessons identified during 2025.

- There are challenges in implementation and prioritisation. Overall, the national dialogues from Activity 1 revealed valuable insights that will assist in focusing activities on the Member States' needs. The priority areas are supervision, incident reporting, security measures and capacity building, and coordinated efforts are planned to support the Member States. Activity 2 created strong collaborative bonds with Activity 5 regarding incident reporting.

- Scaling-up and efficiencies are required. Overall, there is a need to find a balance between sectoral and horizontal actions. Mature sectors require intense support to navigate sector-specific legislation, which overlaps with general cybersecurity legislation. The most mature entities (in the scope of the NIS 2 Directive) are often also the most critical, and they need specific support. ENISA will focus on reusing the horizontal frameworks (as per the priorities identified), which were developed for the mature sectors, and sharing useful guidance and good practices.

- Looking forward, to improve alignment across regulatory requirements and national implementation across sectors, the activity and Member States would benefit greatly from the expertise of the other Member States regarding such undertakings.

- The current KPIs do not correspond to ENISA's work. Overall, the KPIs in relation to the maturity of the sectors should be further refined to reflect the value of ENISA's work. They should also go into deeper detail to precisely measure the efficiency of the current activities in increasing the sectors' posture.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Effective and consistent implementation of EU policies for cybersecurity	• Uptake of ENISA recommendations to support Member States and stakeholders in implementing EU legislation

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET	2025 RESULTS
2A. By 2026 conduct a pilot, and by the end of 2027 implement common frameworks and joint tools for the implementation of the NIS 2 Directive in the areas of (a) risk management, (b) security measures and (c) incident reporting for all EU sectors, and in line with industry best practices and international standards.	CSA, Articles 5 and 6; NIS 2 Directive	Develop frameworks in 2025	Frameworks' development.	2 frameworks developed.	2 NIS 2 frameworks initiated (security measures finalised and adopted, incident reporting in process).
		Pilot frameworks in 2026	Implementation of pilot programme (number of sectors piloting the frameworks, feedback scores on usability).	20 Member States to adopt/ use/endorse the frameworks.	NIS security measures guidance document is utilised or referenced by all Member States.
		Full implementation in 2027		> 75 % usability score.	Results expected as from 2027
2B. Provide continuous comprehensive support to Member States for implementing the EU's regulatory requirements on cybersecurity and raising resilience across critical sectors.	CSA, Articles 5 and 6; NIS 2 Directive	2027	Requests received by the NIS CG or Member States or other community groups.	> 80 % of requests received resolved for a maximum of 20 requests.	Results expected as from 2027
				> 75 % satisfaction with ENISA support over the relevant period.	Results expected as from 2027
2C. By the end of 2027, help to increase the overall maturity level of critical sectors under the NIS 2 Directive.	CSA, Article 5	2027	Assessment of maturity based on updated *NIS360* methodology.	> 2 sectors improving in maturity.	8 sectors recorded improvements in maturity (3 advancing to the next band; 5 evolving within their existing band).

OUTPUTS	OUTCOME
2.1. Support Member States in their implementation of the NIS 2 Directive.	**In 2025, ENISA achieved the following.** • Supported the NIS CG, coordinated three sectoral and seven industry-wide workstreams and supported four additional strategic workstreams, including those pertaining to 5G, ICT supply chain security, elections and EU-coordinated risk assessments. • Supported Member States in the transposition of the NIS 2 Directive. ENISA organised NIS101 risk management training for NIS authorities, consisting of a half-day knowledge-sharing workshop with scenario-based discussions led by health-sector NIS authorities. • Handled 14 individual requests from Member States for advice on NIS 2 transposition.

	• Published the Technical Implementation Guidance on NIS 2 security measures, which helps NIS entities implement cybersecurity requirements in a practical and consistent manner by translating regulatory obligations into concrete, actionable technical controls (available at https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance). • Mapped the NIS 2 implementing guidance to international standards and national frameworks with the aim of aligning the requirements of the NIS 2 Directive with existing frameworks to support consistent, interoperable and efficient implementation across organisations and Member States. • Produced guidelines on common notification templates adopted by the NIS CG. The document contributes to the simplification and streamlining of the information reported as per the NIS 2 Directive. • Further developed the EU Digital Infrastructure Registry (EUDIR), building on the first version, which was published last year. Following the development of a pilot version, ENISA began populating the registry this year with EU cross-border entities. Some 1 044 entities have been registered to date (see https://eudir.enisa.europa.eu/).
2.2. Support Member States with EU toolboxes, EU-coordinated risk evaluations and EU-coordinated preparedness tests.	**In 2025, ENISA achieved the following.** • Delivered the ICT supply chain toolbox. The toolbox development was heavily supported by ENISA, in collaboration with all relevant stakeholders, empowering the NIS CG to establish a methodology and a roadmap for conducting EU-level risk evaluations. ENISA, with the European Commission, delivered a mature draft in July 2025, and then addressed comments from Member States in the second half of 2025, ahead of formal adoption and publication in Q4 2025. The toolbox features 11 supply chain risk scenarios and practical recommendations for Member States. • Supported the EU risk assessments process. The NIS CG workstream on risk assessments and risk scenarios delivered two EU risk assessments – one on connected and automated vehicles and another on detection equipment (with the Directorate-General for Taxation and Customs Union). Following the framework set out by the ICT supply chain toolbox, the workstream group worked on a methodology and a roadmap for the upcoming risk assessments in areas of particular concern for the EU's security and sovereignty. This work is expected to gain further pace in 2026, continuing to be heavily supported by ENISA. • Supported the follow-up to the Council of the European Union's conclusions on the EU's cyber risk. As part of the preparedness actions set forth by the CSOA, the first set of highly critical sectors for coordinated preparedness testing was identified and agreed within the NIS CG, namely the health sector (in particular hospitals) and the digital infrastructure sector, including fixed networks and submarine cable infrastructure. ENISA drafted the risk scenarios, validated them with the relevant stakeholders (e.g. the sectoral NIS CG workstream) and delivered the risk scenarios in May 2025. • Published the first *Handbook for Cyber Stress Tests*, which became a central recommendation for Member States in the subsea cable expert group and European Commission report *Security and Resilience of EU Submarine Cable Infrastructures – Mapping risk assessment*, stress tests (October 2025). As a practical follow-up to the handbook, ENISA started to prepare the ground for a stress test in the gas sector to be held in 2026. • Leveraged its sectoral situational awareness capabilities by delivering 12 situational awareness bimonthly reports to 4 sectors, and 10 online/physical presentations to its constituency. This ENISA product is estimated to reach over 950 recipients.

2.3. Improve cybersecurity and resilience in the NIS sectors.

In 2025, ENISA supported the NIS sectors through its catalogue of services, focusing efforts in three areas: community building, policy alignment and maturity building. In specific NIS sectors, ENISA achieved the following.

- **Health**. It continued growing the community through flagship events, such as the eHealth Conference, and supporting the NIS CG health workstream and the EU Health ISAC. The agency actively engaged with different directorates-general in the Commission, providing technical advice on health-related legislative acts, such as the Medical Devices Regulation and the European Health Data Space. To ensure alignment with the NIS 2 Directive, a mapping of the policy and regulatory framework in health was developed (looking at the NIS 2 Directive, the Medical Device Regulation, the European Health Data Space Regulation, the General Data Protection Regulation, etc.). Maturity was also strengthened through workshops to build up the knowledge of national authorities on the NIS 2 Directive's provisions and by repeating the Cyber Europe exercise in several Member States. On top of all these, ENISA supported the implementation of the healthcare action plan.
- **Rail**. The conference for cybersecurity in the rail sector took place in Tallinn. In addition, to supporting community building, ENISA continued to engage with rail sector stakeholders. To ensure alignment with the NIS 2 Directive, the agency provided assistance to make sure sectoral standards match the NIS 2 Directive's requirements, including trainings being prepared by the support action programme for some Member States. To further build maturity, support for risk scenarios and the planning of 2026 Cyber Europe was provided.
- **Aviation**. ENISA contributed to a mapping document on aviation cybersecurity policy (that looked at the NIS 2 Directive, which provides clear, practical guidance to authorities on security measures, incident reporting and supervision, helping to simplify and align requirements. The document was well received by the NIS CG and national authorities and adopted by AVSEC in the fourth quarter (Q4) of 2025. Its impact is already visible, with Greece implementing the recommendations through single-incident reporting, joint audits and a common security framework.
- **Maritime**. ENISA conducted preparatory work in support of the EU port security strategy by providing cybersecurity expertise, delivered situational awareness updates for the maritime domain, maintained close collaboration with EMSA, and hosted a Maritime ISAC meeting in Athens.
- **Finance**. The agency continued strengthening cooperation with the three European supervisory authorities in the finance sector by implementing the annual action plan, including activities related to cross-border incidents, crisis management and oversight of critical ICT service providers. ENISA participates as an observer in the critical third-party providers designation, an exercise coordinated by the European supervisory authorities, and will perform the same role on joint examination teams when these have been finalised.
- **Digital infrastructure and telecoms**. ENISA organised the 2025 Telecom and Digital Infrastructure Security Forum, in which 180 people participated, alongside the digital infrastructure and digital providers workstream. The agency also led the task force on the definition of services under this workstream, developing guidelines for a harmonised definition of services for the entities in scope. In addition, ENISA led the NIS CG 5G workstream by analysing and presenting updates to the 5G toolbox regarding technical measures. Additionally, ENISA integrated the European Competent Authority for Secure Electronic Communications into the NIS CG 5G workstream, establishing it as a sub-workstream for technical topics, while enabling the 5G workstream to focus on strategic priorities.

	• **Energy**. ENISA organised the Cybersecurity Energy Forum, which involved 250 participants and high-level panellists, receiving positive feedback and media interest. The agency also led the NIS CG energy workstream, including an in-person meeting in Brussels with representatives from 16 Member States to advance energy stress tests in the gas sector. ENISA provided sustained contributions to network code and network code on cybersecurity benchmarking work, acknowledged by the European Union Agency for the Cooperation of Energy Regulators. • **Public administrations**. The efforts focused mainly on community building. ENISA elevated cybersecurity as a priority topic for local and regional governments through the Council of European Municipalities and Regions and the Major Cities network. In addition, an informal community of public administration authorities was created. In conjunction with Activity 5, ENISA published a sectoral version of the cybersecurity threat landscape. Through a series of workshops, the agency enabled the sharing of knowledge and best practices. The first workshop was organised to present the sectoral threat landscape.
2.4. Perform an annual check on policy implementation.	**In 2025, ENISA achieved the following.** • Published the outcomes of the *NIS360* assessment of sectoral cybersecurity maturity and criticality for the first time, presenting key insights stemming from the analysis of data gathered in the previous year from national authorities, sector entities and EU-level data sources. • Published the sixth edition of the annual *NIS Investments* study, presenting key insights stemming from the analysis of data gathered from organisations all operating within highly critical sectors impacted by the NIS 2 Directive. • Continued to expand the evidence base underpinning the *NIS360*. The expanded evidence base now integrates the outcomes of dedicated surveys of entities and national authorities, consultations with industry experts and internal sectoral expertise. The most recent edition of the *NIS360* report was published in Q1 2026. • Produced cyber risk position briefs for the health, rail and gas sectors (three in total). The agency built on its flagship studies NIS Investments, *NIS360* and *ENISA Threat Landscape*. Enriched with data from multiple sources, these briefs are aimed at providing a strategic 'at-a-glance' view of a sector's maturity, criticality, threat context, interdependencies and challenges.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
2.1. Support Member States in their implementation of the NIS 2 Directive.	The NIS 2 frameworks for risk management, security measures and incident reporting achieve harmonisation.	Directorate-General for Communications Networks, Content and Technology NIS CG	Framework usage.	Annual (internal count)	10 Member States to adopt, use or endorse the frameworks.	Parts of the 2 NIS 2 frameworks are adopted/ endorsed by the NIS CG.
			EUDIR used by all Member States.	Annual (report)	20 Member States to use EUDIR.	18 Member States use EUDIR.

			Alignment between DORA and the NIS 2 Directive.	Satisfaction survey	> 80 %	> 80 % of Member States say DORA is aligned with the NIS 2 Directive. 77 % of the finance sector use the NIS 2 Directive-implementation guidelines, which means better DORA–NIS 2 Directive alignment.
2.2. Support Member States with EU toolboxes, EU-coordinated risk evaluations and EU-coordinated preparedness tests.	Support is given to EU-wide risk evaluations and risk scenarios and their follow-up (5G, Nevers call). Coordinated risk assessment of critical supply chains is undertaken.	Directorate-General for Communications Networks, Content and Technology NIS CG	Risk assessment framework for critical supply chains.	Annual (internal count)	1 coordinated risk assessment per domain or sector.	2
			Number of sectoral situational awareness reports.	Annual (internal count)	12	12
2.3. Improve the cybersecurity and resilience of the NIS sectors.	Stakeholders use the NIS service packages to improve sectoral security and resilience.	Directorate-General for Communications Networks, Content and Technology NIS CG Sectoral EU ISACS Sectoral EU agencies	Number of critical sectors increasing in maturity (from build to sustain or involve – *NIS360*).	Annual (internal count)	5	8 sectors recorded improvements in maturity (3 advancing to the next band; 5 evolving within their existing band).
			Number and frequency of services or workflows delivered to NIS sectors according to the maturity of the sector.	Annual (internal count)	24	30 services were delivered to 10 NIS subsectors.

2.4. Perform an annual check on policy implementation.	Member States and EU institutions (both general and sectoral stakeholders) use the *NIS Investments*, the *NIS360* and the cyber posture briefs as reference documents for policymaking.	Directorate-General for Communications Networks, Content and Technology NIS CG Sectoral EU ISACS Sectoral EU agencies	Number of critical or essential sectors covered by *NIS Investments*.	Annual (internal count)	12 subsectors covered.	14 subsectors were covered (22 sectors and subsectors in total).
			Number of critical sectors assessed by the *NIS360* and cyber posture briefs.	Annual (internal count)	12	22 sectors and subsectors were covered by the *NIS360*; 3 sectors covered by cyber posture briefs.
			Implementation tracker.	Annual (internal count)	5 requests stemming from the implementation of the NIS 2 Directive in Member States.	N/A (initiative incorporated into 2026 NIS 2 hub).

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. The Directorate-General for Communications Networks, Content and Technology; NIS CG; national competent authorities; sectoral directorates-general; sectoral EU agencies; and sectoral ISACs.

Involve/engage. NLOs, essential and important entities in the scope of the NIS 2 Directive and industry associations/ representatives.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	11	**NUMBER OF FTES ACTUALLY USED** [2]	9.2
PLANNED BUDGET (EUR)	343 123.55	**BUDGET CONSUMED (EUR)**	448 010.58
AMENDED BUDGET (EUR)	448 010.58	**OF WHICH CARRIED OVER TO 2026 (EUR)**	59 404.21

[2] FTEs available for the activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

ACTIVITY 3

Capacity building

Activity 3 sought to improve the response capabilities and preparedness of Member States and EU institutions, bodies and agencies (EUIBAs), as well as organisations in the scope of the NIS 2 Directive. Furthermore, it also aimed at reducing the cyber skills gap in the EU by, among other things, maintaining the European cybersecurity skills framework (ECSF).

Outlined below are the key accomplishments of the activity in 2025.

- The ECSF was adopted by a further 4 Member States in 2025 to make a total of 18 (up from 14 in 2024), contributing to the harmonisation of cybersecurity skills across the EU. Additionally, the ECSF has been mapped to the NIS 2 Directive's provisions. A pilot with eight Member States was conducted on a European attestation scheme for skills required by the incident response profile.

- More than 9 cyber exercises were delivered, 2 of them replaying existing Cyber Europe scenarios, involving more than 1 000 players directly and more than 9 000 experts indirectly. The agency's exercise methodology[3] was published and now acts as a first step to empower stakeholders running their own exercises using ENISA's tools and methodologies.

- ENISA's AR[4] in a box has impacted more than 26 000 professionals and 16 Member States through train-the-trainer programmes and/or 4 online platforms.

- More than 34 countries and 40 000 people (students and young professionals) took part in national and European challenges, demonstrating 290 % growth. Around 40 % of participants find very well-paid jobs in the sector and thus narrow the skills gap in the EU. Team Europe won every category at the International Cybersecurity Challenge (ICC), Europe's fourth consecutive win.

- ENISA and the European Cybersecurity Competence Centre (ECCC) signed a cooperation agreement to support European and international challenges, ensuring the business continuity of an activity that significantly reduces the skills gap in Europe and demonstrates EU excellence to the world.

Presented below are key lessons identified during 2025 and possible recommendations that will guide future implementation.

(3) https://www.enisa.europa.eu/publications/the-enisa-cybersecurity-exercise-methodology.
(4) Awareness raising.

- The agency is pivoting to a targeted number of exercises going forward, thus developing an annual programme of EU-level high-impact cybersecurity exercises. Member States will have the full suite of ENISA's tools and methodologies available to organise capacity-building programmes with ENISA's support. In addition, funding mechanisms are also available to Member States via the ECCC, the Cyber Reserve and other cooperation agreements.
- ENISA will continue to update the ECSF to be in sync with recent technological (e.g. AI) and policy developments (e.g. the Cyber Resilience Act (CRA)) and use it as basis for developing attestation schemes for specific profiles, as demonstrated by ENISA's pilot study.
- ENISA will expand its strategic cooperation with the ECCC to cover capacity-building areas (e.g. AR in a box, the ECSF, exercises). ENISA will also assist Member States to further improve their response capabilities and preparedness, and expand the scope of the NLO subgroup on exercise to also cover skills, awareness and challenges.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Strong cybersecurity capacity within the EU	• Rate of satisfaction with ENISA's capacity building activities (e.g. exercises, training sessions) • Percentage of Member States that use the ECSF

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET
3A. Maintain and regularly update the ECSF.	EU Communication on the Cybersecurity Skills Academy, CSA Articles 6 and 10	2027	Number of Member States endorsing the updated ECSF framework.	23
			Stakeholder satisfaction rate.	95 %
3B. Between 2025 and 2027, enhance the cybersecurity skills and capabilities of at least 100 000 professionals in the EU.	CSA, Articles 4, 6, 7(5) and 10 CRA, Article 10 REU[5], Article 10	2027	Number of professionals whose skills have been directly or indirectly improved by capacity building activities.	100 000 professionals
			Satisfaction survey of stakeholders on ENISA's capacity-building activities.	70 %
3C. Between 2025 and 2027, ensure that ENISA has put in place frameworks to support the development of at least 100 000 additional cybersecurity professionals in the EU.	CSA, Articles 4, 6, 7(5) and 10 CRA, Article 10 REU, Article 10	2027	Stakeholder satisfaction survey on new frameworks put in place.	75 %

[5] REGULATION (EU, Euratom) 2023/2841 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

OUTPUTS	OUTCOME
3.1. Support the adoption and uptake of the ECSF.	**In 2025, ENISA achieved the following.** • **Reported on the NIS 2 Directive and the ECSF.** The report ([6]) took the complex requirements of the NIS 2 Directive and translated them into real-world examples, linking legal obligations directly to specific roles and skills within the ECSF. To help organisations that are just starting their cybersecurity journey, the report provided clear step-by-step use cases to get them started. Ultimately, this work proved that the ECSF is not just a theoretical framework – it is a hands-on tool that makes compliance with the NIS 2 Directive much more manageable. • **Supported community building and knowledge sharing.** At a dedicated EU workshop ([7]), 18 co-funded projects came together to share exactly how they are putting the ECSF into practice. The main takeaway was the sheer scale of the impact: these projects have already used the ECSF as a shared foundation to successfully train thousands of people across Europe. • **Piloted the attestation** of skills. ENISA ran a pilot programme to create a standardised **incident responder** profile, using the corresponding ECSF role profile to build the foundation for a future EU-wide skills attestation. The goal was to see how different countries currently handle skills certification and gauge actual market demand. With **eight Member States** stepping up to participate, the pilot delivered excellent cross-border insights and showed that an EU-wide approach is highly viable.
3.2. Organise targeted exercises and support stakeholders to plan and execute their own exercises.	**In 2025, ENISA achieved the following.** • Empowered communities by focusing on how to maximise efficiency and promote more impactful exercises. The team consciously shifted their approach; instead of acting as a pure service provider that runs every event, ENISA became an enabler, empowering communities to organise their own exercises. A major milestone in this shift was the finalisation and publication (in early 2026) of *The ENISA Cybersecurity Exercise Methodology* ([8]). Validated by the NLO subgroup and key authorities **–** including the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU); the European Central Bank; the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), Frontex and sectoral authorities from Denmark, Latvia and Portugal **–** showing that this methodology works in practice, not just on paper. While this first version was built for complex events like Cyber Europe, the ultimate goal is for it to become community-driven, using collaboration platforms, like GitHub, to let stakeholders adapt, tweak and simplify the framework for their own needs. • Led the extensive planning for **2026 Cyber Europe** through hybrid conferences, online plenaries and 13 task force sessions. Key deliverables included a finalised scenario, a new evaluation framework and 18 technical artefacts for flexible attack paths. The scope was also expanded to test the EU blueprint for cybersecurity crisis management, supported by a newly established political-level task force to ensure strategic alignment. The evaluation framework is a key feature that will lead to better assessments of the performances of the teams of participants, eventually resulting in a more impactful exercise. • Upgraded to exercises solution, making it much easier to edit and replay past scenarios. These upgrades allow Member States to organise their own exercises using the Support Action programme and Cyber Reserve funds. The true success of this approach became clear when a strong community effort emerged: experienced Member State experts actively reached out to help first-timers, sharing advice and even fully customised scenarios.

(6) https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities.
(7) https://www.enisa.europa.eu/events/european-cybersecurity-skills-workshop/ECSF2025.
(8) https://www.enisa.europa.eu/publications/the-enisa-cybersecurity-exercise-methodology.

	• Managed or contributed to nine major cybersecurity exercises in 2025, directly engaging over 1 000 players and indirectly reaching around 9 000 experts. Key highlights included: - testing the entry/exit system alongside eu-LISA and Frontex ([9]), - the first HWPCI political tabletop exercise of the Danish EU Presidency, - the BlueOLEx tabletop exercise with the upcoming Cypriot EU Presidency ([10]), - the cyber standard operating procedures exercise (SOPEx), exploring cooperation between the CNW and EU-CyCLONe, - the Jasper exercise, in collaboration with CERT-EU, - two Cyber Europe scenario replays in Denmark and Latvia, focusing on the healthcare sector.
3.3. Organise targeted training and awareness programmes and support stakeholders to plan and execute their own training/ programmes.	**In 2025, ENISA achieved the following.** • It focused on the AR-in-a-box methodology and the highly successful Ad Hoc Working Group (AHWG) on Awareness Raising and Cyber Hygiene. • It renewed the AHWG (its initial term ended in June 2025) to ensure continuous expert guidance. The call for seats was a massive success, drawing 200 applications. After reviewing the candidates, ENISA selected 25 core members and 9 observers from EU bodies and Member State public entities in September 2025. This brought together an enthusiastic mix of professionals from the public and private sectors, academia, civil society and the cybersecurity industry. • Both the AR-in-a-box methodology and the AHWG directly supported the requirements of the CSA and the NIS 2 Directive implementation, particularly regarding cybersecurity awareness and training (CSA, Article 10; the NIS 2 Directive, Articles 7(1)(h), 20(2) and 21(2)(g)) by: - providing guidance on good practices and supporting Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education, - providing frameworks and resources that national authorities can adapt for public awareness campaigns, - providing tools to develop and deliver effective training programmes for employees, - offered resources focused on enhancing awareness and promoting good cyber hygiene. • The second Cybersecurity Awareness Raising Conference, organised in Zagreb with extensive support from the Croatian government, continued to explore the human dimension of cybersecurity communication with more than 300 participants. The event built on the outcomes of the first conference, helping cybersecurity awareness become more accessible, actionable and impactful across Europe. Following the physical meeting in Zagreb, the AHWG created a dedicated task force to develop a methodology for successful community building using state-of-the-art practices. The group discussed the scope, and the first draft is currently underway, set to be presented at the AHWG's first plenary meeting in 2026. Concurrently, the ambassador's programme helped further promote AR in a box through webinars, articles, presentations and social media. The tool was integrated into 4 online platforms, making its content available to over 4 800 participants. Additionally, a successful pilot course was delivered in partnership with the ESDC, equipping participants from Member States and EU entities with the practical tools and knowledge to design and implement effective awareness programs using the AR-in-a-box framework. • The agency directly and indirectly impacted over 26 000 professionals across 16 Member States through AR in a box. This massive reach contributed to stakeholder resilience and improved cyber hygiene skills, driving real behavioural change and ultimately increasing preparedness.
3.4. Organise and support cybersecurity challenges, including the European Cybersecurity Challenge (ECSC).	**In 2025, ENISA achieved the following.** • Stepped back from hands-on execution to focus on transferring key responsibilities to ECSC management, adopting a new and clearly more strategically oriented role. The aim was to give the community more ownership, spend fewer precious resources, use the agency's reputation and connections to attract other partners and, most importantly, safeguard the fairness and integrity of the competitions. The steps undertaken in 2025 should lead to a more mature and sustainable European programme that showcases European values and excellence.

(9) https://www.eulisa.europa.eu/activities/large-scale-it-systems/ees.

(10) https://www.enisa.europa.eu/news/blueolex-2025-testing-the-capabilities-of-eu-crisis-management-executives.

- Prepared the 2025 European Cybersecurity Challenge (2025 ECSC) final. National cybersecurity competitions across participating Member States and European countries drew in thousands of students, building a strong talent pool for Europe. These local events act as an attractor for future professionals, guiding top players from national selections all the way to the ECSC finals – and for some, a place in Team Europe. The 2025 ECSC finals – hosted in Warsaw, Poland – gathered 390 contestants from 39 national and invited teams, supported by coaches, jury members and the Polish organisers. The 2025 challenge demonstrated increased organisational maturity, including improved governance structures and processes, and transparent scoring and complaint mechanisms. ENISA ensured strategic coordination, playing a key role in the perception of the competition's fairness, transparency and procedural integrity. Community involvement grew stronger as the ECSC MB gained more day-to-day independence, the Steering Committee collaborated more closely and alumni became even more engaged. These were crucial steps in guiding the ECSC toward becoming a self-sustaining European model under ENISA's strategic oversight. At the same time, ENISA experts worked closely with their peers at the ECCC to secure funding for 2026 activities. This teamwork makes it easier for both agencies to cooperate and contribute their unique strengths. In November 2025, Team Europe took first place at the ICC in Tokyo, Japan – their fourth consecutive win. ENISA launched this global competition in 2022, and its continued success relies on strong cooperation with regional and international partners. This year, the EU delegation to Japan supported Team Europe's preparation and managed their logistics. Having ENISA representatives on the ground in Tokyo provided a fantastic platform to contribute to the JP–US–EU Industrial Control Systems Cybersecurity Week for the Indo–Pacific Region. Through keynote talks and hands-on training, they showcased the 'European way' – highlighting how inclusiveness, teamwork and strong community engagement lead to success.
- Supported dedicated bootcamps and mentoring under the female team Europe framework, to boost female participation and actively developed this crucial talent pool.
- Expanded its engagement with the other partners. Initiatives like compete with Team Europe created a unique bridge between generations, attracting broader industry and institutional participation. These events gave seasoned professionals a first-hand look at the incredible hands-on expertise of upcoming talent. In turn, the seasoned professionals showed the young talent that a career in cybersecurity can take many shapes and that it is genuinely fun, challenging and engaging.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
3.1. Support the adoption and uptake of the ECSF.	Review and update the ECSF in line with the Cybersecurity Skills Academy Communication. Measure and report the skills gap, including developing indicators to be used for the cybersecurity index. Promote the adoption of the ECSF in Member States, in training organisations and academia. Regularly update the ECSF.	AHWG on Cybersecurity Skills ECCC WG 5 on Skills	Number of Member States endorsing the ECSF.	Annual	10	18
			Number of training organisations endorsing the ECSF in their training programmes.	Annual	15	26

3.2. Organise targeted exercises and support stakeholders to plan and execute their own exercises.	Organise a limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders. Develop, deploy and promote exercises, tools and frameworks that enable stakeholders, in particular in sectors impacted by the NIS 2 Directive, to independently execute their own cybersecurity exercises. Develop a community to 'train the trainers' that leverages the tools, platforms and frameworks developed by ENISA.	CERT-EU CSIRTs network (as applicable) EU ISACs (as applicable) EU-CyCLONe members (as applicable) NIS CG (as applicable) NLO network (as necessary) NLO subgroup of cyber Europe planners (as applicable)	Number of people impacted directly and/or indirectly by exercises organised by ENISA.	Annual (report)	> 7 000	> 9 000
			Number of sectoral authorities, including EUIBAs, using ENISAs exercise solutions and frameworks.	Annual	5	7
			Number of Member States participating in the community of 'train the trainers'.	Annual	10	27
3.3. Organise targeted training and awareness programmes and support stakeholders to plan and execute their own training/ programmes.	Develop, deploy and promote training and awareness-raising tools, frameworks and content that enable stakeholders, in particular those in sectors impacted by the NIS 2 Directive, to independently execute their own training or awareness-raising programmes. Develop a community to 'train the trainers' that leverages the tools, platforms and frameworks developed by ENISA. Harmonise training activities sponsored by Cybersecurity Support Action.	CSIRTs network (as applicable) EU ISACs (as applicable) EU-CyCLONe members (as applicable) NIS CG (as necessary) NLO network (as necessary) NLO subgroup of Cyber Europe planners (as necessary)	Number of participants in ENISA online training sessions.	Annual (report)	4 000 (depending on the Support Action contribution).	> 4 800
			Number of participants in ENISA's train-the-trainer and train-the-planner events.	Annual (report)	> 250	> 300
			Number of professionals impacted by ENISA's AR in a box.	Annual (report)	10 000	> 26 000

3.4. Organise and support cybersecurity challenges, including the ECSC.	Deliver the ECSC final. Form and train an elite team representing Europe at the ICC. Create challenges and a platform with access to new potential cybersecurity professionals.	ECSC Steering Committee NLO subgroup	Number of countries represented in the Team Europe cohort.	Annual (report)	26	32
			Number of users participating in ECSC and national capture the flags, who potentially are new cybersecurity professionals.	Annual (report)	20 000	35 000

STAKEHOLDERS AND ENGAGEMENT LEVELS

Involve/engage. Training organisations; private entities in sectors impacted by the NIS 2 Directive; CSIRTs network and related operational communities; EU ISACs; EU-CyCLONe members; cyber blueprint stakeholders; Security operations Centers (SOCs), including national and cross-border SOCs; national competent authorities through the NIS CG workstreams; the AHWG on Awareness Raising and Education; the AHWG on Skills; the European External Action Service (EEAS); the Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR); the Directorate-General for Communications Networks, Content and Technology; and cybersecurity professionals.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	12	**NUMBER OF FTES ACTUALLY USED [11]**	10.6
PLANNED BUDGET (EUR)	703 508.34	**BUDGET CONSUMED (EUR)**	859 919.50
AMENDED BUDGET (EUR)	859 919.50	**OF WHICH CARRIED OVER TO 2026 (EUR)**	208 643.44

[11] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

ACTIVITY 4

Enabling operational cooperation

Activity 4 supported operational cooperation among Member States; EUIBAs and between operational activities. The main aim of the activity was to provide support and assistance to ensure the efficient functioning of EU operational networks and cyber crisis management mechanisms. In addition, ENISA supported operational communities by developing and maintaining secure and highly available networks, information technology (IT) platforms and communication channels. Finally, this activity managed the ENISA cyber partnership programme and information exchange with security vendors and non-EU cybersecurity entities.

Outlined below are the key accomplishments of the activity in 2025.

- **Operational alignment**. In 2025, a new workstream on operational alignment was launched to connect and better align the different operational stakeholder communities and networks, such as the CSIRTs network and EU-CyCLONe. The objective was to further leverage internal synergies to support the various communities, presidency requests and ad hoc transversal workstreams that fed into strategic optimalisations, such as the EU cyber blueprint revision. Under this workstream, ENISA coordinated the relevant activities to align agendas and messages ahead of all major networks' plenary meetings, and to coordinate internally on key common files.

  For the Polish Presidency, ENISA coordinated several ad hoc activities that emerged during the semester and culminated in the adoption of the Council recommendation on an EU blueprint for cyber crisis management. For the Danish Presidency, ENISA supported a range of activities, including the cyber attaché visit to ENISA and, in particular, the organisation of a dedicated political-level exercise to test the new EU blueprint. This was the first-ever exercise focused on upper-level political cyber crisis coordination, aligning with the Danish Presidency's aim to strengthen the EU's security and preparedness.

- **International cooperation and collaboration with private partners**. ENISA continued the cyber partnership programme and linked its activities with EU-CyCLONe, the work of the EEAS and related efforts. Work on the international front also continued. In 2025, the total number of ENISA's international engagements increased, continuing the upward trend from previous years. This reflects both improved capture of actual engagements and a genuine sustained rise in activity. In 2025, ENISA deliberately focused its international engagements to support its priority outreach activities. The agency also successfully adopted its international strategy in December 2025, further refining their priority areas.

- **Operational IT**. IT governance and accountability were reinforced by consolidating all operational IT assets serving external ENISA stakeholders under a single operational IT manager. This new operating model delivered a high internal satisfaction rate. In parallel, ENISA began streamlining the portfolio by designing an IT architecture that will serve as the blueprint for future enhancement, integration and consolidation.

Presented below are the key lessons identified during 2025 that will guide future implementation.

- Reinforce the secretariat, for example, by engaging operational national seconded experts, and provide training to relevant and interested colleagues outside the secretariat to help cover peak periods and escalation scenarios. This stream of work needs specialised resources, ideally with an operational link to the Member States. This need is also echoed by the governance of the CSIRTs network, stressing that adequate resources are needed to be able to offer continuous high-quality support.
- Further integrate operational IT with corporate IT, potentially under the guidance of a chief information and technology officer.
- The operational alignment effectively resulted in synergies, both at the community level and internally within the agency. Further consolidation of stakeholder management would leverage this even further, connecting other stakeholders (e.g. CERT-EU, the European Cybercrime Centre (EC3), ECCC, the advisory group, etc). At the same time, the KPIs will need to be re-evaluated, to effectively measure the impact and effectiveness of this support and alignment.

Given that the cyber partnership programme required only limited resources, the programme yielded a big return of investment, specifically enabling the agency's situational awareness activities under Activity 5. Thus, it would be opportune to see if this programme can be leveraged further, expanding beyond the current scope. This would require adequate resources. In addition, the importance of stakeholder engagement cannot be understated; therefore, consolidating activities and using existing systems and frameworks could yield substantial benefits to both the agency and stakeholders.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Effective EU preparedness and response to cyber incidents, threats and cyber crises • Consolidated and shared cybersecurity information and knowledge support for Europe	• Use of ENISA's secure infrastructure and tools and added value of the support to the operational cybersecurity networks • The EU Vulnerability Database (EUVD) is operationalised by ENISA, resulting in a high satisfaction rate (among Member States and stakeholders) with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET
By the end of 2026, strengthen the interaction and trust within and between key EU operational and cybersecurity communities (the CSIRTs network, EU-CyCLONe, the HWPCI and the NIS CG).	CRA, Article 16 CSA, Articles 6 and 7 CSOA, Article 11 NIS 2 Directive, Articles 7, 10, 15 and 16	2026	Assessment of high level of operational interaction across the CSIRTs network, EU-CyCLONe, the HWPCI and the NIS CG.	> 60 % of stakeholders agree that ENISA has enabled the functioning of or supported the building of trust within the network.
			ENISA is judged as a key enabler of trust within and between the CSIRTs network, EU-CyCLONe, the HWPCI and the NIS CG.	> 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, Article 12	2026	Coherence of ENISA international engagement with the agency's strategy.	Updated international strategy.
			Comprehensive knowledge management and stakeholder management system is established.	Established framework for knowledge management and stakeholder management.
Develop and maintain relevant operational IT systems and platforms to support all operational communities and enhance synergies.	CRA, Article 16 CSA, Article 7 NIS 2 Directive, Articles 7, 10, 12, 15 and 16	2026	Relevant IT systems are maintained, and new mandatory platforms are developed.	IT operations are consolidated and a synergy plan has been designed (2025) and implemented (2026).

OUTPUTS	OUTCOME
4.1. Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs network, EU-CyCLONe members, the HWPCI and the NIS CG.	**In 2025, ENISA achieved the following.** • Provided operational alignment and support to the Council presidencies and the HWPCI. A new workstream on operational alignment was bootstrapped from zero in order to connect all ENISA activities on an operational level and streamline efforts in a coordinated manner. The goal was to exploit all internal synergies to support the different activities, presidential requests and ad hoc transversal activities, which resulted in the EU cyber blueprint revision. Under the operational alignment, ENISA coordinated the relevant activities to sync agendas and messages ahead of all the main networks' plenary meetings and Cyber Week. The agency also internally coordinated the work on main common files. In particular, for the Polish Presidency, ENISA coordinated several ad hoc activities that emerged during the semester, culminating with the adoption of the Council recommendation of 6 June 2025 on an EU blueprint for cyber crisis management. For the Danish Presidency, ENISA supported several activities, such as the cyber attaché visit to ENISA and, in particular, the organisation of a dedicated political-level exercise to test the new EU blueprint for cyber crisis management. This was the first-ever cyber crisis coordination exercise at the political level, and it followed the Danish presidential aim to enhance the EU's security and preparedness.

This resulted in:

- providing support for the blueprint revision; after its approval, kicked off the blueprint's operationalisation with the launch of the dedicated task force, workstream and HWPCI exercise,
- enhanced coordination across communities and networks; kicked off the engagement and interplay of the HWPCI, the NIS CG, EUIBAs and the cyber partnership programme with the operational networks, CSIRTs network and EU-CyCLONe;

- Supported the operations of the CSIRTs network via its secretariat function as mandated by the NIS 2 Directive, with specific heightened support for specific events and vulnerabilities. ENISA provided concrete operational support to the CSIRTs network, including the following:
  - facilitated information sharing and the establishment of situational awareness through the operation of multiple tools hosted by ENISA,
  - ensured seamless 24/7 cooperation across all cooperation modes, including by facilitating information flow, producing reports, sharing ENISA's situational awareness products and disseminating network approved reports,
  - liaised with vendors and security researchers for specific vulnerabilities and incidents (including collaboration via the cyber partnership programme),
  - managed access to collaboration tools,
  - ensured the financial coverage, management, development and maintenance of the network's secure tools,
  - supported the chair by developing the network's internal and external reports,
  - supported cooperation in working groups,
  - facilitated the network's internal coordination meetings,
  - together with the EU presidency, coordinated the organisation of the plenary meetings in addition to contributing financially,
  - facilitated cooperation between the network and the EU institutions,
  - organised the network's exercises;
- Optimised tools for situational awareness and reporting.
- Developed interaction of the CSIRTs network, cyber hubs and ECCC, with dedicated sessions and validation of the ENISA CSOA, Article 6(4) interoperability guidelines.
- Streamlined procedures for standardised processes across the networks and for internal cooperation with other ENISA units.
- Finalised (the update of) multiple important documents for smoothing cooperation within the network, namely, the multiannual work programme, its rules of procedure, the dedicated maturity framework and coordinated vulnerability disclosure policy.
- Supported the first yearly cyber partnership programme / Member States in-person workshop to bring the public and private sectors closer.
- Strengthened synergies between the CSIRTs network and EU-CyCLONe via the first joint online SOPEx25 exercises combining the former CyberSOPEx, for the CSIRTs network, and CySOPEx, for EU-CyCLONe.
- Organised three plenary meetings: 25th CSIRTs network meeting in Brussels, 26th CSIRTs network meeting in Krakow with the Polish Presidency and 27th CSIRTs network meeting in Copenhagen with Danish Presidency.
- Supported all EU-CyCLONe activities via its secretariat function and facilitated the network's information exchange and ongoing development. Working closely with the trio of Council presidencies, the agency prepared and supported:
  - the adoption of the first 2026–2027 EU-CyCLONe work programme,
  - the second report to the European Parliament and the Council in accordance with the NIS 2 Directive, Article 16(7);
- Organised the following plenary EU-CyCLONe meetings in close cooperation with the Polish and Danish Council Presidencies:
  - 18th EU-CyCLONe officers' meeting and joint session with the CSIRTs network in Brussels,
  - 19th officers' meeting and joint session with the CSIRTs network, as well as the EU-CyCLONe executives' meeting, in Krakow,
  - 20th officers' meeting and joint session with the CSIRTs network in Copenhagen,
  - 21st EU-CyCLONe officers' meeting, held in Brussels;

	• Regarding preparedness and situational awareness, assisted the working groups on standard operating procedures and exercises, notably in revising the standard operating procedures, coordinating with the CSIRTs network and organising both BlueOLEx and the first joint exercise with the CSIRTs network (SOPEx). The 2025 iteration of the senior-level exercise BlueOLEx25 was hosted by Cyprus and took place in Nicosia. At this occasion, EU-CyCLONe executives met with participants from the ENISA cyber partnership programme to exchange views on public–private cooperation in the context of incidents and large-scale cyber crises. • Strengthened information sharing. • Organised workshops with reference to the NIS 2 Directive. • Prepared targeted reports to assist EU-CyCLONe members in further developing the network.
4.2. Maintain, develop and promote the ENISA cyber partnership programme to enable the exchange of information to support the agency's understanding of threats, vulnerabilities, incidents and cybersecurity events.	**In 2025, ENISA organised the following meetings:** • four physical meetings with partners related to the joint cyber assessment report (JCAR) cycle in cooperation with activity 5, • one physical executive-level meeting, • a joint event for EU-CyCLONe executives and cyber partnership programme executives *en marge* at BlueOLEx, • the first yearly cyber partnership programme / Member States in-person workshop to bring the public and private sectors closer, • a dedicated workshop with EEAS, • several ad hoc interactions between the private sector and CSIRTs network members.
4.3. Implement ENISA's international strategy and outreach.	**In 2025, ENISA achieved the following.** • Successfully adopted its international strategy in December, following input from the MB through an extensive survey. • Engaged with approximately 224 international partners from outside the EU. Some 41 % of these were dedicated to singular limited engagements under ENISA's outreach activities, while a further 37 % took place outside ENISA's outreach areas. Some 12 % of ENISA's international engagements were in response to specific requests from EU institutions (the European Commission / EEAS), hence under an assisting approach. There were 23 (10 %) singular international engagements needed in 2025 to make new outreach activities happen. In 2025 ENISA declined 43 (19 %) international engagements, which were not seen as priority engagements. • The total number of ENISA's international engagements has increased, supporting the trend of previous years. This reflects both a deeper capturing of actual engagements, as well as a genuine continuing rise in the number of engagements. • Concentrated its international engagements in support of its priority outreach activities. These were linked to the working arrangements with Ukraine and the USA, as well as the organisation of the ICC and the engagements needed to implement the contribution agreement with the Western Balkans EU candidate countries and the cyber reserve deployment activities with Moldova. The engagements reflect areas outlined in the international strategy and the yearly list of priority areas ENISA wants to invest in, which support the agency's strategic objectives and provide the greatest added value for ENISA's mandate. • **Responded to assisting requests consistently, with tailored contributions.** The agency has become a permanent part of the EU's cyber dialogues and contributed to the 2025 G7 cybersecurity workstreams. • **Maintained its overall 'limited by default' approach to international engagements.**

	Some further 2025 highlights are detailed below. • Under its outreach activities, progress was made on ENISA's working arrangements, covering capacity building (e.g. by bringing Ukraine into the ECSC); best practice exchange on topics such as energy modelling, incident reporting or vulnerabilities management; and regular information/knowledge exchange around situational awareness. These were adapted to the geopolitical developments and EU priorities. With the support of a contribution agreement for Western Balkans candidate countries, the agency can now extend specific ENISA frameworks and tools through measures such as a cyber index or exercise methodologies and better leverage ENISA expertise through tailored training programmes. ENISA's role in the EU's incident response Cyber Reserve now allows the deployment of services also to non-EU digital-Europe-programme-associated countries, such as Moldova. • Under its assisting approach, ENISA contributed in tailored ways to six EU cyber dialogues in 2025 (respectively, with Brazil, India, the North Atlantic Treaty Organization, South Korea, the UK and Ukraine), actively contributing to ensuring dialogue deliverables (e.g. in the case of Ukraine and the UK), and also leading to increasing demand for ENISA's contributions in cooperation frameworks outside these dialogues.
4.4. Develop comprehensive coordinated vulnerability disclosure platforms by operationalising the EUVD and designing the CRA Single Reporting Platform.	**In 2025, ENISA achieved the following.** • Advanced the operationalisation of the EUVD and progressed the design of the CRA Single Reporting Platform, in line with the expected results set for 2025 to 2027. This work builds on the 2024 baseline, when ENISA finalised the first phase of the EUVD and strengthened the coordinated vulnerability disclosure ecosystem, including by becoming a common vulnerabilities and exposures (CVE) numbering authority (CNA). • Delivered operational readiness. For the EUVD, this included preparing the service for use by operational stakeholders and supporting adoption through user enablement, including training activities as provided for in the programming objectives. For the CRA Single Reporting Platform, work in 2025 concentrated on establishing the technical specifications needed for implementation and putting in place the conditions to begin delivery with an implementation partner. • Ensured governance and quality assurance through structured validation processes and ongoing engagement with relevant communities and business owners. These efforts contribute to long-term performance goals, including a target stakeholder satisfaction rate of 66 % by 2027, demonstrating the platforms' sustained usability and value as they scale up.
4.5. Develop and maintain IT systems and platforms for operational activities.	**In 2025, ENISA achieved the following.** • Continued to develop, operate and improve the IT systems and platforms that enable its operational activities and serve key operational communities. Delivery priorities remained focused on reliability and service continuity, and strengthened security controls and predictable operations across the full service life cycle, from onboarding and support to maintenance and incremental enhancement. • Met planned objectives across the core enabling workstreams that underpin operational service delivery. These objective included improvements to IT service management and security practices, reinforced staff development and performance evaluation mechanisms, stronger day-to-day service to business owners, continued development of new technology platforms, and digital transformation initiatives supporting more efficient and resilient delivery. Governance and accountability were further strengthened by consolidating all IT assets serving external ENISA stakeholders under a single operational IT manager. This new operating model achieved an internal approval rate of 93 % among the business owners of the IT assets under management. In parallel, ENISA initiated work to streamline the IT infrastructure portfolio by designing an IT architecture that will serve as the blueprint for future enhancement, integration and consolidation. • Maintained a stakeholder-driven delivery approach through structured validation and regular engagement with communities and business owners, ensuring that priorities, risks and dependencies were continuously assessed and addressed. This governance model supports the multi-year modernisation trajectory, including the objective to update one third of the current operational systems each year, progressing towards full renewal by 2027, while preserving stable service levels throughout the transition.
4.6. Development of stakeholder and knowledge management systems and frameworks.	In 2025, the activity supported the Associate Chief Cybersecurity & Operations Officer (ACOO) with the development and eventual adoption of the ENISA stakeholder strategy thus providing a framework for engaging with stakeholders.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
4.1. Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs network and EU-CyCLONe members, the HWPCI and the NIS CG.	Enhanced information sharing and cooperation among the CSIRTs network and EU-CyCLONe members and enhanced interaction with the HWPCI and the NIS CG.	CSIRTs network EU-CyCLONe HWPCI NIS CG	Continuous use and durability of platforms (including prior to and during large-scale cyber incidents).	Annual (report)	> 60 % use of platforms.	CNW 81.3 % EU-CyCLONe 63.4 %
			Number of joint sessions established.	Annual (report)	2 joint sessions per year with operational outcomes.	5 joint sessions.
4.2. Maintain, develop and promote the ENISA cyber partnership programme to enable the exchange of information to support the agency's understanding of threats, vulnerabilities, incidents and cybersecurity events.	Operational-isation of the cyber partnership programme.	CSIRT network EU-CyCLONe EUIBAs HWPCI MB	Number of new and total partners in the ENISA partnership programme.	Annual (report)	6	1 new in 2025 and 9 entities in total.
			Percentage of RFI answered by members of partnership programme.	Annual (report)	65 %	67 %
4.3. Implement ENISA's international strategy and outreach.	EU values recognised by international stakeholders. International cooperation supports ENISA's objectives.	European Commission EEAS MB (as required ENISA Management team	Staff satisfaction with international coordination.	Annual (survey)	3.5	3.9 (survey revised to use a 1–5, where 1 means very dissatisfied and 5 means very satisfied).
4.4. Develop comprehensive coordinated vulnerability disclosure platforms by operationalising the EUVD and designing the CRA Single Reporting Platform.	The EUVD is deployed. The CRA Single Reporting Platform is being developed.	CSIRTs network				

4.5. Develop and maintain IT systems and platforms for operational activities.	Consolidation of operational IT with a view to supporting ENISA operations.	Business owners of ENISA's operational IT systems CSIRTs network EU-CyCLONe HWPCI NIS CG	IT architecture for external operational IT services.	Biennial update	End of 2025.	Completed on time.
			ENISA operational IT.	Annual (report)	All operational IT systems are consolidated under one IT operational manager by 2025.	All IT operational assets are consolidated and streamlined on time.
					One third of current systems are updated every year to reach 100 % in 2027.	One third of current IT assets were updated and systems upgraded based on need.
			EUVD.	Annual (report)	EUVD is produced and users are trained.	EUVD is live and provides services to the EU.
			CRA Single Reporting Platform.	Annual (report)	Technical specifications of the CRA Single Reporting Platform are available and the service provider is contracted to start implementation.	The design and the development of the CRA started. The contactor is delivering milestones according to plan.
4.6. Development of stakeholder and knowledge management systems and frameworks.			Stakeholder satisfaction with knowledge management and stakeholder management system.	Biennial (survey)	> 60 % by 2026.	The results will be attained at the end of 2026 after a full year of implementation.

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. Blueprint actors; EUIBAs ; CSIRTs network members; EU-CyCLONe members; HWPCI; NIS CG; and SOCs, including national and cross-border SOCs.

Involve/engage. NIS CG, Operators of Essential Services and Digital Service Providers , and ISACs.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	15	**NUMBER OF FTES ACTUALLY USED [12]**	11.3
PLANNED BUDGET (EUR)	1 549 190.03	**BUDGET CONSUMED (EUR)**	1 719 918.17
AMENDED BUDGET (EUR)	1 721 189.50	**OF WHICH CARRIED OVER TO 2026 (EUR)**	767 668.51

(12) FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

ACTIVITY 5

Provide effective operational cooperation through situational awareness

Activity 5 contributed to cooperative preparedness and responses at the EU and Member State levels through data-driven analyses of threats and risks, and operational and strategic recommendations based on incidents, information on vulnerabilities and threats in order to contribute to the EU's common situational awareness.

Outlined below are the key accomplishments of the activity in 2025.

- Oversaw a coherent situational awareness portfolio, supported by the increase in Member States contributing to key publications (e.g. the report mandated by CSA, Article 7(6), known as the JCAR, and *ENISA Threat Landscape*) and matured usage of the private-sector community through ENISA's cyber partnership programme. This effort in particular has allowed the agency to progress towards achieving a common situational awareness through shared data validated by joint analysis. Over 75 % of Member States contributed to and validated reports. Success in this regard was also due to the progress made in establishing a threat management platform to foster and facilitate the sharing and validation of threat data. Additionally, the reallocation of tasks on vulnerabilities and incidents has increased data integration to further improve consolidation for situational-awareness purposes.
- Launched the EU Vulnerability Database (EUVD) in April 2025, strengthening ENISA's position within the global vulnerability ecosystem. Moreover, ENISA as both a CNA and a root within the CVE programme allows the agency to better support Member States and the EU internal market regarding vulnerability management. This dual role of the agency helped it achieve the strategic objective indicator of establishing and operating the EUVD.
- Worked towards establishing the EU's CRA Single Reporting Platform. In 2025, the agency set the foundation for the platform's development, including finalising and awarding contracts to external providers, finalising the hiring of the personnel, advancing the establishment of functional requirements and starting the implementation of the platform. The platform launch is expected by 11 September 2026 to meet legal requirements. The platform will act as the foundation for collating high quality and accurate information about exploited vulnerability and severe incidents. Through this, ENISA will be able to maintain an accurate repository of EU known exploitable vulnerabilities, which will underpin organisations' vulnerability management practice at the EU and global levels.

Presented below are the key lessons identified during 2025 that will guide future implementation.

- Increase readiness to operate the new CRA Single Reporting Platform securely. In turn, through this investment, the agency will be ready to absorb, establish and operate future EU level systems.

- Increase cooperation with Member States on situational awareness and threat analysis. The agency will continue cooperating with external stakeholders (primarily Member States and private partnerships) to enhance the agency's ability to provide quality and timely situational awareness on cyber issues, including by making available tools to facilitate information collection and monitoring. This way, the agency can move towards a single repository of high-quality non-classified information about threats, incident and vulnerabilities to better provide a common picture. Following on from this strategy, the agency will be able to not only function as an aggregator of high-quality validated data but also unlock additional resources to support Member States and businesses to mature their situational awareness. In addition, the agency will further work on integrating information available to the agency, including NIS 2 reporting, vulnerability information through the EUVD as well information from the CRA Single Reporting Platform.

- Strengthen EU vulnerability services. The agency will continue to invest in its role in the global vulnerability space to support strategic programmes, such as CVE, and continue developing EU strategy around the EUVD and the CRA Single Reporting Platform. A new service layer will need to be built to better support EU organisations in dealing with vulnerability management. This service must be built with the Member States to be able to harvest the knowledge and capacity already available in the EU. The adoption of new technologies, such as AI, should also be considered to support scaling up the service, especially taking into account that such technologies are already used to find and exploit vulnerabilities. Due to the increased importance of vulnerability services as stand-alone services, in 2026–2027, ENISA should expect additional focus on this topic and tasks. As such, a dedicated output with related KPIs should be established to better reflect the scope of the tasks and measure performance.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Effective EU preparedness and response to cyber incidents, threats and cyber crises • Consolidated and shared cybersecurity information and knowledge support for Europe	• The EUVD is operationalised by ENISA, and there is a high satisfaction rate (among Member States and stakeholders) with ENISA's ability to contribute to common situational awareness through accurate and timely analyses of incidents, vulnerabilities and threats • A successfully operated reporting platform under the CRA is established within 21 months of the regulation's entry into force

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET	2025 RESULTS
By the end of 2027, build a common situational awareness between Member States based on accurate shared data and underpinned by validated joint analysis.	CSA, Article 7 CSOA, Article 18 NIS 2 Directive, Article 23(9)	2025–2027	Content of the JCAR is contributed to and validated by Member States.	Produce at least 1 comprehensive joint analysis report every quarter, contributed to and validated by at least 75 % of Member States (the JCAR).	24 Member States contributing (CNW and EU-CyCLONe) (13 more than in 2024).
			ENISA data repository is open to and includes information directly provided by Member States.	Data repository is accessible by Member States.	Access to OpenCTI SaaS instance provided to 7 Member States (CNW) as part of a beta test since November 2025.
				Percentage of information in the data repository validated or provided by Member States is above 75 % and 100 % for significant events impacting Member States.	Applicable from 2027.
			Establish and test processes and procedures for the incident review mechanism under CSOA, Article 18.	Incident review mechanism is established and endorsed by Member States.	A workshop to consult Member States and COM was held in November 2025; work to finalise the draft standard operating procedure is ongoing.
Provide regular general as well as specific threat landscapes and threat analyses, based on observed data-driven trends in incidents and vulnerabilities.	NIS 2 Directive, Article 23(9) CRA, Articles 14–17 CSA, Articles 7 and 9 CSOA, Article 18	2025–2027	Produce *ENISA Threat Landscape*.	Maintain the regular publishing schedule for the general threat landscape reports (yearly) and specific threat analysis and sectoral reports (e.g. bi-monthly).	2025 *ENISA Threat Landscape* and the threat landscape report for public administration published.

			The JCAR includes threat analysis based on incidents and vulnerabilities available within ENISA's data repositories (EUVD, Cybersecurity Incident Reporting and Analysis System (CIRAS), CRA Single Reporting Platform).	Incident analysis is included in the JCAR as of Q3 2025.	Information (versus analysis) regarding CIRAS reporting over the reporting period included since the JCAR of Q4 2025.
				EUVDB vulnerability analysis is included by Q2 2025.	Information (versus analysis) from the EUVD over the reporting period included since the JCAR of Q1 2025.
				CRA Single Reporting Platform Adversarial Exposure Validation (AEV) and incidents analysis are included by Q4 2026.	Applicable from 2027.
			ENISA's ability to produce accurate threat analyses based on incidents, vulnerabilities and threat information based on the agency's own monitoring, shared by external stakeholders due to legal obligation [13] or voluntarily shared.	80 % of Member States score the quality of ENISA's threat analyses above 4 (on a 1–5 scale).	Overall customer satisfaction score from Member States re. quality of SitAw and Threat analysis reports = 3.5.
				80 % of Member States score ENISA's ability to use the available information to produce threat analyses and recommendations above 4 (on a 1–5 scale).	Overall CSAT from Member States regarding the usefulness of situational awareness and threat analysis reports = 3.5.
			CRA Single Reporting Platform is established and operational.	CRA Single Reporting Platform is used to carry out tasks under the CRA by the end of 2026.	Applicable from 2027.

(13) The NIS 2 Directive, the CRA and Regulation (EU, Euratom) 2023/2841.

OUTPUTS	OUTCOME
5.1. Collect, organise and consolidate information (including from the general public) on common cyber situational awareness, technical situational reports, incident reports and threats, and support the consolidation and exchange of information on the strategic, operational and technical levels [14].	In 2025, ENISA focused primarily on revamping and enhancing the ENISA Threat Information Management platform and continuously strove to improve their data collection, monitoring and analysis processes. Highlights for 2025 include introducing a quality assurance role and the overall streamlining of processes to accommodate all the agency's reporting needs and situational awareness contributions. In addition, 24 Member States (13 more than in 2024) and 11 ENISA cyber partnership programme members (2 more than in 2024) contributed to the JCAR. The agency continued to deliver on all its situational awareness service catalogue, including the establishment of ENISA sectoral reports to support the *NIS360* strategy. The agency's achievements in this area in 2025 can be summarised as follows. • Improved the **structure of daily collection and monitoring through the first ENISA cyber threat intelligence doctrine**. As result, the agency achieved a **higher collection rate (> + 70 %)** while maintaining accuracy and timeliness. ENISA expects to maintain this level in 2026, with throughput reaching a plateau. • Optimised processes and tools. In 2025, all listed events were tracked and **enriched in open source threat intelligence (OpenCTI)**, daily and weekly open-source intelligence reports are produced within the platform through the development of connectors. 2025 also saw the operationalisation of Open Retriev al and Analysis System (ORAS), atool currently used to track hacktivism-related data and expected to expand monitoring scope in 2026. • **Standardised processes for daily briefs** and reports, providing up-to-date information about relevant events. The daily brief makes use of the dashboard in Union Regular Situational Awareness (URSA)for delivery. • Continued delivering the **standard product portfolio, maintaining quality and customer satisfaction**. There were more flash reports as a result of a higher number of interesting events (50% more than in 2024). Continuously contributed to three ISAA workflows Integrated Political Crisis Response (IPCR) activation on Ukraine – Russian, Israel - Hammas and the EU election). • Executed **synergies with other operational activities** (e.g. Activity 2 for sectoral matters and Activity 4 for outreach) and initiated a workstream to ensure Threat Analysis Services (TAS) contribution to risk assessment reports in 2026. • **Executed the cyber situation awareness and analysis centre strategy** by onboarding two HCs, which allowed the **offboarding** of a number of tasks (e.g. ISAA and reviewing the Cyber Coordination Task Force bi-weekly report). • Nurtured cooperation with **CERT-EU** via structured cooperation. Together, the agency produced **four Joint Rapid Reports** to date and managed the **programme and joint initiatives**, including the possible revamping of the joint publication report. ENISA supported the EC3 in conducting Operation Eastwood (related to NoName057(16) takedown). CERT-EU and the EC3 joined the ENISA cyber threat intelligence conference. An initiative to collectively discuss OpenCTI was also launched, gathering CERT-EU and Strategic communications. • Increased participation in the Cyber Diplomacy Toolbox process via situational awareness. The agency provided **six briefings at the HWPCI and contributed to four high-level EU dialogues in support of EEAS**, which contributed to increasing ENISA's relevancy as a EU-level situational awareness key player. • Executed three exchanges on the threat situation with Ukraine and two with the Cybersecurity and Infrastructure Security Agency (CISA). • Produced two strategic annual documents, *ENISA Threat Landscape* and *ENISA Sectorial Threat Landscape – Public administration*. A new methodology was released for the *ENISA Threat Landscape*, which includes review and validation from Member States via the CSIRT network and from private-sector actors through the cyber partnership programme.
5.2. Provide analysis and risk assessment jointly with other operational partners, including EUIBAs, Member States, industry partners and non-EU partners.	
5.3. Collect and analyse information to report on cyber threat landscapes.	

(14) Advisory group proposal for standby emergency incident analysis team provisioned within Output 5.1.

5.4. Analyse and report on incidents as required by Article 5(6) of the CSA and other sectoral legislation (e.g. DORA, Electronic Identification and Trust Services Regulation (eIDAS) Article 10, etc.).	**In 2025, ENISA achieved the following.** • Established a team, with new colleagues joining throughout 2025, to implement the CRA Single Reporting Platform, incident reporting and vulnerability services. • Facilitated successful staff mobility with the European Securities and Markets Authority (ESMA) for DORA, a project Incidents and Vulnerabilities Services is also working on. • Cooperated strongly with internal and external stakeholders. The agency had frequent contact and strong cooperation with corporate support services (CSS) (mainly regarding recruitment and procurement) and Activities 2 and 4 (to align on issues like incident reporting and the CRA Single Reporting Platform). The agency also worked hand-in-hand with the Directorate-General for Communications Networks, Content and Technology; CSIRTs; the NIS CG; CISA; and The MITRE Corporation, establishing trusted relationships. • Completed the CRA Single Reporting Platform tender and awarded the contract. The CRA Single Reporting Platform implementation project is in its execution phase, and development is on track. Internal testing of the platform's main components has started. The CRA Single Reporting Platform team created and are applying PM2 methodology to the project. • With extensive CSS support, negotiated and amended the 2025–2028 CRA Single Reporting Platform contribution agreement for a further EUR 8 million in order to maintain the future platform. • Launched Cybersecurity Incident Reporting and Analysis System v2 (CIRAS 2) and the EUVD; both are fully deployed. Upgrades are constantly developed based on feedback. • Established the NIS 2 Directive reporting regime of two biannual findings presentations in the NIS CG and CSIRTs network and one annual report. The last trusted service providers and telecommunications incident reportsand NIS 1 reports were issued. • Continued to deliver CNA services (as of 2025, 21 CVEs have been published with 12 reserved), supported the build up of the EU known vulnerability catalogue. • Achieved root CNA status within the CVE programme and started onboarding five new CNAs under the ENISA CNA root.
5.5. Develop the CRA Single Reporting Platform and operationalise the EUVD.	

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
5.1. Collect, organise and consolidate information (including from the general public) on common cyber situational awareness, technical situational reports, incident reports and threats, and support the consolidation and exchange of information on the strategic, operational and technical levels ([15]).	Establishment of a threat information management platform. Production of briefings, reports and summaries of incidents, threats and vulnerabilities. Increased understanding and timely access to information regarding the latest threats, incidents and vulnerabilities.	CSIRT network EU entities EU-CyCLONe National authorities within Member States subscribed to the products	Timeliness and accuracy of reports.	Annual (survey)	> 85 %	Overall accuracy score of 3.8 out of 5 and an overall timeliness score of 3.9 out of 5 (based on responses from 49 respondents out of 660 surveyed).

(15) Advisory group proposal for standby emergency incident analysis team provisioned within Output 5.1.

5.2. Provide analysis and risk assessment jointly with other operational partners, including EUIBAs, Member States, industry partners, and non-EU partners.	EU joint assessment and reports, sectoral analysis and threat analysis [16]. Recipients receive accurate and timely assessments of threat actors and associated risks to the EU internal market.	CSIRT network EU entities EU-CyCLONe HWPCI MB	Number of contributing Member States to the JCAR.	Annual (report)	> 40 %	24 Member States contributing (an increase of 13).
5.3. Collect and analyse information to report on cyber threat landscapes.	Mapping threats. Generating recommendations for stakeholders to take up.	Advisory group and Cybersecurity Threat Landscape AHWG CSIRTs network NLOs	Number of downloads of *ENISA Threat Landscape*.	Annual (report)	> 5 % increase year on year	6 195 downloads in a five-week period
5.4. Analyse and report on incidents as required by Article 5(6) of the CSA and other sectoral legislation (e.g. DORA, eIDAS Article 10, etc.).	Analysing incidents. Generating recommendations for stakeholders to take up.	European Competent Authority for Secure Electronic Communications European Competent Authority for Trust Services Expert Group NIS CG workstream 3	Operational processes expected for 2025 are defined. Implementation work in progress.	Survey	80 % of the stakeholders agree on the established process and score them > 4 (Scale 1 to 5).	100 % of respondents gave a satisfaction score of ≥ 4 for the platform so far.
5.5. Develop the CRA Single Reporting Platform and operationalise the EUVD.	CRA Single Reporting Platform work is scoped, and implementation is initiated. Operational and business processes are defined together with primary stakeholders.	CSIRT network				

[16] Including the JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and Directorate-General for Communications Networks, Content and Technology Situation Centre.

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. Member States (including CSIRTs network members and EU-CyCLONe members), EUIBAs, other technical and operational blueprint actors, partnership programme members for Activity 5.3 (e.g. trusted vendors, suppliers, partners) and CTL AHWG.

Involve/engage. Other types of CSIRTs and PSIRTs and the private sector.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	14	**NUMBER OF FTES ACTUALLY USED [17]**	11.2
PLANNED BUDGET (EUR)	1 488 217.69	**BUDGET CONSUMED (EUR)**	1 549 520.38
AMENDED BUDGET (EUR)	1 552 391.38	**OF WHICH CARRIED OVER TO 2026 (EUR)**	479 099.63

[17] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

ACTIVITY 6

Provide services for operational assistance and support

Activity 6 contributed to the further development of capabilities to prepare and respond at the EU and Member State levels for large-scale cross-border incidents or crises related to cybersecurity through the implementation and delivery of *ex ante* and *ex post* services. The action implements the cybersecurity support action through which the agency provides services such as penetration testing, threat hunting, risk monitoring and assessment, customised exercises and training, and supports the Member States in responding to incidents.

Outlined below are the key accomplishments of the activity in 2025.

- **Streamlining the service catalogue of the support action and EU Cybersecurity Reserve.** Activity 6 streamlined and updated the support action service catalogue, taking into account Member States' needs and the anticipated operationalisation of the EU Cybersecurity Reserve. To achieve this, Activity 6 conducted structured consultations with Member States, analysed service uptake data and aligned the portfolio with managed security service provider market capabilities, refining both *ex post* (incident response) and *ex ante* (preparedness) services accordingly. The revised catalogue delivers a coherent, market-aligned and comprehensive set of incident prevention and response services that better reflect Member State demand while strengthening operational readiness for the reserve. The updated catalogue constitutes a key milestone in supporting the implementation of Outputs 6.1–6.4 of the ENISA SPD, ensuring strategic coherence between service delivery and the operationalisation of the EU Cybersecurity Reserve.
- **Transition from support action to the EU Cybersecurity Reserve.** During 2025, the transition from the support action programme to the operational model of the EU Cybersecurity Reserve was prepared and implemented. In order to achieve this, it was necessary to ensure continuous alignment among all key stakeholders, including Member States' cyber crisis management authorities, NIS single points of contact and service providers. Activity 6 systematically defined incident response activation workflows and playbooks, while establishing the necessary technical infrastructure and operational protocols to support their implementation. As a result, the EU Cybersecurity Reserve became fully operational at the beginning of 2026, in parallel with the conclusion of the support action programme.
- **Cybersecurity services assessment framework.** Activity 6 designed and

implemented a cybersecurity services assessment framework to systematically evaluate the quality, impact and strategic alignment of services delivered under the support action programme, with a view to its continued use in the EU Cybersecurity Reserve era. Activity 6 established a structured methodology to measure how service delivery meets the objectives and expectations of important and essential entities in Member States, while enabling ENISA to identify areas for improvement and implement corrective actions to maintain high-quality delivery. The framework was developed and operationalised in 2025, with the first consolidated results expected in 2026, fully aligned with the operationalisation of the EU Cybersecurity Reserve.

- **Mapping the EU Cybersecurity Reserve's services.** In view of the operationalisation of the EU Cybersecurity Reserve and in accordance with Article 16(6) of the CSOA, ENISA prepared a comprehensive mapping of the services required by reserve users. Activity 6 conducted a systematic analysis of user needs alongside an assessment of services' availability within managed security service providers' portfolios. The analysis confirmed the overall completeness and relevance of the service catalogue, demonstrating that it largely meets Member States' needs and that EU-controlled managed security service providers are capable of supporting Member States, and European Economic Area / European Free Trade Association and DEP-associated countries. Through this action, Activity 6 provided evidence-based consultation to the Directorate-General for Communications Networks, Content and Technology regarding the provision of EU Cybersecurity Reserve services by vendors or entities established and controlled within the EU, in line with Article 12(5) of the DEP.

In 2025, a total of 145 services were delivered within the framework of the cybersecurity support action and the EU Cybersecurity Reserve:

- 129 *ex ante* / preparedness services (penetration testing, exercises, threat landscapes, risk monitoring, customised services classified as 'other'),
- 16 incident response retainers (*ex post* services).

From January to December 2025, incident response support was provided for four cybersecurity incidents – three under the cybersecurity support action and one under the EU Cybersecurity Reserve.

The main sectors that benefited from the services in 2025 were public administration, transport, health and energy.

Presented below are the key lessons identified during 2025 that will guide future implementation.

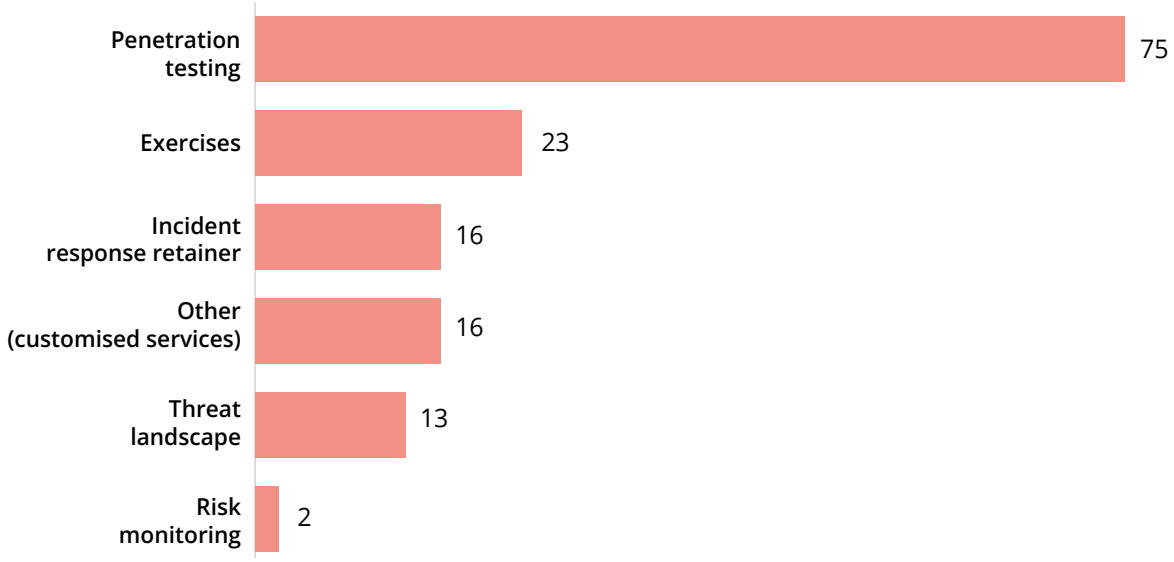
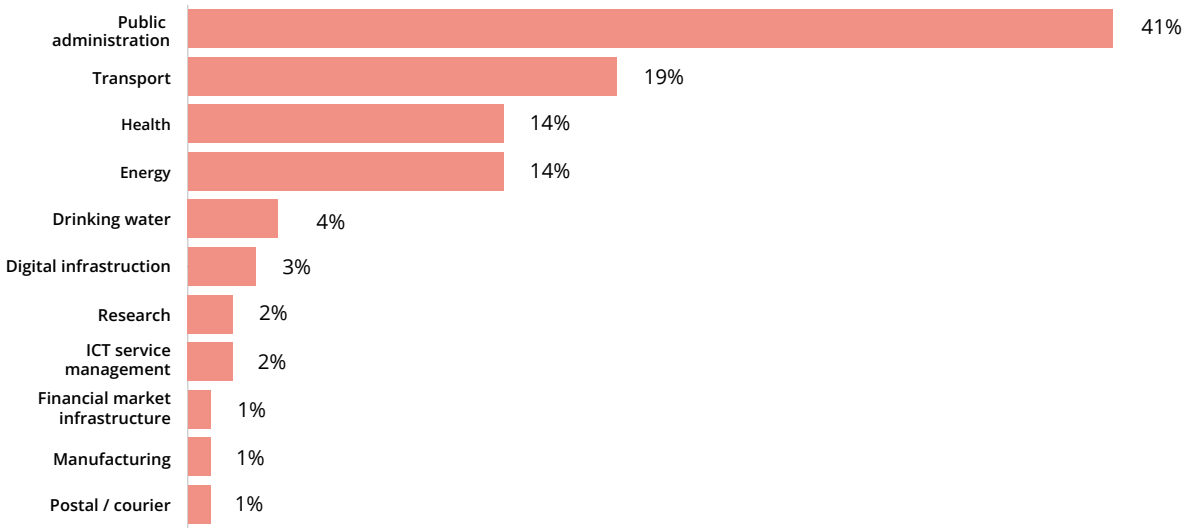


Figure 1. *Services delivered in 2025 per service type*



NB: *The split per sector is presented for ex ante / preparedness services only, as the ex post services are cross-sectors.*

Figure 2. *Ex ante / preparedness services delivered in 2025 per sector*

The key lessons identified during 2025 that will guide future implementation pertain to this activity's close links with the developments under the EU-CyCLONe group and the blueprint for cyber crisis cooperation. In this context, it is important to closely follow the developments under EU-CyCLONe and seek regular feedback from the group.

Another key lesson concerns how the activity is depicted within the agency's SPD. Specifically, in order to better reflect the overall service delivery framework, the activity's outputs could be restructured according to the following three distinct outputs:

- service delivery, that is, the operationalisation of the reserve for the provision of incident response support services and conversion services in case of unused pre-committed incident response resources for Member States and EU entities;
- administration of the reserve, involving all necessary functions and services to support service delivery and ensure service quality, such as development and maintenance of the service catalogue, procurement activities, the project management office, the assessment framework and the mapping of services;
- service delivery to DEP-associated non-EU countries, that is, delivery of incident response support services or conversion services to DEP-associated non-EU countries in accordance with Article 14(2)(c) of the CSOA, given the specific nature of and eligibility criteria for users from these countries.

In terms of resources, Activity 6 has four FTEs from ENISA's establishment plan, while the majority of the activity's resources are contract agents (CAs) funded via the respective contribution agreements. This poses two challenges: contracts are limited to CA grades, which makes it challenging to recruit senior-level expertise/staff, although the nature of the tasks required to be performed are of a sensitive nature and require appropriate seniority. However, the temporary nature of these contracts, tied to the contribution agreement implementation period, provides less stability to staff, resulting in higher staff turnover rates and in turn leading to a lot of time being spent onboarding and offboarding team members. This indicates the need for more permanent, rather than temporary, resources to ensure some level of team stability and minimise the impact on service delivery.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Effective EU preparedness and response to cyber incidents, threats and cyber crises	• Operationalisation of the EU Cybersecurity Reserve of which the administration and operation is to be entrusted fully or partly to ENISA and used by Member States, EUIBAs and on a case-by-case basis by DEP-associated non-EU countries

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET
By the end of Q2 2026, deliver and complete ENISA support actions.	CSA, Articles 6 and 7	2026	Ability of ENISA to support Member States to further develop preparedness and response capabilities through implementation and delivery of *ex ante* and *ex post* services delivery (survey). Complete tasks on time and within budget (survey).	4 (1–5 scale)
By the end of Q2 2026 and onwards, deploy the EU Cyber Reserve as per the CSOA.	CSA, Articles 6 and 7	2026	Reaching consensus with the European Commission on the EU Cyber Reserve (survey). Timely delivery (survey).	4 (1–5 scale)

OUTPUTS	OUTCOME
6.1. Provide penetration testing and threat-hunting services for selected entities within Member States [18].	In 2025, ENISA refined the Output 6.1 service catalogue, including: • infrastructure weaknesses analysis; • adversarial tactics and techniques simulation; • threat hunting (new). 175 services were requested in 2025, of which 116 have already been delivered, with the remaining services ongoing in 2026. These services were requested by 21 Member States, reflecting broad uptake and sustained demand across the EU.
6.2. Provide customised exercises and training for selected entities within Member States.	In 2025, ENISA refined the Output 6.2 service catalogue, including: • training (bespoke training, awareness raising (AR in a box), self-paced platform-based online training); • exercises (cyber exercises, cyber defence skills validation (red and blue team exercises)). Some 82 (15 training and 67 exercise) services were requested from 16 Member States during 2025, of which 31 (5 and 26, respectively) were delivered in 2025, with 29 (5 and 24, respectively) services ongoing. These services were delivered to 9 Member States, reflecting consistent demand for capacity-building services across the EU. All 27 Member States agreed to use the self-paced online training platform offered by ENISA. In 2025, 165 learners from 11 Member States were registered on the platform.
6.3. Support risk monitoring and assessment for selected entities within Member States.	In 2025, ENISA refined the Output 6.3 service catalogue, including: • the threat landscape and risk scenarios (rescoped); • risk monitoring (rescoped); • organisational risk assessment (new); • incident response and crisis management plan development (new); • cybersecurity maturity and capabilities assessment (rescoped); • NIS 2 gap analysis and compliance advisory (new).

[18] The beneficiaries of Activity 5 services are specified in the contribution agreement.

	45 services were requested in 2025, of which 32 have already been delivered, with the remaining services currently ongoing. These services were requested by 13 Member States. The revised catalogue, supporting Objective 6.3, consistently complements the most in-demand services while addressing Member States' newly emerging needs. **Some highlights from 2025 are outlined below.** • Two Member States entrusted ENISA and the support action programme with the development or revision of their national cyber crisis management plans, while two additional Member States utilised the service catalogue to design new incident response playbooks for critical sectors. • Five risk-monitoring services were deployed for governmental computer emergency response teams to address emerging operational needs, including cyber threat intelligence, external attack surface management and supply chain exposure analysis. • In the context of transposing the NIS 2 Directive, eight NIS 2 gap analysis and compliance advisory services were delivered to support five Member States address the new regulatory requirements.
6.4. Support incident response and incident management for selected entities within Member States.	In 2025, ENISA refined the Output 6.4 service catalogue, including the following full spectrum of incident response subservices: • information security incident analysis • artefact and forensic evidence analysis • cybersecurity incident response • cybersecurity incident coordination • cybersecurity incident initial recovery • incident-handling capability development • customised incident response playbook development. The incident-reporting retainer service was enabled to all 27 Member States and to one DEP-associated non-EU country (Moldova[19]). Numerous incident-reporting activation exercises were conducted throughout the year. Also, four incident-reporting activation requests were successfully supported in 2025.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
6.1. Provide penetration testing and threat-hunting services for selected entities within Member States [20].	Penetration testing and threat-hunting services are delivered in a timely and accurate manner to Member States.	Beneficiaries Directorate-General for Communications Networks, Content and Technology Member States	Percentage of Member States requesting the service. Satisfaction score.	Annual	50 % > 4	82 % requested services (22 out of 27 Member States). Overall satisfaction score of 4.65.
6.2. Provide customised exercises and training for selected entities within Member States.	Customised exercise and training services are delivered in a timely and accurate manner to Member States.	Beneficiaries Directorate-General for Communications Networks, Content and Technology Member States	Percentage of Member States requesting the service. Satisfaction score.		50 % > 4	100 % requested. Overall satisfaction score of 4.

(19) Exceptional Negotiated Procedure ENISA D-OSU-25-T11 (PPMT Ref: ENISA/2025/NP/0006) "Supporting ENISA for the provision of cybersecurity services to Moldova and Ukraine":
Following the extremely urgent need for Ukraine and Moldova to receive support from the EU Cybersecurity Reserve in responding to emerging cybersecurity incidents, the contracting authority decided to proceed with an exceptional negotiated procurement procedure, in accordance with point 11(1)(c) of Annex I to the Financial Regulation. This procedure was necessary to provide the required support without delay, as otherwise ENISA would not have been able to meet the standard time limits prescribed by the Financial Regulation combined with the need to conduct Ownership Control Assessments (OCAs) for service providers. Without a negotiated procedure, ENISA would not have been able to provide timely support despite the urgent need. It is noted that especially for Moldova the incident response support was highly required in connection with the elections held in September 2025.

(20) The beneficiaries of Activity 5 services are specified in the contribution agreement.

6.3. Support risk monitoring and assessment for selected entities within Member States.	ENISA provides regular risk monitoring of specific targets or at the national level, including by leveraging commercial off-the-shelf platforms, as well as providing specific risk assessment and threat landscapes as requested by Member States.	Directorate-General for Communications Networks, Content and Technology Member States Other beneficiaries	Percentage of Member States requesting the service. Satisfaction score.		50 % > 4	48 % requested. Overall satisfaction score of 4.3.
6.4. Support incident response and incident management for selected entities within Member States.	ENISA provides 24/7 incident-response support to Member States.	Directorate-General for Communications Networks, Content and Technology Member States Other beneficiaries	Percentage of Member States requesting the service. Support provided in a timely manner. Satisfaction score.		50 % > 4	100 % requested. Overall satisfaction score of 5.0.

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. European Commission, Member States and selected beneficiary entities.

Involve/engage. EU-CyCLONe, the CSIRT network and the Directorate-General for Communications Networks, Content and Technology.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	4	**NUMBER OF FTES ACTUALLY USED** [21]	3.5 [22]
PLANNED BUDGET (EUR)	N/A	**BUDGET CONSUMED (EUR)**	N/A
AMENDED BUDGET (EUR)		**OF WHICH CARRIED OVER TO 2026 (EUR)**	N/A

NB: The table above refers to the EU subsidy budget and FTEs. For the budget and FTEs from contribution agreements, please see Annex VI.

[21] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

[22] Nine FTEs used in this activity were funded by the cooperation agreement that funds the Cybersecurity Reserve activities.

ACTIVITY 7

Supporting the development and maintenance of the EU cybersecurity certification framework

Activity 7 is responsible for the implementation of Title 3 of the CSA, namely supporting the development and maintenance of the EU cybersecurity certification framework. The aim of the activity is to build trust in secure digital solutions by developing and maintaining EU cybersecurity certification schemes. The agency is conducting efforts in the field with the support and collaboration of the European Commission; Member States (in particular national cybersecurity certification authorities (NCCAs)); national accreditation bodies and their coordination organisation European Accreditation; and the private-sector bodies, both those providing solutions to be certified and those providing evaluation and certification activities (conformity assessment bodies). Community engagement, stakeholder participation and the transparency of the agency's actions remain a priority, with the most relevant information and consultations taking place via the ENISA certification website. Moreover, in 2025, ENISA took over the stakeholders' service platform, the Connecting Europe Facility (CEF), from the European Commission. The platform is used for collaboration, publication and the promotion of the cybersecurity certification framework's implementation.

Outlined below are the key accomplishments of the activity in 2025.

- In 2025, ENISA received a new request from the European Commission to draft a cybersecurity certification scheme for managed security services (the European Union cybersecurity certification for managed security services (EUMSS)). Accordingly, ENISA established an AHWG and commenced the drafting, taking due consideration of relevant standards, technical specifications and national initiatives and schemes. It should be noted that ENISA conducted a feasibility study prior to the request for the scheme and said study fed into the request itself. Moreover, the agency continued drafting the candidate scheme for the EU Digital Identity Wallet (EUDIW) in close cooperation with the established ENISA AHWG and the Electronic Identification CG. In parallel, ENISA supported the drafting of national certification schemes for digital identity wallets, a stream of work for which in 2026 a contribution agreement will be granted to the agency to strengthen its efforts for a duration of two years.

- 2025 saw the second amendment of the act implementing the EU cybersecurity certification scheme on common criteria (EUCC) and the continuation of EUCC maintenance activities, both in the context of

the relevant ISAC and the dedicated European Cybersecurity Certification Group (ECCG) subgroup. The EUCC scheme has reached new levels of maturity, with 24 conformity assessment bodies notified in the course of 2025 (16 IT security evaluation facilities and 8 certification bodies) and 16 certificates published on the ENISA certification website. The arduous tasks of supporting the EUCC maintenance work via inter alia the maintenance of up-to-date state-of-the-art documents is an effort that deserves to be underlined.

- ENISA finalised the candidate EU 5G network equipment security assurance scheme (EU5G NESAS) cybersecurity certification scheme and submitted it to the European Commission, whereas work on the EU Cloud Certificaiton Scheme (EUCS) did not see any progress in 2025. In addition, via a contribution agreement and a request from the European Commission, ENISA built on the successful publication of the EUCC–CRA interplay study, by conducting dedicated pilot studies to identify potential needs to establish presumption of conformity for the CRA based on the EUCC.

Activity 7 contributes to the effective implementation of the CSA and in particular the European cybersecurity certification framework (ECCF) in close cooperation with European Commission and Member States, whereas additional policy files related to the activity's scope of work involve the CRA (and therein the alignment of the conformity assessment regimes between the CSA and CRA), the European digital identity (EUDI) framework (for the EUDIW draft candidate scheme) and the NIS 2 Directive (for the draft EUMSS candidate scheme). To ensure harmonised implementation of the framework, ENISA contributed to the definition, piloting and adoption of the NCCAs' peer review mechanism, which will start being used in 2026 with ENISA support (including guidelines and templates), capacity-building actions for NCCAs, and coordination and guidance related to planning.

The significance of the conformity assessment ecosystem in the success and uptake of both the ECCF and the CRA cannot be understated, since said ecosystem is fundamental for ensuring that certification schemes are implemented in practice and evaluations are performed in a consistent and harmonised manner, an element that applies to the CRA as well.

Throughout 2025, ENISA worked closely with European Commission and Member States (mainly NCCAs) via established bodies, such as the ECCG, to support the implementation of the ECCG, and industry via the Stakeholder Cybersecurity Certification Group (SCCG). Together, ENISA contributed to the organisation of various events, notably the European Certification Week in April 2025. In addition, ENISA delivered – with the support of the ecosystem (e.g. NCCAs, national accreditation bodies, conformity assessment bodies, developers of solutions) – the first magazine fully dedicated to European certification.

The work of the activity spans different dimensions, from technical expertise and guidance in support of certification schemes (e.g. the competence to develop technical standards on security measures and evaluation methods, feasibility studies, state-of-the-art documents and technical guidelines) to industry-wide matters, such as cryptography (the major highlight of the work involves the approved cryptographic mechanisms document accepted by the ECCG Subgroup and contributions delivered to the EU post quantum computing roadmap), and lastly to international cooperation to promote mutual recognition, notably in the context of the EUCC.

In 2026, focus and priority will be on delivering two initial versions of candidate schemes, namely the EUDIW and EUMSS. Furthermore, the agency will promote the uptake of the ECCF, showcasing its value and potential to promote assurance and trust in the EU cybersecurity ecosystem and EU competitiveness in general. In doing so, a key priority of the agency is to strengthen its ties to the 27 NCCAs and establish regular dialogues with all of them.

Presented below are the key lessons identified during 2025 that will guide future implementation.

The need to structure service provisioning and delivery in a more scalable and sustainable manner is evident given that the tasks associated with maintaining certification schemes are becoming more prominent and considering how the activity operated in a scheme-centred manner 2025. This will necessitate the long-term planning of service tasks and resource prioritisation in order to handle the diverse requirements in competences and expertise required by the different in-force, ongoing and prospective draft candidate schemes.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Building trust in secure digital solutions	• The number of EU certification schemes developed and maintained, the number of EU regulations making reference to the CSA and the number of active Member States' NCCAs (e.g. issuing European certificates)

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET
Between 2025 and 2027, the timely development of feasibility studies for future potential schemas.	CSA, Article 49	2027	Number of feasibility studies concluded in view of upcoming requests, including managed security services (ongoing).	3 (pending potential new requests for schemes).
			Elements of feasibility study reflected/aligned with the. European Commission's request for new schemes.	More than 50 %
Between 2025 and 2027, the timely finalisation of candidate schemes following formal requests for drafting new cybersecurity certification schemas.	CSA, Article 49	2027	Number of drafts of certification schemas delivered to the European Commission (EUIDW certification and, pending formal COM request, EUMSS).	2
			ECCG endorsement of draft certification schemes.	Positive ECCG endorsement.
			SCCG opinion on draft certification schemes (satisfaction survey).	More than 60 %

Ensure the maintenance of existing schemes and support their roll-out.	CSA, Article 49	2027	Number of schemes maintained with active ENISA involvement.	1 (EUCC) and EUCS, pending final approval.
			Satisfaction of ECCG with ENISA's support for maintenance documents.	75 %
			Number of certificates issued and published under an EU certification scheme; high rate of use in the market.	Proportionate [23] number of certificates issued migrating to a new EUCC scheme compared with previous framework.

OUTPUTS	OUTCOME
7.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes.	**In 2025, ENISA achieved the following.** • Completed the EUMSS feasibility study. • Received a request for a draft candidate cybersecurity certification scheme on managed security services (EUMSS); established an AHWG on EUMSS; and agreed a certification strategy with the European Commission and Member States, with the aim of delivering the scheme in 2026. • Continued working on the draft candidate cybersecurity certification scheme for EUDIW and delivered the first draft. The template for national certification schemes was delivered for review and a dedicated contribution agreement with the European Commission will be granted to ENISA in 2026 to further support the Member States. The work involved standardisation gap analysis, security requirements for the EUDIW and other work on technical specifications. • Finalised the EU5G NESAS in the EU5G AHWG in December 2025. • Published a dedicated study on certification uptake in December 2025 [24]. • Organised European Certification Week together with the Polish Presidency in April 2025, with two additional Cybersecurity Certification Weeks taking place in 2025.
7.2. Implementation and maintenance of established schemes, including evaluation of adopted schemes, participation in peer reviews etc., and monitoring the dependencies and vulnerabilities of ICT products and services.	**In 2025, ENISA achieved the following.** • Completed the second EUCC implementing regulation amendment in 2025, with 11 state-of-the-art documents updated and drafted in the year. ENISA continued stakeholder engagement and technically advising and supporting the EsEm ISAC (EUCC maintenance) and providing guidance and supporting uptake of the ecosystem. • Published the EUCC–CRA interplay study to analyse the presumption of conformity interplay between the two pieces of legislations. Dedicated webinars, with more than 2 000 participants, were conducted. • Received a contribution agreement based on a European Commission request to conduct pilot studies to identify potential needs for the presumption of conformity of the EUCC to the CRA. • Participated as an observer in a pilot NCCA peer review, which led to the agency's role becoming concrete for the upcoming 2026 peer reviews with the publication of the relevant European Commission implementing regulation.

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

[24] https://www.enisa.europa.eu/publications/voices-of-eu-cybersecurity-certification.

7.3. Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks.	**In 2025, ENISA:** • continued actively participating and engaging with ECCG; • organised a meeting of the SCCG in May 2025; • managed the secretariat for the ECCG subgroup on cryptography (five meetings held in 2025).
7.4. Developing and maintaining the necessary provisions, tools and services concerning the ECCF (including the certification website and supporting the Commission in relation to the core stakeholders service platform, CEF, for the collaboration, publication and promotion of the implementation of the cybersecurity certification framework etc.).	**In 2025, ENISA achieved the following.** • Continued actively publishing articles, guidance and news about the ECCF on the certification website. • Reinforced the annual hybrid conference by renaming it the European Cybersecurity Certification Conference and organising it within the Polish Presidency. Some 200 participants attended on site and close to 1 000 attended online. • Continued the promotion of the ECCF to major key communities and held specialised events to this end. • Successfully onboarded the CEF platform for the European Commission. • Ported all certification websites to the EC DIGIT infrastructure to promote resilience, and consolidate and streamline delivery.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
7.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes.	Scheme meets stakeholder requirements, notably those of the Commission and Member States.	AHWGs on certification ECCG European Commission	Number of opinions of stakeholders managed.	Annual (report)	100 opinion items per scheme.	370 opinions of stakeholders managed for the EU5G NESAS draft candidate scheme.
	Take-up of schemes by stakeholders. Timely delivery by ENISA of all schemes requested in cooperation with the Commission. Statutory bodies and AHWGs actively involved.		Number of people or organisations engaged in the preparation of certification schemes.	Annual (report)	At least 20 AHWG members from third-party experts; at least 15 Member States joining AHWGs.	25 experts in EUDIW AHWG. 23 Member States in EUDIW AHWG. 30 experts in EUMSS AHWG. 22 Member States in EUMSS AHWG.

7.2. Implementation and maintenance of established schemes, including evaluation of adopted schemes, participation in peer reviews etc., and monitoring the dependencies and vulnerabilities of ICT products and services.	Review schemes to improve efficiency and effectiveness. Take-up of schemes by stakeholders.	ECCG European Commission	ECCG's satisfaction with ENISA's efforts on schemes adopted.	Triennial (survey)	75 %	To be assessed in 2027.
			Satisfaction with ENISA's role in NCCA peer reviews.	Triennial (survey)	75 %	To be assessed in 2027.
7.3. Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks.		ECCG European Commission SCCG	Feedback from statutory bodies, including NCCAs, on ENISA's role.	Annual (survey)	75 %	Rescheduled to 2027
7.4. Developing and maintaining the necessary provisions, tools and services concerning the ECCF (including the certification website and supporting the Commission in relation to the core stakeholders service platform, CEF, for collaboration, publication and promotion of the implementation of the cybersecurity certification framework etc.).	Transparency and trust in supporting ICT products, services and processes. Stakeholder engagement in promotion of certification.	ECCG European Commission SCCG	User satisfaction with the services on the certification website.	Annual (survey)	75 %	Rescheduled to 2027
			Use of the certification website.	Annual (report)	75 %	Rescheduled to 2027

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. European Commission, Member States (including NCCAs, the ECCG), EUIBAs and selected stakeholders, as represented in the SCCG.
Involve/engage. Private-sector stakeholders with an interest in cybersecurity certification, conformity assessment bodies, national accreditation bodies and consumer organisations.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	10	**NUMBER OF FTES ACTUALLY USED [25]**	7.8
PLANNED BUDGET (EUR)	582 188.15	**BUDGET CONSUMED (EUR)**	619 170.41
AMENDED BUDGET (EUR)	620 054.41	**OF WHICH CARRIED OVER TO 2026 (EUR)**	120 792.50

[25] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

ACTIVITY 8

Supporting the European cybersecurity market, research and development, and industry

Activity 8 consolidated ENISA's efforts on promoting cybersecurity in the EU market and industry. The activity aimed to promote good cybersecurity practices for security-by-design and security-by-default, monitor and analyse cybersecurity market trends, support effective and impactful decision-making, guide relevant actions, understand and, via collaboration with the European Cybersecurity Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs). In addition, the action also aimed to support research and innovation (R & I) programmes in cybersecurity in the EU and promote and contribute to cybersecurity standardisation activities. ENISA's strategic objective with Activity 8 entails building trust in secure digital solutions and looking ahead to emerging and future cybersecurity opportunities and challenges.

Activity 8 contributed to the implementation of the CRA in close cooperation with the European Commission and Member States, whereas additional policy files related to the activity's scope of work involve the ECCC Regulation, the AI Act, the Data Governance Act, the EUDI framework (eIDAS2) and the General Data Protection Regulation.

The activity built upon ENISA's understanding of cybersecurity market dynamics from both the demand and supply sides (Output 8.2) and identified emerging and future cybersecurity trends (Output 8.3) to enable informed decision-making about product security engineering, thus supporting implementation of the CRA. In addition, this work also provided technical guidance on software and hardware security (Output 8.3). In doing so, the work on cybersecurity standardisation underpins relevant efforts by providing solid baselines for harmonisation (Output 8.4).

Outlined below are the key accomplishments of the activity in 2025.

- Revised its market analysis framework. The updated ENISA cybersecurity market analysis framework is more responsive to constraints and is more concise, targeted, flexible and fit for purpose. The revised methodology will be applied in 2026 across the categories of products identified in the CRA's annexes. As part of this revision, ENISA identified the need to expand its community engagement to better understand the cybersecurity market in the EU. Accordingly, the agency engaged and liaised with the ECCC and NCCs to ensure their participation and formed an AHWG on the cybersecurity market to steer and validate future work.
- Developed a technology and innovation radar methodology (Output 8.1), building

on ENISA's solid foresight methodology and experience, to assess the maturity of technological developments and identify weak/strong signals of emerging opportunities and threats in order to proactively contribute with pertinent technical advice. The technology and innovation radar became operational in 2026.

- Worked closely with the European Commission and Member States (mainly CRA-designated market surveillance authorities) via established bodies, such as the CRA Expert Group, in support of the implementation of the CRA. The area of product security engineering was established, entailing coming up with a method and delivering the first-of-its-kind technical advisory on software package managers. ENISA also delivered fundamental work on security bill of materials (SBOMs) and security-by-design, providing technical input throughout the year to various strands of the CRA Expert Group. ENISA also received a new role (by means of a contributions agreement) on cybersecurity standardisation by supporting the European Commission on assessing 41 harmonised standards. Thus, the agency moved to a more active role in supporting regulation. Furthermore, in the scope of the new EU standardisation challenges, ENISA called for an AHWG on standardisation, requesting market actors, standardisation bodies and Member States to participate.

Presented below are the key lessons identified during 2025 that will guide future implementation.

- Prioritise actions and levels of engagement. The work of the activity spans different dimensions – from product security and supporting CRA implementation, to ECCC relations, data protection, the EUDI framework and the Data Governance and AI Acts. Given the diversity of topics and limited resources, prioritisation is necessary.

- Further consolidate the different workstreams to support Member States' implementation of the CRA. As evidenced by the endorsed outputs in the SPD, the focus in 2025 was on the CRA, product security, the market and standardisation. 2025 was the first year that ENISA systematically addressed product security, and the agency's maturity grows in tandem with that of the European Commission and the Member States as they move towards full CRA enforcement. In 2026, further consolidation of the different workstreams will continue, providing value-added services to market surveillance authorities, industry and manufacturers, while promoting ENISA as a technical centre of expertise for product security engineering.

- Conformity assessment ecosystem.The conformity assessment ecosystem is a significant part of the success and uptake of the CRA; however, the ECCF is another element that rose in prominence in 2025, and its importance will intensify in 2026 and beyond. Said ecosystem is fundamental for ensuring that the CRA conformity assessment is implemented and that evaluations are performed in a consistent and harmonised manner.

- Develop competences. As became evident in 2025, this activity requires new sets of competences in terms of technical expertise due to the prioritisation of the work to support CRA implementation, the strategic significance of which necessitated the commitment and reshuffling of resources to address emerging relevant tasks, such as providing technical guidance and product security, and supporting the work on standardisation and conformity assessment. The criticality of CRA implementation will only increase in 2026 as the due date for the CRA coming into force inches closer; thus, efforts will intensify in building on and developing further relevant competences and resources in order to meet expectations in fast-paced fields, such as product and technology security.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
• Empowered communities in an involved and engaged cyber ecosystem • Building trust in secure digital solutions • Foresight on emerging and future cybersecurity opportunities and challenges	• Rate of satisfaction with ENISA's support for the implementation of the CRA (among market supervisory authorities) and the ECCF (among the ECCG), the number of advisories and the level of support given to R & I needs and priorities for the ECCC and its uptake by the ECCC

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIME FRAME OF OBJECTIVE	INDICATOR	TARGET
By the end of 2026, implement a market monitoring and analysis framework that delivers ad hoc as well as relevant and regular reports on the trustworthiness of critical products and services with digital elements under the CRA.	CRA	2026	Timeliness of ENISA reports.	Reports delivered on time.
			Acceptance of ENISA reports by Member States.	Two thirds of Member States endorse ENISA reports.
			Validity of ENISA framework.	All Member States validate and endorse ENISA's framework.
Provide continuous comprehensive support to Member States' market supervisory authorities and to the COM for implementing CRA requirements.	CRA	2026	Member States 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.	CRA CSA, Article 9	2026	Number of cybersecurity trends and patterns accurately identified through an evidence-based methodological approach.	5 % increase over reference data.
			Assessment of impact of EU cybersecurity R & I.	5 % increase over reference data.

OUTPUTS	OUTCOME
8.1. Collect and analyse information on new and emerging ICT, and provide strategic advice to the ECCC on the EU agenda on cybersecurity research, innovation and deployment.	**In 2025, ENISA achieved the following.** • Established a technology and innovation radar for emerging cybersecurity trends and in doing so, a methodology for filtering trends and signals from emerging technologies was delivered and validated by NLOs and the ENISA Advisory Group. • Built on 2024 work and the relevant framework and worked on an assessment of cybersecurity R & I actions to complement the efforts of the NIS 2 Directive Article 18 report (the *State of Cybersecurity in the Union*) and provide strategic input to the ECCC and NCCs. • Developed and delivered a value proposition toolbox to empower NCCs to better articulate their services and engage with their communities. • Hosted Cyber EUnnovate 2025 in September, a unique ENISA hybrid event focused on AI, post-quantum computing and semiconductors that gathered over 270 participants from EU institutions, national authorities, research and industry. Some 94 % of attendees rated the event as 'excellent' or 'very good'. • Continued maintaining the successful Data Protection Engineering AHWG and conducted webinars focused on the engineering for personal data protection in the AI era and PQC.

8.2. Conduct market analysis of the main trends in the cybersecurity market on both the demand and supply sides, and evaluations of certified products, services and processes; prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements.	**In 2025, ENISA achieved the following.** • Delivered the third update of the ENISA cybersecurity market analysis framework, which was completed and validated by the NLOs and the advisory group. It offers a more streamlined, user-friendly approach (e.g. by introducing reusable templates) to facilitate and expediate market analyses, while additionally it supports the recurrence of analyses and continuous market monitoring. • Held the ENISA CRA Conference 2025 in October, a large-scale event (attended by over 500 people) that brought together stakeholders across the entire spectrum of products with digital elements available on the EU single market. • Conducted a comprehensive analysis of the competences needed by notified bodies under the CRA, having identified the significance of proactively setting up a vibrant and established conformity assessment community for CRA effective enforcement. Together with the European Commission, the agency is in close collaboration with relevant notifying authorities, accreditation bodies and conformity assessment bodies. • Established an AHWG on the cybersecurity market (launched in Q1 2026).
8.3. Support the activities of market surveillance authorities and the identification of categories of products for simultaneous coordinated control actions and, upon request, conduct evaluations of products that present a significant cybersecurity risk.	**In 2025, ENISA achieved the following.** • Supported, through giving technical advice and input, the European Commission, the CRA Expert Group and the Member States' market surveillance authorities on various topics related to CRA implementation, such as security-by-design, defining a catalogue of categories of products, remote data processing, SBOMs, support for small and medium-sized enterprises (SMEs) and regulatory sandboxes, to name but a few. • Actively contributed to all key COM guidance on the CRA. • Published for public consultation in December a state of SBOM in the Member States study in close collaboration with Member States, focusing on technical aspects related to SBOM. • Together with the European Commission, commenced working on a CRA SME roadmap, focusing on aspects such as raising awareness, providing simplified guidelines and promoting higher levels of maturity. • Actively contributed to all three CRA Expert Group meetings held in 2025 and the informal meeting held in November 2025. • Established the area of product security engineering. The agency developed a method and delivered the first technical advisory of its kind on software package managers in November 2025 and attract stakeholder communities. • Worked closely with several DEP-funded projects on CRA implementation and delivered numerous presentations on the topic.
8.4. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification.	**In 2025, ENISA achieved the following:** • At the European Commission's request (via a contribution agreement), supported the CRA standards review (41 standards), a key support activity that highlights the importance of the role the agency plays in cybersecurity standardisation; • In March, jointly held the ninth Cybersecurity Standardisation Conference, a large-scale event (with over 2 500 registrations), gathering policymakers and experts in cybersecurity standardisation from EU and Member State institutions, European standardisation organisations, industry and associations; • In September, held the 11th Trust Services and Electronic Identification Forum, a large-scale event (with over 1 000 participants) that has become the place to be for stakeholders in the eIDAS Regulation, collocated with other events in the field; • Developed the landscape exploration for norms and standards framework and the first pilot report of the cybersecurity standards observatory, which entered into the production phase in Q1 2026.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
8.1. Collect and analyse information on new and emerging ICT, and provide strategic advice to the ECCC on the EU agenda on cybersecurity research, innovation and deployment.	Identifying current and emerging ICT gaps, trends, opportunities and threats. Advising EU funding programmes, including the ECCC and its strategic agenda and action plan.	Academia Entities, including NCCs and EUIBAs European Commission, including the Directorate-General for Communications Networks, Content and Technology and the Joint Research Centre (JRC) and the ECCC as appropriate Industry Member States' market authorities National R & I	Findings endorsed by Member States (NCCs and market authorities).	Annual	> 60 %	No updates in 2025 on the ECCC strategic agenda and action plan.
			Alignment with the ECCC strategic agenda and action plan.	Annual (survey with ECCC)	> 60 %	No updates in 2025 on the ECCC strategic agenda and action plan.
8.2. Conduct market analysis of the main trends in the cybersecurity market on both the demand and supply sides, and evaluations of certified products, services and processes; prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements.	Improved understanding of the market and industry.	Advisory group AHWGs for cybersecurity market analysis ECCG (as necessary) Member States' market authorities NLO (as necessary) SCCG	Cybersecurity market analysis; cybersecurity products and services.	Annual (report)	All reports produced as planned (Y out of Y reports).	1 ENISA cybersecurity market analysis framework (version 3) completed and validated by NLO and the advisory group.

			Member States' endorsement of the report on emerging trends regarding cybersecurity risks in products with digital elements.	Biennial (report)	27 Member States endorse report.	First report expected in 2028 as per the CRA.
8.3. Support the activities of market surveillance authorities and the identification of categories of products for simultaneous coordinated control actions and, upon request, conduct evaluations of products that present a significant cybersecurity risk.	Produce a catalogue of market surveillance authorities; survey market surveillance authorities' requirements; identify categories of products; produce a methodology on market sweeps; carry out market sweeps. Evaluations to be carried out ideally on the basis of input from market sweeps; rely on external expertise.	European Commission NLO/NCCA SCCG (as appropriate)	Collection of requirements. Matching requirements with deliverables. Time to carry out market sweeps. Methodology for evaluations. Profiles of experts.	Catalogue, survey and categories of products in 2025–2026. Market sweeps as from 2027 (3-year transition) or earlier if requested. Method to evaluate products. Guidance and criteria to accept evaluation results.	Stake-holder satis-faction above 60 %	The CRA enters into force in December 2027, hence criteria cannot be assessed.
8.4 Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification.	Alignment with standards.	Advisory group NLO (as necessary) SCCG	Reports on analysis of standardisation aspects on cybersecurity, including cybersecurity certification.	Annual (report)	All reports produced as planned (Y out of Y reports).	1/1 ENISA cybersecurity standardisation repository report completed. Report to be published in 2026.

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. European Commission; Member States, including market authorities and entities with an interest in cybersecurity market monitoring (e.g. NCCAs, national standardisation organisations); EUIBAs; European standardisation organisations (European Committee for Standardisation, European Committee for Electronical Standardisation, the European Telecommunications Standards Institute); private sectår or ad hoc standards-setting organisations; the JRC; national and EU R & I entities; academia; industry; the ECCC; and national cybersecurity coordination centres.

Involve/engage. Private-sector stakeholders (entrepreneurs, start-ups, investors) with an interest in the cybersecurity market and/or standardisation, the International Organization for Standardization, the International Electrotechnical Committee and consumer organisations.

ALLOCATED FULL-TIME EQUIVALENTS (FTES) BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	12	**NUMBER OF FTES ACTUALLY USED** [26]	8.2
PLANNED BUDGET (EUR)	575 786.30	**BUDGET CONSUMED (EUR)**	585 427.65
AMENDED BUDGET (EUR)	585 427.65	**OF WHICH CARRIED OVER TO 2026 (EUR)**	81 708.00

[26] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

ACTIVITY 9

Performance and sustainability

Activity 9 sought to improve ENISA's organisational performance, risk management and compliance with the applicable regulatory framework. The work undertaken within this activity was based on Article 4(1) of the CSA, which sets an objective for the agency to:

> *be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.*

In addition, in line with Article 4(2) of the CSA, this activity contributed to efficiency gains, for example, via shared services with the EU Agencies Network (EUAN) and in key areas of the agency's expertise. As part of this activity, ENISA pursued key objectives of the corporate strategy (to be a service-centric and sustainable organisation), including by establishing an efficient quality assessment framework, ensuring proper and functioning internal controls and compliance checks, and maintaining a high level of cybersecurity across all of the agency's corporate and operational activities. In terms of resource management, the Budget Management Committee ensured that the agency adheres to sound financial management. In the area of IT systems and services, the IT Management Committee (ITMC) oversaw and monitored the comprehensive application of the agency's IT strategy and relevant policies alike.

Outlined below are the key accomplishments of the activity in 2025.

- Developed and resourced a cybersecurity maturity plan for 2025–2028 that will further advance and strengthen the agency's cybersecurity position in view of the new responsibilities entrusted to ENISA under the CRA and the European Commission's proposals on the digital omnibus and the revision of the CSA.

- Chaired EUAN, including leading the EUAN Steering Board and its various subnetworks, coordinating the heads of agencies, heads of resources and the Accounting Officers Network. As chair, ENISA represented EUAN before interinstitutional partners, and hosted multiple events in support of EUAN activities. During this term in office, ENISA pursued cybersecurity as a key theme to give agencies a new impetus in their cooperation, learning and service delivery to improve their position. As a hands-on cybersecurity agency, up to one FTE was availed as a shared service for the purpose of elevating cybersecurity within the EU's institutions and agencies. This approach complemented ENISA's drive for cost-effective services across cybersecurity, human resources

and legal services, so that greater capacity could be built at a fraction of the cost of employing a full FTE. As a trusted institutional partner to the Commission, ENISA, acting on behalf of the agencies, delivered the agency's choice for the chief confidential counsellor service as proposed by the Commission.

- Strengthened the performance management framework via coordinated management of the internal legal production, simplified risk management procedures and put in place a new anti-fraud management framework.

Presented below are the key lessons identified during 2025 that will guide future implementation.

- Address the emerging and urgent priority of developing an AI policy and action plan to meet the agency's operational and corporate needs.
- Continue close coordination and monitoring of the cybersecurity maturity plan, in particular to ensure that adequate (human and financial) resources are available or proceed with re-prioritisation in the absence of these resources.
- Examine in depth certain internal controls areas, in particular the management of conflict of interest. Scrutinise budget and project management with regards to contribution agreements.
- Monitor the slightly higher number of complaints from an internal control and a legal standpoint. In view of its growth in appropriations and perceived influence in terms of cybersecurity policy, ENISA is likely to receive more attention of applicants and complainants alike, and a proportionate response needs to be provided in the interest of the service.

GENERAL ACTIVITY OBJECTIVES	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	TARGET	2025 RESULTS
9A. Enhance corporate performance and strategic planning.	Ensure efficient corporate services.	Proportion of SPD KPIs meeting targets.	Annual	> 80 of indicators overperformed.	155 indicators of which 75% above target 10% below target 10% postponed / rescheduled for 2027 5% discontinued or N/A
	Continuous innovation and service excellence.	Results of assessment of internal control framework.	Annual	Effective level 1 or 2 (Scale 1 – 4, with 1 being the highest)	Assessed as category level 2 - The Internal Control provides reasonable assurance that policies, processes, tasks, behaviours of the agency facilitate its effective and efficient operation
	Develop service propositions with additional external resourcing.	High satisfaction with essential corporate services in the areas of compliance and coordination.	Annual	> 60 %	> 63 %

9B. Increase corporate sustainability.	Ensure ENISA is climate neutral by 2030.	Maintain EU eco-management and audit scheme (EMAS).	Annual	Implement follow-up actions to ensure EMAS certification is maintained.	EMAS certificate formally obtained; focus shifted towards maintenance.
	Develop an efficient framework for ENISA's continuous governance to safeguard a high level of IT.	Agency's 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 the agency.	Annual	70 % implementation (ITMC reporting).	Corporate strategy is expected to be reviewed and updated in 2026
				20 %	29 %

OUTPUTS	OUTCOME
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.	**In 2025, ENISA:** • coordinated the drafting and publication of the SPD and AAR, including the internal assessment and calibration of processes to increase efficiency and effectiveness; • conducted the internal controls assessment, managed audit recommendations from the European Court of Auditors (ECA) and Internal Audit Service (IAS), conducted risk assessments and consolidated reporting to the agency's management; • revised the anti-fraud policy and action plan; • managed legal coordination and support across the agency, including the management of court cases and requests from supervisory authorities; • provided data protection advice, and managed the data-processing register and contact with the European Data Protection Supervisor (EDPS); • implemented the new IT governance scheme and adopted the revised IT strategy (ITMC); • coordinated budget management across the agency, including developing a methodology for managing costs from contribution agreements (Budget Management Committee); • coordinated environmental management across the agency in cooperation with CSS (Activity 13), including the successful conclusion of the agency's EMAS audit and issuing of the EMAS certificate.

9.2. Maintain and enhance ENISA's cybersecurity position.	**In 2025, ENISA achieved the following.** • Developed the 2025–2028 cybersecurity maturity plan, which ENISA's management team adopted. The plan includes an action plan, a resource plan and an investment plan and encompasses all the agency's IT assets and services. • Supported day-to-day cybersecurity controls across the agency, including log monitoring, organising penetration testing, incident management, providing technical advice and coordinating with IT units. • Complied with Regulation (EU, Euratom) 2023/2841 on a high common level of cybersecurity in EUIBAs. All objectives and milestones have been met. • Organised internal cybersecurity awareness-raising sessions (training, phishing exercises).
9.3. Provide support services to EUAN in key areas of the agency's expertise and chair EUAN in 2025.	**In 2025, ENISA:** • coordinated the EUAN chairmanship, which included day-to-day support and collaboration with the SSO, chairing the EUAN Steering Board, chairing various subnetworks, representing EUAN at the interinstitutional level and hosting multiple EUAN events; • participated in the EUAN shared service initiative by providing cybersecurity services; • prepared a memorandum of understanding with the European Institute of Innovation and Technology (EIT) and the European Food Safety Authority (EFSA) on shared services, which was signed in February 2026; • provided cybersecurity advice to two agencies on risk management in collaboration with CERT-EU; • provided Data Protection Officer and accounting services to the ECCC (under a specific service-level agreement (SLA)).
9.4. Ensure the implementation of single administration processes across the agency.	In 2025, ENISA provided continuous administrative support services to all units in Athens and Brussels via the centralised pool of administrative assistants.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
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 the SPD. Annual assessments of risk and internal controls performed and reported. Legal and regulatory compliance monitored; issues and areas for improvement identified.	Budget Management Committee External and internal audits IT Management Committee Management team Statutory bodies	Number of high risks identified in annual risk assessment.	Annual	≤ 3	6 high risks (0 critical, 6 medium and 4 low).

Outcomes are included in the annual assessments of risk and internal controls. Streamlined IT system management across the agency and in accordance with ENISA's IT strategy under the ITMC. Streamlined budget management across the agency, under the Budget Management Committee. A plan to reduce CO2 emissions at ENISA's headquarters.		Effective monitoring of high risks and critical recommendations to follow up on timely implementation of mitigation measures by business owners.		Quarterly status reporting to the management team. Internal controls assessment, including reporting on implementation for year N–1. Risk assessment.	Completed. Completed. Completed.
		Percentage of identified deficiencies in internal controls addressed within timelines.		100 % for critical, 80 % for major, 60 % for moderate risks.	No critical weakness has been identified in the 2025 ICF assessment. While improvements have been noted, out of six recommendations issued in the 2025 ICF assessment , three important and two desirable recommendations remains to be followed up from the previous year while one important recommendation has been newly introduced on the implementation of specific and/ or horizontal internal controls going above and beyond financial transactions.
		Timely follow-up and resolution of internal and external audits recommendations and findings (in particular from the IAS and the ECA).		Monitoring audit action plans. Results of corrective actions taken during year N–1 are reported in the current year AAR.	Audit plans were monitored as appropriate. Completed.
		Number of identified regulatory breaches.		≤ 3	No regulatory breach identified in 2025.

		Percentage of revised and up-to-date corporate rules (Managing Board decisions, Executive Director decisions, policies, processes).		Review 50 % of corporate rules that have not been reviewed in the last 4 years and 60 % of corporate rules that have not been reviewed in the last 5 years. Provide or confirm motivation for non-revision, as a baseline requirement.	60 active Management Board decisions from before 2022.
		Annual report on ARES maintenance and actions.		80 % resolution of identified open issues, incorporating lessons learned.	100% resolution of identified issues
		Efficiency and effectiveness of ITMC and Budget Management Committee (survey).		> 60 %	Satisfaction rate of 69% for the BMC

9.2. Maintain and enhance ENISA's cybersecurity position.	Compliance with new regulations on a high common level of cybersecurity within EU entities. Timely identification and response to cybersecurity risks. Continuous monitoring of the cybersecurity of IT systems and timely identification of issues and areas for improvement (first-level and second-level controls).	External and internal audits Management team and relevant committees Statutory bodies	Percentage of identified high-risk mitigation measures addressed within timelines.	Annual	90 %	100 % (all the previously identified risks are being addressed).
			Annual risk assessment and risk treatment plan with the relevant business owners.	Annual	Implement annual risk assessment follow-up actions.	Implemented and in progress; follow-up with the risk owners.
			Implement action plan for implementation of cybersecurity risk management measures in line with Regulation (EU, Euratom) 2023/2841.	Annual	Report on the level of accomplishment of action plan.	Initial risk review was submitted in due time, and 60 % of identified actions are in progress.
			Address all potential cybersecurity incidents.	Annual	Respond to > 90 % of tickets submitted to the ticketing system.	100 %; all potential incidents were addressed in due time and without impact.
			Cybersecurity training for staff and managers.	Annual	At least 2 training sessions a year.	100 % achieved (first session by CERT-EU for managers and the second session for staff by the ISO team).
9.3. Provide support services to EUAN in key areas of the agency's expertise and chair EUAN in 2025.	Cybersecurity advisory on implementation of the new regulation on a high common level of cybersecurity within EU entities and in cooperation with CERT-EU. Shared services in the area of data protection, legal services and accounting.	Agencies receiving ENISA's support Budget Management Committee EUAN Management team	Satisfaction within EUAN with ENISA support services.	Annual	> 80 %	100 % satisfaction from all EU entities that have received services from ENISA.

9.4. Ensure the implementation of single administration processes across the agency.	Streamlined document management practices.	Management team Staff Committee	Percentage of staff considering that the information they need to do their job is easily available or accessible within ENISA.	Annual	55 %	As per the 2025 Staff Satisfaction Survey, 53 % of respondents agree and 17 % strongly agree with this statement; ≥ 70 %.
			Response timeliness to external parties (internal reporting).	Annual	Rate according to rules of procedures	Response rates in accordance with ENISA's procedures

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. European Commission, EUAN, relevant EU entities, Staff Committee and the management team.

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	14 [27]	NUMBER OF FTES ACTUALLY USED [28]	11.3
PLANNED BUDGET (EUR) [29]	743 000	BUDGET CONSUMED (EUR) [30]	690 656.40
AMENDED BUDGET (EUR)	690 656.40	OF WHICH CARRIED OVER TO 2026 (EUR)	353 158.57

[27] Including the Executive Director, Chief Cybersecurity and Operating Officer, Associate Chief Cybersecurity and Operating Officer and Accounting Officer.

[28] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

[29] Direct costs only – the budget includes consultancy linked to Activity 9 managed by Executive Director Office and the corporate website and security.

[30] Direct costs only – the budget includes consultancy linked to Activity 9 managed by Executive Director Office and the corporate website and security.

ACTIVITY 10

Reputation and trust

Activity 10 sought to meet the requirements set out in Article 4(1) of the CSA, which sets an objective for the agency to:

> *be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out* its tasks.

This objective requires that a transparent and proactive approach is taken to maximise the quality and value provided to stakeholders. It also includes contributing to efficiency gains by optimising the way ENISA engages with stakeholders. The activity seeks to further build the agency's reputation as a trusted entity through consistent messaging, adherence to corporate rules for communications activities and improving knowledge sharing internally and externally.

Outlined below are the key accomplishments of the activity in 2025.

- ENISA's chairing of EUAN (from 1 March 2025 for 1 year) yielded 14 EUAN meetings with 936 participants in total, bringing together, inter alia, senior agency and European Commission officials from across EUIBAs and confirming that the agency can coordinate large institutional groups in a composed manner.
- As Chair of the Heads of Communication and Information Network, ENISA organised a number of events and joint activities. For the communications and digital communications networks' plenary meetings, there was a 100 % satisfaction rate among the participants with the content of the meetings.
- 22 *ad personam* and 7 appointed members formed the new advisory group, and their mandate was expanded to include implementation of CRA in support of the agency's new tasks.
- The review of the first ENISA stakeholder strategy was conducted in 2025. As a result, a revised ENISA stakeholder strategy was developed in coordination with the MB. It aligns with the agency's strategic objective of 'empowered communities in an involved and engaged cyber ecosystem'. New processes for data gathering and reporting were established. The priorities for stakeholder management were set for 2026 to focus on the Member States' national authorities, EUIBAs and the private sector.
- ENISA organised a total of 109 events, including meetings, workshops and webinars. ENISA conducted 11 satisfaction surveys for operational events, receiving 719 responses and an overall 'very satisfied' or 'satisfied'

rate of 83 %. The participants came mainly from industry (34.29 %) and national public organisation (27.69 %).

- The agency oversaw 14 meetings of statutory bodies (the MB, Executive Board, the advisory group, the NLO network), and their satisfaction rate with ENISA's support to fulfil their tasks was 89 % in 2025. Particularly engaging was the Advisory Group on Vulnerabilities's contribution paper in terms of eliciting requirements for the CSA revision.
- Social media impressions of ENISA's posts increased to around 3.9 million in 2025, up from 3.3 million in 2024. Social media engagement has also increased from 75 000 to 83 000, suggesting that the content resonates with the audience.
- The migration of ENISA's corporate website to the Directorate-General for Digital Services has resulted in a more secure and stable website. The new website in its new environment received an estimated 1.3 million visits in 2025, a decrease due to structural and technical changes rather than a decline in user interest.

Presented below are the key lessons identified during 2025 that will guide future implementation.

- ENISA undertook citizen engagement for the first time, including a joint campaign with Debating Europe, which was successful. In the future, new stakeholder outreach will be focused on Member States, EUIBAs and industry.
- The functionality of statutory bodies' portals remains challenging, which creates additional workload and dissatisfaction among external stakeholders, so other options are to be considered.
- A large portion of the activity's resources were deployed in supporting the 2023–2025 ENISA Advisory Group in drafting four opinion papers. Given the outcome of the papers, the activity will seek more efficient ways of supporting the advisory group in preparing any future papers.

GENERAL ACTIVITY OBJECTIVES	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	TARGET	2025 RESULTS
10A. Protect and grow the agency's brand.	Ensure efficient corporate services.	ENISA brand management.	Annual	Target set in crisis communications playbook by 2025.	N/A
10B. Improve outreach of ENISA's mandate.	Ensure efficient corporate services.	Corporate satisfaction with essential communication and administrative assistants services.	Annual (management team survey)	60 %	Cost sharing model discontinued in 2025
		Corporate satisfaction with demand driven communication and assistants services.	Annual (management team survey)	60 %	Cost sharing model discontinued in 2025

		Stakeholder satisfaction with ENISA events.	Annual	> 60 %	83 %
		Number of unique visitors.	Annual	> 10 % increase year on year.	Estimated 1 million.

OUTPUTS	OUTCOME
10.1. Review and implement the multiannual communications strategy and support the stakeholders strategy, including corporate outreach.	**In 2025, ENISA achieved the following.** • Implemented 17 individual communication plans, developed in collaboration with operational units. • Supported 18 press releases and 11 news items. • Organised 109 events, including meetings, workshops, webinars, as well as 14 meetings of statutory bodies (the MB, the Executive Board, the advisory group, the NLO network) and 14 meetings as Chair of the EUAN. The targeted stakeholder groups for these events and meetings were as follows: - 63 national entities, - 23 private-sector entities, - 8 EUIBAs, - 6 civil-society organisations, - 5 academic institutions, - 4 international organisations. • Hosted visits, including that of the Executive Vice-President of the European Commission for Technological Sovereignty, Security, and Democracy, Henna Virkkunen, in October 2025. **ENISA as the Chair of EUAN** ENISA chaired EUAN, starting from 1 March 2025, for one year. During its term as the EUAN chair, ENISA organised 14 meetings with 936 participants in total. There was a 100 % satisfaction rate with the content for both the communications and digital communications meetings that were organised by ENISA as Chair of the Heads of Communication and Information Network. **Support for publications and events** The agency issued 20 publications, comprising both corporate documents and operational reports. All operation activities events and engagements were supported with promotion through ENISA's social media channels, where applicable. Additionally, communications assisted in the preparation for speaking engagements and/or interviews through the development and update of 'lines to take', which include ENISA's official position on topics relevant to the agency's mandate. In 2025, in line with its event policy, ENISA conducted satisfaction surveys for 11 of its largest events, for which 719 responses were received. Of the 719 respondents, 83 % were overall 'satisfied' with the outcome of the events. The responses were further processed to define metrics and KPIs for 'lessons learned'. The event participants came mainly from industry (34.29 %) and national public organisation (27.69 %). The remaining stakeholders represent EU public organisations, international organisations, civil-society or consumer organisations and academia or research. **Press and media mentions** A substantial increase in press and media mentions was recorded, with 5 120 press mentions in 2025, compared with 1 149 in 2024. This increase was primarily driven by key publications and announcements, such as the EUVD with 359 mentions throughout the year and the 2025 *ENISA Threat Landscape* report with 270 mentions. Overall, the tone of mentions was neutral (96.3 %).

ENISA's website

ENISA's website received an estimated 1.3 million visits in 2025, a decrease compared with the previous year. A new modern website was launched in December 2024 to update the agency's online image, improve the structure of information and introduce accessibility features.

The drop in the number of visits in the year following the redesign is mainly explained by structural and technical changes rather than a decline in user interest. As part of the redesign, some older content was removed, and several tools and resources were moved to a separate website. These changes reduced traffic to the main domain. The redesign also affected how users navigate the site and how traffic is referred. In addition, changes in analytics collection methods affected how visits were measured, which limits direct comparison with previous years.

Throughout 2025, the website was **constantly enhanced**, including the introduction of a new subscription mechanism at the end of the year and the migration of the site to the **Directorate-General for Digital Services infrastructure** to improve security and the quality of service.

Social media

Despite discontinuing the use of X (formerly Twitter), social media impressions of ENISA's posts **increased to around 3.9 million in 2025**, up from 3.3 million in 2024, while engagement increased to 83 000 from 75 000 in 2024 driven by greater focus and investment in LinkedIn. Key LinkedIn campaigns included the **NIS 2 technical implementation guidance**, posts timed with **key events and international days**, **event coverage** and the **ENISA cyber advent calendar**, introduced for the first time in 2025.

The agency also undertook a few citizen engagements for the first time, including in cooperation with the not-for-profit organisation Debating Europe to reach young people on the topic of cyber awareness through a joint social media campaign during European Cybersecurity Month (October 2025).

Finally, to enhance and modernise ENISA's corporate visual identity and strengthen the agency's brand, a partial but extensive corporate visual identity update was carried out in 2025. This included a comprehensive redesign of ENISA's templates and other communication outputs.

ENISA as a hub of expertise for senior EU officials and key private EU tech stakeholders

During the reporting period, the agency assigned an EU interinstitutional relations contact point with a twofold aim: to (a) provide one direct contact point for senior and high-level EU officials (e.g. MEPs, cabinets of commissioners, director generals, senior policy advisors) and (b) remind EU officials about the role and tasks of the agency.

ENISA has improved information sharing and cooperation with policymakers and policy-shapers. In addition, the agency has raised cybersecurity situational awareness within the EU's policymaking ecosystem.

10.2. Implement the internal communications strategy.

In 2025, ENISA achieved the following.

- Increased knowledge sharing and internal synergies through the internal communications strategy, as part of the overall communications strategy.
- Successfully organised the annual Staff Strategy Days to engage all staff in exploring strategic avenues for growth and foster an agency-wide spirit.
- Rolled out Workleap OfficeVibe, a new tool, which measures how teams are doing across key workplace dimensions of. It had an engagement score of 7.3 out of 10 and survey participation rate of 53 %. Among the positive highlights was the increase in the performance score with regard to 'relationship with management' (7.9), which was the highest-scoring metric overall. Feedback in relation to this metric often highlights open communication, a safe space for sharing and transparent management. Another positive highlight was the performance score regarding 'alignment' (7.3), which suggests that employees feel more connected with the organisation's values and vision. Feedback again indicates appreciation for transparent communication and the organisation's focus on inclusiveness.
- Organised 21 question-and-answer (Q & A) sessions and 3 ENISA Academy sessions for internal knowledge sharing.

	• Conducted two training sessions, specifically for newcomers and open to all staff, to help participants become familiar with communication tools and workflows, enabling them to promote their activities effectively and in full alignment with ENISA's standards. • Released weekly management team updates in the form of short debrief videos (42 videos) and a total of 246 internal announcements (compared with 247 in 2024) in an effort to ensure coherent and consistent information circulation within the agency.
10.3. Manage and provide the secretariat for statutory bodies (i.e. the Executive Board, the MB, the advisory group and the NLOs (excluding certification)).	**In 2025, ENISA organised the following:** • three meetings for the ENISA MB (one online, one hybrid, one physical), • two digital MB votes for Executive Board vacancies, • four meetings of the Executive Board (three online, one physical), • four meetings of the advisory group (two online, of which one was the onboarding webinar for the new advisory group; one hybrid; one physical), • three meetings of the NLO network (two online, one physical). **In 2025, the respective secretariats onboarded:** • 15 new MB members and alternates (8 members, 7 alternates), • 14 new NLO members, • a new advisory group comprising 22 *ad personam* members and 7 representatives from organisations. A number of MB members volunteered to work on strategic topics to support the work of the agency by forming an MB volunteer group. The advisory group was also supported to publish four opinion papers, covering cybersecurity in AI, implementation of the NIS 2 Directive, CVE and the CSA.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
10.1. Review and implement the multiannual communications strategy and support the stakeholders strategy, including corporate outreach.	Enhanced transparency and outreach. Engaged communities. Increased impact of ENISA activities. Relevant and easily accessible information provided to stakeholders. Successful EUAN leadership, communications and EUAN yearly meetings.	Agency stakeholders Management team	Number and types of activities at each engagement level (stakeholder strategy implementation).	Annual (internal report)	Stakeholder strategy under review.	109 events and meetings, involving 63 national entities, 23 private-sector entities, 8 EUIBAs, 6 civil-society organisations, 5 academic institutions and 4 international organisations.

			Number of social media engagements.	Annual (media monitoring)	> 80 000	83 000
			Number of total ENISA website visits.	Annual (website analytics)	> 2.5 million	~ 1.3 million [31]
			Website availability.	Annual (website analytics)		> 97 %
10.2. Implement internal communications strategy.	Engaged staff.	Management team Staff Committee	Staff satisfaction with ENISA's internal communications.	Annual (survey)	> 60 %	64 %
10.3. Manage and provide the secretariat for statutory bodies (i.e. the Executive Board, the MB, the advisory group and the NLOs (excluding certification)).	Support for the operation and organisation of ENISA statutory bodies. Support the effectiveness of the implementation of work programmes (validation of operational outputs). Provide administrative support for the day-to-day workings of the MB's decisions and recommendations from the NLO network and advisory group.	Committees Management team Statutory bodies	Number of feedback instances received per NLO consultation.	Annual (internal report)	> 6	9
			Number of feedback instances received per advisory group consultation.	Annual (internal report)	> 8	10
			Satisfaction of statutory bodies with ENISA's support to fulfil their tasks as described in the CSA.	Annual (survey)	> 80 %	89 % (very) satisfied and 11 % neutral.
			Satisfaction of statutory bodies with ENISA's portals.	Annual (survey)	> 80 %	74 % (very) satisfied, 24 % neutral and 2 % unsatisfied.

(31) (Content to be confirmed)

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. European Commission; members of statutory bodies, such as the MB; advisory groups and NLOs; EUAN; relevant EU entities; Staff Committee; and the press.

Involve/engage. All ENISA stakeholders.

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	9	NUMBER OF FTES ACTUALLY USED [32]	7.3
PLANNED BUDGET (EUR) [33]	760 000	BUDGET CONSUMED (EUR) [34]	812 158.61
AMENDED BUDGET (EUR)	812 738.36	OF WHICH CARRIED OVER TO 2026 (EUR)	228 194.16

[32] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.
[33] Direct costs only.
[34] Direct costs only.

ACTIVITY 11

Effective and efficient corporate services

In 2025, the work of Activity 11 made a strong contribution to ENISA's organisational resilience, operational continuity and people-centred corporate development. The corporate support services unit sustained high-quality delivery in human resources, finance, procurement, IT, facilities and security, despite some resource constraints. The year was marked by concrete progress in workforce planning, service modernisation, financial performance and staff support, all of which strengthened ENISA's ability to meet its strategic and operational objectives.

The most significant achievement was the effective management of ENISA's workforce and organisational transition. The agency implemented the annual workforce review, reached 98 % establishment plan implementation, filled 14 of 16 planned posts and recruited additional staff for new contribution agreements. Recruitment performance remained strong, with vacancy processes completed in 14 to 200 days, and all resignations backfilled within two months. At the same time, CSS supported ENISA's transition to a new organisational structure with 8 operational units, including the revision of over 100 assignment decisions and competency adjustments, ensuring continuity and alignment between staffing and organisational needs. In 2025, the CSS unit also drafted, prepared and coordinated over 150 policy and legal documents to support the appointing authority and also supported EUAN requests from, for example, the European Parliament, the Council of the European Union, the ECA, the IAS and European Data Protection Supervisor. CSS continued to invest in staff development and well-being, delivering over 200 competency-driven training activities and 19 Q & A sessions and orchestrating successful staff strategy and development days.

A second major achievement was the excellent budgetary and financial management performance delivered in 2025. ENISA achieved an overall budget commitment rate of 99.96 %, with a year-end surplus of only EUR 9 748, reflecting exceptionally precise financial planning and execution. The agency also reduced its late payment rate to 0.97 %, down from over 5 %, which represents a major organisational improvement and places ENISA well below the ECA's threshold achieved in one single year. In parallel, CSS successfully processed and administered several major new contribution agreements, successfully ran more than 33 procurement procedures, strengthening ENISA's financial base and operational reach without the additional corresponding reinforcement of internal financial resource capacity.

A third key achievement was the modernisation and professionalisation of corporate services, especially in IT, service delivery and staff support. Corporate IT completed 21 projects, launched

20 more for 2026 and maintained 99.95 % critical systems uptime, while resolving over 3 500 IT requests and 260 incidents. Important advances included the implementation of a unified ticketing solution, IT asset inventory, zero-trust network access controls and progress toward a self-service service model across IT, facilities, security and, increasingly, HR, finance and procurement.

In parallel, CSS assisted the agency in progressing and improving staff satisfaction in several key areas, including working environment and IT resolution with 97 % of staff survey follow-up actions on time.

In 2025, the unit also organised, planned and delivered significant EUAN activities in the area of procurement, HR and resources, Information and Communication Technologies Advisory Committee and joined other EUAN activities and the Greening network in the context of ENISA chairing the EUAN.

Overall, Activity 11 demonstrated that ENISA's corporate services are becoming more agile, digitally enabled and strategically aligned. The achievements of 2025 show a function that not only maintained essential services under pressure but also laid the groundwork for a more integrated service model, stronger internal governance and a more attractive and supportive workplace for staff.

GENERAL ACTIVITY OBJECTIVES	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	LATEST RESULT	TARGET	2025 RESULTS
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.	Annual 2025 workforce review concluded with Executive Decision No 17/2025, and the annual workforce review for 2026 was started in October 2025.
		Implementation of the corporate and HR strategy.		N/A	Actions implemented according to the timelines.	Various policies revisited. All posts outlined in the annual workforce review have been filled or under are recruitment. Over 200 competency-driven training sessions implemented.
		High participation in the Staff Satisfaction Survey.		64 %	75 % participation rate.	The 2025 Staff Satisfaction Survey had a participation rate of 73 %. Although the same number of participants contributed to the survey as in 2024, 15 newcomers joined the agency, leading to a decrease in the 2025 response rate to just under the 75 %.

11B. Ensure sustainable and efficient corporate solutions and promote continuous improvement.	Ensure efficient corporate services. Introduce digital solutions that maximise synergies and collaboration in the agency. Developing service propositions with additional external resourcing. Promote and enhance ecologic sustainability across all the agency's operations. Develop an efficient framework for ENISA's continuous governance to safeguard a high level of IT and to ensure physical security services, such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently.	Implement best practices for sustainable IT solutions.	Annual	75 % of the implementation of the Information Technology Infrastructure Library (ITIL) framework and best practices were implemented during 2024.	IT strategy updated accordingly.	Corporate IT is aligned with the ITIL framework and best practices. All IT staff are ITIL certified.
		Limited disruption of continuity of corporate services.	Annual	Corporate IT implemented an effective business continuity plan.	Business continuity plan for corporate IT, facilities, financial and HR services in 2025.	Corporate IT, facilities and security have a business continuity plan in place.
		Handling EU classified information at the EU secret level.	Annual	Process was ongoing during 2024. Inspection was concluded successfully in 2024.	Operational for the first full year in 2025.	The final inspection report was delivered in August 2025. The next step (security sweep), due to the HR security sweep team's unavailability, was performed by the Council of the European Union's security team in Q1 2026. This was the final step for the accreditation.

OUTPUTS	OUTCOME
11.1. Manage and provide general, recurrent administrative services in the area of resources for ENISA staff and partners.	In 2025, the work under this activity continued provide support services to HR, finance and procurement. • **HR and workforce planning.** In 2025, the activity implemented in full ENISA's workforce planning programme set in the 2025 annual workforce planning report, with the exception of fulfilling two posts in the CSS unit, which were kept as a reserve to support organisational resilience in budget management. Based on the 2025 annual workforce planning report, 14 out of 16 planned posts were filled within a time line ranging from 14 days to 200 days of completion. An additional 11 posts were filled that were not planned in the 2025, annual workforce planning report as part of contributions agreements. All ENISA resignations and the refilling of posts have also been fulfilled within two months. In total in 2025, 31 job offers were sent out, of which 6 were declined and 25 were accepted. In fulfilling this goal and reaching the 99 % of establishment plan implementation, CSS used existing reserve lists, launched new competitions and used European personnel selection office competitions where possible. In addition, CSS continued to support the AIPN and Heads of Units regarding the restructuring of posts envisaged in the 2025 annual workforce planning report (in total five posts (three temporary agent (TA) and two CA posts). The unit also supported the preparation of resourcing of upcoming contributions agreements, which were signed in last days of 2025 or the beginning of 2026, such as those for the e-health action plan, the eIDAS implementation and the Western Balkans cybersecurity support. As the agency transitioned to eight operational units as from January 2025, all related staff were administratively reassigned to the new units; new job descriptions were provided and the competence target proficiency levels adjusted. This led to the revision of over 100 assignment decisions and competency adjustments to fit the new organisational regime. • **Performance, development and well-being**. The agency conducted its annual appraisal exercise, with a closure rate of 99 % completion and dealt with two appraisal appeals. The agency revised its reclassification exercise in 2024 and further finetuned it in 2025. The exercise was concluded later than expected in October 2025. All these exercises were conducted while the new organisational structure in operations was put in place and while support to new middle managers was established. In January 2025, **ENISA Staff Strategy Days** were organised, a key event bringing all agency staff together to understand the priorities for the year, build competences and team-building, including organising the staff assembly and special moments for staff recognition. • **Budget and finance.** CSS continued to implement a number of actions to closely monitor the timely processing of payments. In Q3 and Q4 2025, the unit introduced more assertive communication with dual reporting lines to the management team and the Budget Management Committee on a weekly basis, combined with a weekly reporting to Heads of Units on budget execution. This ensured that the ENISA budget was fully consumed, ahead of the statutory end date of closure of the accounts, ensuring the best financial closure of the year ENISA has ever experienced. As a result, due to proactive and regular communication, the overall ENISA late payment rate was further reduced from over 5 % to 0.97 % out of a total of 2 069 payments, which is a remarkable organisational and financial achievement. This confirms the effectiveness of the measures put in place and demonstrates sustained improvement in payment performance. The agency remains committed to maintaining a structurally low payment rate, well below the 5 % threshold set by the ECA. During 2025, ENISA operated with the annual budget (EU subsidy and European Free Trade Association funds (C1) of EUR 26.7 million. During the year, the MB adopted an amending budget and two budget transfers based on Executive Director decisions have been processed. The execution of the budget 2025 resulted in a surplus of EUR 9 748, corresponding to 0.04 % of the total budget. The overall commitment rate reached 99.96 %, while the overall payment rate amounted to 84.64 %, reflecting a high level of budget implementation for the financial year.

Out of EUR 4 608 449 that were carried forward (C8), EUR 4 498 289 were paid, corresponding to an implementation rate of 97.61 %. An amount of EUR 110 160 was cancelled from commitments carried forward from 2024.

In anticipation of the agency's transition to new budgetary system (SUMMA) as of 1 January 2027 and the impact of this change will have on all financial operations, CSS have started the preparations with Directorate-General for Budget on the transition to the new financial system and in parallel, explored the possibility of requesting additional training assistance to sufficiently involved actors and train them in the course of 2026. Under this view, a series of training sessions have been scheduled to take place in 2026.

During 2025, additional contribution agreements were signed between Directorate-General for Communications Networks, Content and Technology and ENISA, and a total of EUR 28 063 333 has been received as R0 funds based on a number of contribution agreements. As per internal set up, all contribution agreements are accounted for under Title 4.

All these additional agreements were processed and administered by the unit, without additional resources being added to strengthen financial capacity and compliance.

- **Procurement and contract management.** In 2025, the procurement services in the CSS unit further improved the effectiveness and efficiency of their procurement processes to ensure the completion of the 2025 annual procurement plan. Procurement procedures were carried out in line with the 2025 procurement plan wherein a 96 % implementation rate was achieved by 31 December 2025. In total in 2025, CSS handled and concluded 33 procurement procedures: 17 open procedures (52 %), of which were 6 open tender procedures not set in the procurement plan; 13 re-openings of competition (39 %); 1 restricted procedure (3 %); and 2 exceptional negotiated procedures without publication of a contract notice as per Article 11(1) of Annex I of the agency's financial regulation (6 %). Also, the procurement team ran three rounds of lists of individual external experts to assist ENISA evaluations.

  Moreover, ENISA's procurement team is responsible for following up and handling administratively 28 SLAs in force, of which 3 were signed in 2025, and 10 memorandums of understanding. The CSS procurement team provided a full range support to the increasing number of contribution agreements and specific contracts, ownership and control assessment support and coordination in collaboration with the European Research Executive Agency (REA) and further supported all ENISA activities, including those that were externally funded via the indirect management funding programmes of the European Commission and Directorate-General for Communications Networks, Content and Technology.

  In order to support the continuity of ENISA's services, as well as to procure essential and additional services, a further streamlining of procurement processes took place. The procurement team delivered several training sessions on procurement, contract management and lessons learned throughout 2025 in order to strengthen ENISA staff's financial, procurement and contract management awareness. European Commission public procurement management tool. is the main tool to be used. In the future, the unit aims to further streamline procurement procedures via this tool, which in 2025 was connected with further contract management modules in accruals-based accounting.

  Additionally, tender procedure templates were updated to reflect these developments and European Commission standards. A detailed guide on how to handle contribution agreements was developed as an internal practice. The reduction in the ECA's findings related to procurement is the result of the procurement team's growing professionalism and maturity, itself the result of advanced training.

11.2. Implement the agency's corporate strategy, including the HR strategy, with an emphasis on talent development, growth and welfare.

The corporate HR strategy continues to put the people at its core, and to this end, CSS organised and coordinated a range of learning and development initiatives based upon the prioritisation of needs and in conformity with the learning and development plan and budget. The learning and development plan in addition included mandatory training, such as anti-fraud, anti-harassment, cybersecurity and privacy-related training. Also, CSS organised and provided in line with the Staff Satisfaction Survey roadmap, staff training related to, among other things, stress management, workload management, mental well-being, work–life balance, mindfulness and unconscious bias, and ethics. They also organised specialised trainings such as CISP accreditation, PM2 training, leadership, change management and various management development sessions.

Towards the end of 2025, following on from the annual workforce review post reviews, the agency decided to revise how the budget for learning and development is organised for 2026. Although the in 2024 introduced prioritisation of training mechanism proved its value, the approach missed the guidance on budget spending in terms of:

- general development needs open to all staff (e.g. mandatory training, competence, conduct-related and well-being training);
- targeted development needs (e.g. middle management training, unit seminars, away days, 360° feedback and coaching, training related to ENISA, and functional competence target proficiency level growth);
- individual development actions (e.g. under-performance support and high-potential development).

At the end of 2025, the agency launched preparations to include AI in its core agency competences as a separate competence, expanding its competence framework. The agency aims to integrate AI applications in its working methods, increasing the efficiency and effectiveness of its work planning at the operational and corporate levels. Aligned to the introduction of the AI competence, a training programme will be developed with five different target proficiency levels. This will be part of the learning and development planning and budget, and these competences will be used as a pilot for 2026.

- Aligned with the strategic need for the agency to strengthen its overall cybersecurity position and maturity level internally due to the change in its tasks and responsibilities, the first outlines of the training programme falling under the ENISA cybersecurity maturity plan have started to take shape, with the aim to have this plan completed by Q3 2026.
- Upon the Staff Satisfaction Survey outcomes presented to the organisation in November 2024, the roadmap for improvement actions was developed and kicked off at the beginning of Q2 2025, with the involvement of staff, the Staff Committee, the management team and senior leadership. On a quarterly basis, the progress in the actions was presented to staff, the Staff Committee and the management team. In September 2025, the Staff Satisfaction Survey was launched again, and the level of satisfaction related to the jointly identified roadmap actions considerably improved in the areas of leadership and direction, authority and empowerment, respect and well-being (supported by nine training sessions on well-being), performance management, learning and development, and working environment and service orientation. In the survey, corporate support services were evaluated as well received.

In relation to policies and legal work, the CSS unit handled, administered, coordinated and prepared over 130 legal and policy outputs for the AIPN and contributed to over 60 EUAN exchanges in addition to providing continuous support to the European Parliament, European Commission, Council of the European Union, ECA/IAS and other stakeholders' requests as per its statutory obligations.

Last but not least, the CSS unit continues its regular, structural and ongoing social dialogue with staff, via the structured meetings with the Staff Committee and the administration; dedicated Q & A sessions (over 19 were held in 2025); visits to unit meetings to exchange, answer and clarify questions as well as its proactive communication campaign via the internal systems.

11.3. Manage and provide general, recurrent support services in the area of facilities, security and corporate IT for ENISA staff and partners.	In 2025, the Corporate IT sector embarked on a remarkable journey of achievement and transformation. Through dedication and teamwork, the sector, with three statutory FTEs (supported by service providers) and one FTE in facilities/security delivered a series of impactful projects for ENISA that strengthened operations and set the stage for future innovation. Overall, CSS delivered strong portfolio execution, completing 21 projects in 2025 and initiating 20 projects, scheduled for conclusion in 2026. Corporate IT received and resolved over 3 500 IT requests and 260 IT incidents, while dedicating 2 FTEs to work attributed to EDO and operational IT. Highlights of the year include: • data centre migration assessment, including a comprehensive feasibility study for an on-premises data centre option; • Border Gateway Protocol implementation/enhancements; • mobile cost reporting, establishing improved visibility and cost controls; • zero trust network access control implementation • Netwrix Auditor implementation (access reporting tool); • framework contracts established for data centre colocation and for mobile/landline telecommunications services; • process implementation and operationalisation of an integrated and unified change management solution (Change Management in ServiceNow); • unified ticketing solution implementation for IT, facilities and security services; • IT asset inventory implementation; • further enhancement of collaboration between the CSS IT department, security team and operations. The following main projects, initiated in 2025, remain in progress and are scheduled for completion in 2026: • data centre physical security enhancements by the end of Q1 2026, • data centre migration and colocation by the end of Q2 2026, • supporting and contributing to services for the CRA Single Reporting Platform (e.g. test environment, infrastructure, etc.), • ServiceNow ticketing roll-out for HR/procurement/finance by the end of Q2 2026, • Microsoft 365 roll-out/migration to be completed in 2026, • exchange online migration to be completed in 2026, • Disaster recovery and high availability capability for the operational move from Athens to Alicante by the end of Q2 2026, • change of internet service provider for the Brussels office by the end of Q2 2026, • parking system upgrade (for safety) to be completed in 2026, • enhanced floor warden training, to further strengthen safety awareness and emergency preparedness for ENISA colleagues, to be completed in 2026.
11.4. Enhance operational excellence and digitalisation through modern, safe, secure and streamlined ways of working, and introduce self-service functionalities.	During 2025, the CSS unit introduced a radical transformation, by evolving to a service model, that is, a model based on services, not necessarily functions. This is a complex programme, and the first foundation and pillar for the implementation have been set up. Within this programme, dedicated knowledge bases have been created for IT, facilities and security, which serve as a self-service first-line support. A knowledge database has started for HR, finance and procurement, which should be completed in 2026. In parallel, a detailed service catalogue has been created for IT, security and facilities, and users can request more accurately their services via the self-service portal. The first taxonomy catalogue for HR, finance and procurement has been set. In 2025, the CSS unit also capitalised upon the SLAs with the European Commission, under the Office for the Administration and Payment of Individual Entitlements and the Directorate-General for Human Resources and Security, and informed staff of the transition of its services to those two entities through the Commission's dedicated staff portal. The plan is that in 2026, these are further capitalised upon, and services for staff are further categorised with services offered by the European Commission versus services offered by ENISA's CSS. In this way, ENISA will be setting in place its first internal service-level catalogue with exact response timelines. Overall, Corporate IT is using agile methodology as a standard project management approach, and in 2026, the CSS unit will be fully trained in this methodology to maximise efficiency. Overall, the service transformation is a three-year programme that aims to target processes, systems and services and is scheduled to be completed by 2028.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	2025 TARGET	2025 RESULTS
11.1. Manage and provide general recurrent administrative services in the area of resources for ENISA staff and partners.	Services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently. Implementation of the Executive Director decision on the annual workforce review (adopted in April 2024).	Budget Management Committee ITMC Management team Staff Committee	Turnover rates (statutory staff and seconded national experts (SNEs)	Annual	< 5 %	6.4 %
			Turnover rates (staff under contribution agreements).		< 5 %	7.4 %
			Establishment plan posts filled.		> 95 %	99 %
			Lag between vacancy announcement to candidate selection (offer out).		< 300 days median across all posts.	Range between 14 days and 200 days.
			Percentage implementation of the approved recruitment plan.		> 90 %	98 %
			Percentage implementation of the approved procurement plan.		> 90 %	96 %
			Percentage procurement procedures launched via e-tool.		> 90 %	100 %
			Percentage budget implementation.		> 95 %	99.96 %
			Average time to initiate a transaction by financial initiating agent.		< 7 days	7 days
			Average time for verifying a transaction by financial verification agent.		< 3 days	0.17
			Number of budget transfers.		< 4	2
			Late payments resulting in interest payments.		< 10 %	0.97 %

11.2. Implement the agency's corporate strategy, including the HR strategy, with an emphasis on talent development, growth and welfare.	Objectives and goals set out in the corporate and HR strategy are met.	Budget Management Committee EUAN Management team MB Staff Committee	Number of policies reviewed.	Annual	> 1	17
			Number of processes revised.		> 1	25
			Percentage of staff satisfaction with talent development.		> 50 %	60 %
			Percentage of actions implemented as follow up on Staff Satisfaction Survey results and implemented on time.		> 95 %	97 %
			Number of implemented competency-driven training and development activities.		> 1	200
			Number of multisource feedback evaluations implemented and followed up.		> 5	43
11.3. Manage and provide general, recurrent support services in the area of facilities, security and corporate IT for ENISA staff and partners.	Services such as corporate IT, facilities and security are performed efficiently with minimal disruption. Upgrade of meeting rooms.	Budget Management Committee ITMC Management team Staff Committee	Staff satisfaction with working environment.	Annual	> 70 %	81 %
			Time to respond to safety and security incidents.		< 1 day to acknowledge and < 3 days to respond.	KPI met.
			Average time to respond to facilities management requests.		< 1 day to acknowledge and < 3 days to respond.	KPI met.
11.4. Enhance operational excellence and digitalisation through modern, safe, secure and streamlined ways of working, and introduce self-service functionalities.	Services such as access management, meeting room facilities, equipment renewals, cloud-based solutions and data availability are efficient.	ITMC Management team	Critical systems uptime and downtime.	Annual	99 %	99.95 %
			Staff satisfaction with IT resolution.		85 %	93 %

STAKEHOLDERS AND ENGAGEMENT LEVELS

Partners. ENISA staff members and EUIBAs.

Involve/engage. Private-sector and international organisations.

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2025 YEAR END	21	NUMBER OF FTES ACTUALLY USED [35]	14.8
PLANNED BUDGET (EUR) [36]	4 631 348	BUDGET CONSUMED (EUR)	4 944 465.36
AMENDED BUDGET (EUR)	4 944 465.36	OF WHICH CARRIED OVER TO 2026 (EUR)	1 702 603.39

[35] FTE available per activity, deducting any type of absence, such as part-time work, parental and family leave, sick leave, special leave, annual leave, recuperation and time off in lieu.

[36] Direct costs only. Budget includes staff development, staff welfare, external temporary staffing, building costs, consultancy under Activity 11, corporate and administrative expenditure under Activity 11, core and corporate ICT under Activity 11 and missions under Activity 11.

II

PART II (a)

MANAGEMENT

2.1. Management Board

ENISA is governed by its MB, which is composed of one representative per Member State and one member representing the European Commission. Each member has an alternate and each participating member or alternate carries one vote per Member State or on behalf of the European Commission. The Executive Director participates in the MB but they are not a member and have no vote. The term of office for the members of the MB and their alternates is four years, renewable; there is no set limit for a maximum term in office. The work programme provides the policy priorities to support the approval of the agency budget, also approved and monitored by the MB. The MB appoints the Executive Director of the agency and adopts appropriate rules within the boundaries set by the CSA.

In 2025, the MB held four meetings, including one strategy and one extraordinary meeting. In addition, on two occasions the MB held a vote to fill the position of the board's Deputy Chairperson and one position on ENISA's Executive Board. In April 2025, during the MB's strategy meeting, the board discussed geopolitical developments and their impact on ENISA, along with the outlook for the EU cybersecurity agenda, with a particular focus on the European action plan on the cybersecurity of hospitals and healthcare providers and the proposal for a Council recommendation on an EU blueprint for cybersecurity crisis management. In the context of the evaluation of the CSA, an in-depth discussion was held on Title II of the act, concerning ENISA's mandate, and on Title III, relating to the ECCF. A joint meeting of ENISA's MB and the ECCC's Governing Board was convened to discuss the enhancement of inter-agency cooperation and to further clarify each board's roles and responsibilities. At the MB's June meeting, it decided to establish a working group composed of voluntary MB members to follow up on discussions concerning strategic topics of relevance to the board. In 2025, the group met three times, during which it addressed the review of the CSA, the review of ENISA's international strategy, the review of ENISA's strategic KPIs and cooperation with the CSIRT network.

In total, the MB adopted 22 decisions, including decisions to extend the appointment of the Accounting Officer, to establish ENISA's Advisory Group, and to adopt ENISA's stakeholder strategy and international strategy, along with its anti-fraud strategy and action plan for 2025–2027.

In accordance with the CSA and the MB's rules of procedure, the MB's decisions were prepared by the Executive Board and adopted by the MB. The 2024 AAR was duly adopted, contributing to the discharge of the Executive Director, and the MB expressed its opinion on the final annual accounts for the 2024 financial year. Additionally, the 2026–2028 ENISA SPD, including the 2026 budget and establishment plan, was adopted. The MB approved one amending budget for the 2025 financial year and adjusted the 2025

establishment plan. Finally, the MB issued the opinion on the functioning of ENISA's MB.

2.2. 2025 statistics for statutory bodies

ENISA organised four meetings of its MB (two ordinary, one strategy and one extraordinary); two digital elections, one for the MB's Deputy Chair and one for an Executive Board vacancy; four meetings of its Executive Board (three online and one physical); three meetings of the MB volunteers group (online); four meetings of its Advisory Group (two online, of which one was the onboarding webinar for the new Advisory Group; one hybrid; and one physical); and three meetings of the NLO network (two online and one physical).

2.3. Major developments

The following internal and external factors affected ENISA in 2025.

EU cyber blueprint

During the course of 2025, an important milestone in strengthening the response to large-scale incidents and crises in the EU was reached, with the adoption by the Council of the European Union of the revised blueprint for cybersecurity crisis management.

The EU cyber blueprint is an important guideline: it enables Member States to enhance their preparedness, detection capabilities and response to cybersecurity incidents, while aiming to tackle an increasingly complex cyber threat landscape by strengthening existing EU networks and fostering cooperation across the EU.

Common vulnerability and exposure numbering authority

In 2025, ENISA became a CVE programme root, thus establishing itself as a central point of contact within the CVE programme for national and EU authorities, EU CSIRT network members and cooperative partners falling under ENISA's mandate.

ENISA's new role is part of the EU's investment in strengthening vulnerability coordination and management in the EU. As such, this new role complements and supports the coordinated vulnerability disclosure activities conducted by Member States and in particular the establishment and operation of the EUVD, along with ENISA's new tasks under the CRA in relation to the provision of guidance to manufacturers on compliance, assistance with the implementation of the new cybersecurity framework and the implementation of the single reporting platform.

EU Vulnerability Database

ENISA launched the EUVD as provided for by the NIS 2 Directive. The EUVD, to be maintained by ENISA, became operational in 2025. The database provides aggregated, reliable and actionable information, such as mitigation measures and exploitation status on cybersecurity vulnerabilities affecting ICT products and services.

EU managed security services certification

Following a request from the European Commission in 2025 to develop a candidate certification scheme for managed security services, ENISA launched a call for expression of interest to participate in the relevant AHWG.

Managed security services are of increasing interest as a means of supporting the enhancement of cybersecurity across all sectors and infrastructures, whether public or private, small or large, or commercial or critical. Rapid developments and the complexity of the evolving cyber threat landscape lead all kinds of entities to outsource a considerable part of their security functions to managed security service providers to effectively safeguard their operations. This makes managed security service providers essential for the cybersecurity of organisations but also renders them prime targets of cyberattacks.

ENISA's new Advisory Group

In 2025, ENISA selected the members whose expertise would support the agency's strategic objectives, set by its MB.

Out of 300 eligible applications received, ENISA selected 26 experts to form the new Advisory Group. These experts were formally appointed by the agency's MB. Based on personal expertise and merits, members are selected *ad personam*. As such, they do not represent their country of origin, nor do they represent the organisation they work for. As a consequence, they cannot delegate their responsibilities to any other member of the group or to any other third party.

The new Advisory Group was set up for a term of 2.5 years, with an indicative starting date of 1 August 2025. The term of the previous Advisory Group will end on 31 July 2028.

EU cybersecurity reserve

ENISA and the European Commission signed a contribution agreement, through which the Commission entrusts ENISA with the administration and operation of the EU Cybersecurity Reserve, and provides ENISA with a financial contribution to that end.

The EU Cybersecurity Reserve, envisaged in Article 14 of the CSOA, consists of incident response services from trusted managed security service providers.

This support mechanism will be used for the purpose of responding to and recovering from significant and large-scale cybersecurity incidents, should they occur.

Procured by ENISA, services offered will be contracted from trusted managed service providers. Such providers were selected by means of public procurement calls.

The services are intended for users representing critical sectors of Member States as described in the NIS 2 Directive, along with EU institutions, bodies, offices and agencies. The services may also be requested by non-EU countries that have been associated with the DEP and whose association agreements include provisions granting access to the EU Cybersecurity Reserve.

When operating the EU Cybersecurity Reserve, ENISA will rely on its extensive experience built over its years of successfully managing the agency's cybersecurity support action.

International Cybersecurity Challenge

ENISA supported Team Europe to claim first place in the fourth edition of the ICC. Hosted in Tokyo, Japan, the ICC gathered top cybersecurity talent from around the world to compete against each other, testing their cybersecurity skills. A total of eight teams, from Africa, Asia, the Association of Southeast Asian Nations, Canada, Europe, Latin America, Oceania and the United States took part in the competition, representing more than 80 countries.

The ICC is a global Capture the Flag event encouraging the development of cybersecurity skills and fostering international cooperation. Competing with teams of nationalities from all over the world is a unique opportunity for new cybersecurity talent to learn from cultural differences and still be able to efficiently cooperate.

ENISA's revised international strategy

The agency renewed its approach to engaging with its international partners, thus strengthening its alignment with the EU's international cybersecurity policies, promoting EU values and fortifying its mission to achieve a higher common level of cybersecurity across Europe. As part of ENISA's overall strategy and in particular its recently renewed stakeholders' strategy, the renewed international strategy focuses on international partners sharing the EU's values, and with which the EU has strategic relationships.

ENISA's stakeholder strategy

The ENISA's new stakeholder strategy sets out the agency's approach to identifying and engaging stakeholders in a value-driven, coordinated and transparent way. It establishes common principles and governance for stakeholder engagement, aligned with ENISA's mandate and priorities, while ensuring effective outreach and avoiding the duplication of efforts and stakeholder fatigue.

ENISA as Chair of the EU Agencies Network for 2025–2026

ENISA led inter-agency cooperation on key priorities and contributed to raising the common level of cybersecurity across EU agencies. As Chair of EUAN in 2025, ENISA pursued key priorities on implementing the new governance framework of the network, asserted the role of agencies as key institutional partners and strengthened cybersecurity across the EU agencies and joint undertakings, improving efficiency through sharing its services.

The role of the EUAN is to enable structured collaboration across the EU's decentralised agencies and joint undertakings to drive innovation, enhance efficiency and strengthen Europe's competitiveness. Through closer cooperation, EUAN members can deliver better services and build a smarter, safer Europe that meets the needs of all citizens.

During ENISA's term as Chair, the agency proactively interacted with selected EU institutions, including the European Commission, the European Parliament and the Council of the European Union, along with the ECA and other stakeholders, as appropriate.

In an effort to increase user awareness, ENISA made available tools and methods to strengthen cybersecurity across EU agencies and joint undertakings, as its standing priority during its chairpersonship. In this vein, ENISA supported agencies in improving cybersecurity preparedness and thus helped them comply with EU requirements.

2.4. Budgetary and financial management

Financial management

During 2025, ENISA operated with a budget of EUR 26.7 million, higher than the 2024 budget of EUR 26.2 million (annual EU contribution).

During the year, ENISA implemented activities under a contribution agreement between DG Communications Networks, Content and Technology and the agency, which was signed in late December 2023. The agreement granted ENISA a total of EUR 20 million to provide cyber support and implement situational centre actions during 2024–2026. The first instalment, amounting to EUR 16 million, was received in February 2024.

In addition, in 2025 ENISA received a total of EUR 28.1 million under various contribution agreements signed with DG Communications Networks, Content and Technology, in which agreed actions span multiple years:

- an instalment of EUR 240 000 covers the activities agreed under the contribution agreement signed on 9 December 2024 with the purpose of conducting a feasibility study on the CRA Single Reporting Platform;
- an instalment of EUR 12 million funds the activities agreed under the contribution agreement signed on 19 December 2024 covering incident and vulnerability response and reporting;

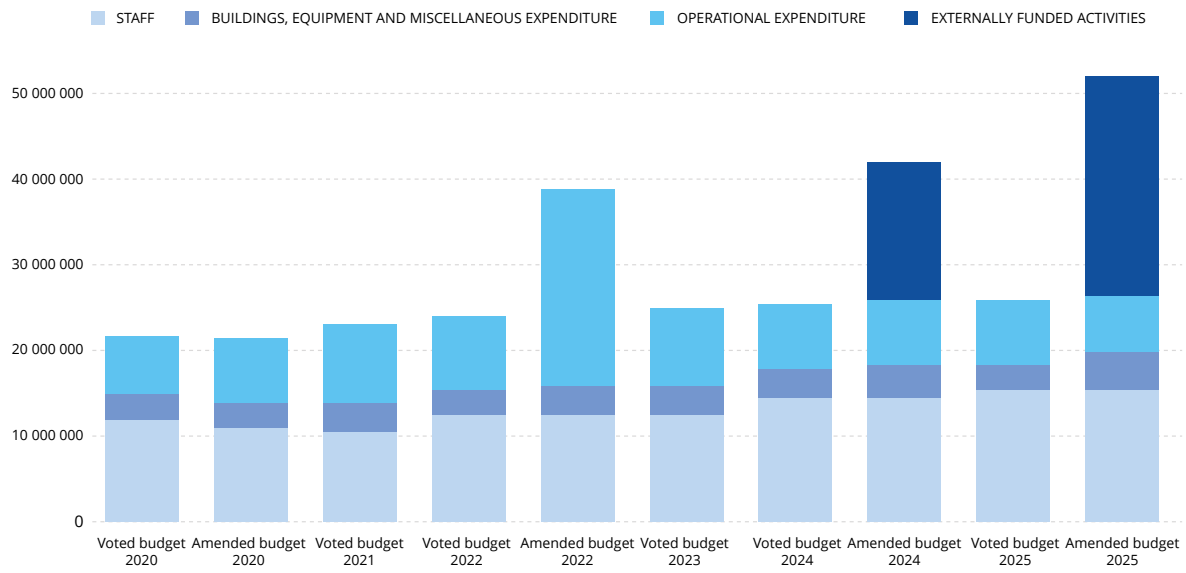


Figure 3. *Change in voted and amended budgets between 2020 and 2025 (EUR)*

- an instalment of EUR 12.2 million covers the activities agreed under the contribution agreement signed on 31 July 2025 with the purpose of implementing the EU Cybersecurity Reserve and establishing a cyber situation and analysis centre;
- an instalment of EUR 3.6 million finances the activities agreed under the contribution agreement signed on 16 December 2025 with the purpose of setting up a European cybersecurity support centre for hospitals and healthcare providers.

During 2020–2025, the EU budgetary contribution (including European Free Trade Association funds) for ENISA increased from EUR 21.1 million to EUR 26.7 million (or by 22.6 %).

Over this five-year period, ENISA increased its commitment rate from 97.35 % to 99.96 %.

In 2025, ENISA concluded 33 public procurement procedures: 17 using an open procedure (51.5 %), 13 through the reopening of competitions under framework contracts (39.4 %), two through an

exceptional negotiated procedure without publishing a contract notice as per Article 11(1) of Annex I of the agency's financial regulation (6.1 %) and one using a restricted procedure (3.0 %).

In 2025, the agency did not pay any interest on late payments.

The table below shows ENISA's budget implementation targets and achievements in 2025, which remained at the same high level as in 2024.

AREA	OBJECTIVE	LEVEL OF COMPLETION IN 2024 (%)	2025 TARGET (%)	LEVEL OF COMPLETION IN 2025 (%)
Budget implementation (appropriations committed through the year)	Efficiency and sound financial management	100.00	95	99.96
Payments against appropriations of the year (C1 funds)	Efficiency and sound financial management	83.05	80	84.64
Payments against appropriations carried over from the previous year (C8 funds)	Efficiency and sound financial management	96.19	95	97.61

Budget execution of EU subsidy (C1 funds for 2025)

From 1 January to 31 December 2024, ENISA executed EUR 26 704 584 in commitment appropriations, representing 99.96 % of the total budget for the year, and EUR 22 609 962 in payment appropriations, amounting to 84.64 % of the total budget.

Commitment execution was maintained at a high rate (99.96 %) in 2025, compared with 100.00 % in 2024 (and 100.00 % in 2023). Overall, payment execution improved slightly, reaching 84.64 % (compared with 83.05 % in 2024).

The target of 95 % for the commitment rate, set by the Commission (DG Budget), was reached. The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not paid at the end of 2025 were carried forward to 2026.

The table below summarises the execution of ENISA's budget in 2025.

2025 BUDGET IMPLEMENTATION						
AREA OF BUDGET ALLOCATION	APPROPRIATION AMOUNT (EUR)	COMMITMENT AMOUNT (EUR)	PERCENTAGE COMMITTED	PAYMENT AMOUNT (EUR)	PERCENTAGE PAID	AMOUNT CARRIED FORWARD TO 2026 (EUR)
	(1)	(2)	(2)/(1)	(3)	(3)/(1)	(2)–(3)
Title I	15 486 205	15 486 005	100.00	14 841 454	95.84	644 551
Title II	4 362 727	4 362 727	100.00	2 952 729	67.68	1 409 997
Title III	6 865 400	6 855 852	99.86	4 815 779	70.15	2 040 073
Total	**26 714 332**	**26 704 584**	**99.96**	**22 609 962**	**84.64**	**4 094 622**

Amended budget / budgetary transfers

According to Article 26 of ENISA's applicable financial regulations, the Executive Director may transfer appropriations:

a. from one title to another, up to a maximum of 10 % of the appropriations for the financial year shown on the line from which the transfer is made;

b. from one chapter to another and within each chapter, without limit.

Beyond these limits, the Executive Director may propose transfers of appropriations from one title to another to the MB. The MB has two weeks to oppose the proposed transfers. After that time, the proposed transfers will be deemed to be adopted.

During 2025, ENISA's budget increased by EUR 284 089 as part of the EU's first general budget amendment to support salary indexation ([37]). The MB decision on Amending Budget 1/2025 of 20 November 2025 was adopted accordingly, allocating the additional funding to cover personnel costs.

In 2025, ENISA received a total amount of EUR 28.1 million under various contribution agreements signed with DG Communications Networks, Content and Technology, in which agreed actions span multiple years. It should be noted that an instalment of EUR 3.6 million covering the activities agreed under the contribution agreement signed on 16 December 2025 with the purpose of setting up a European cybersecurity support centre for hospitals and healthcare providers was received on 23 December 2025; therefore, this amount was not included in Amending Budget 1/2025. A total of EUR 28.1 million of funds received were accounted as R0 funds under Title IV.

During 2025, the agency made two transfers by Executive Director decision in the amended budget (for comparison, the Executive Director also made two transfers in the budget for 2024).

Transfers in the 2025 budget included the transfer of funds within titles and between titles. Funds were moved from Title I and Title III to Title II to finance long-planned corporate ICT-related projects.

The table below summarises changes to the 2025 budget.

2025 BUDGET, (EUR)	INITIAL BUDGET	AMENDING BUDGET 1/2025	TRANSFERS APPROVED BY THE EXECUTIVE DIRECTOR	FINAL BUDGET
Title I	15 271 440.00	284 089.00	−69 325.16	15 486 203.84
Title II	4 159 348.00	—	203 378.81	4 362 726.81
Title III	6 999 454.00	—	−134 053.65	6 865 400.35
Title IV	—	24 523 333.00	—	24 523 333.00
Total	**26 430 242.00**	**24 807 422.00**	**0.00**	**51 237 664.00**

Carry-forward of commitment appropriations

The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not consumed by payments at the end of 2024 were carried forward to 2025 (C8 appropriations).

In 2025, overall payment execution for C8 funds reached 97.61 %, with payment rates of 97.90 % for Title I, 97.68 % for Title II, 97.39 % for Title III and 98.52 % for Title IV.

Compared with 2024, there was an increase in payment execution for the implementation of C8 funds, from 96.19 % to 97.61 %.

Payments cancelled total EUR 110 160, which represents 2.39 % of the total amount carried forward.

A large part of the amount cancelled had been provisionally committed to missions, events, website maintenance services and EUDIR development services. The amounts had to be modified due to unexpected circumstances. In addition, rental costs for ENISA's Brussels office and related facilities costs, expenses associated with DG Human Resources and Security's handling of complaints, insurance and facilities management expenses for the agency's buildings in Athens and Heraklion, and other items had to be modified as the actual amounts were lower than anticipated. Moreover, costs associated with the provision of medical services (pre-recruitment medical visits, psychosocial interventions, etc.) and various training sessions were challenging to estimate accurately.

The table below summarises the execution of the C8 budget per title in 2025.

Further financial information can be found in Annex II.

[37] Definitive Adoption (EU, Euratom) 2025/31 of the European Union's annual budget for the financial year 2025, OJ L, 2025/31, 27.2.2025, ELI: http://data.europa.eu/eli/budget/2025/31/oj.

IMPLEMENTATION OF C8 FUNDS

2025 budget (C8 funds) (EUR)	Appropriations carried forward from 2024 to 2025 (EUR)	Payment amount (EUR)	Percentage paid	Amount cancelled (EUR)
Title I	884 337.50	865 810.16	97.90	18 527.34
Title II	1 661 539.29	1 623 002.30	97.68	38 536.99
Title III	2 001 712.56	1 949 517.07	97.39	52 195.49
Title IV	60 859.78	59 959.78	98.52	900.00
Total	**4 608 449.13**	**4 498 289.31**	**97.61**	**110 159.82**

2.5. Delegation and subdelegation

As per Articles 39 and 41 of ENISA's applicable financial rules, 'the Executive Director shall perform the duties of authorising officer. He or she shall implement the revenue and expenditure of the budget in accordance with the financial rules'. In addition, 'the Executive Director may delegate the powers of budget implementation to staff of the Agency to the conditions he shall define and within the limits laid down in the instrument of delegation'.

ENISA's internal structure was revised in 2025, with the reorganisation taking effect as of 1 January 2025. This revision introduced the role of the Chief Cybersecurity and Operations Officer (COO), who assists in the coordination of the operational activities of the agency and supports the Executive Director in fulfilling their responsibilities, as outlined in Article 20(3)(c), (d) and (e) of the CSA. By Executive Director Decision No 2025-41, the COO is delegated as Authorising Officer on behalf of the Executive Director for budget transfers between budget lines within Title III, including the release of funds from operational missions and large-scale events to local lines, to be managed by heads of unit and deputy heads of unit.

Heads of units are, under the same decision, delegated as authorising officers on behalf of the Executive Director for amounts up to EUR 1 million) for:

- all transaction types, including budget transfers between local budget lines of an activity they manage within a single title and budget line (i.e. budget transfers between titles and between budget lines are not allowed);
- all amounts;
- all budget lines for which they have been assigned as budget managers [38]; or all relevant budgetary implementing actions for activities or outputs of the SPD for which they are responsible, including all activities related to tendering and contracting.

Deputy heads of unit are also delegated as authorising officers on behalf of the Executive Director for amounts up to EUR 1 million.

In accordance with Article 41(2) of the ENISA's financial rules, heads of unit may, with the explicit agreement of the Executive Director, further subdelegate their financial rights to heads of sector, with a financial limit of up to EUR 500 000 for all relevant budget lines, subject to certain conditions outlined in Executive Director Decision No 2025-41. If a head of unit is absent, for the duration of their absence the delegated transfers may not exceed EUR 1 million. The acceptance of delegation should be signed off by the Authorising Officer by delegation or subdelegation.

As provided for in Article 45(7) of ENISA's financial rules, non-staff actors can take on the role of financial initiating agents, with a financial limit of up to EUR 50 000. For amounts exceeding this limit, non-staff actors need to be granted annual explicit authorisation by the relevant Authorising Officer by delegation, subject to the following conditions.

- They can be granted access to specific budget lines with a financial limit of up to EUR 200 000 to perform their duties in processing transactions in the financial IT system.
- The Authorising Officer by delegation has to nominate a staff member who will, at least on a quarterly basis, monitor and assess the performance of the non-staff actor based on the KPIs established in the last paragraph of Article 45. The staff member needs to accept the nomination,

[38] Including off-budget lines (HB).

as adherence to the KPIs by the non-staff actor will be taken into account in assessing the performance of the nominated staff member in their annual career development reports.

Detailed tasks and responsibilities are provided in the annexes of Executive Director Decision No 2025-41, along with a list of actors that are covered by the decision.

In the event of a change in the person of the Executive Director, all delegations (and sub-delegations) would become automatically null and void after 90 days from the date on which the new Executive Director takes up their duties, unless the continuation of delegated authority is explicitly confirmed by the newly appointed Executive Director. Checks on these delegation rights are carried out through a periodic review of the access rights granted to the accrual-based accounting system within the main financial system and are shared on an annual basis with the Commission (DG Budget).

2.6. Human resources management

On 1 January 2025, a new organisational structure came into effect. The agency continued to follow its defined HR strategy, which was first implemented in 2024, by further streamlining and professionalising the main HR processes: performance management and reclassification processes were revised, by clarifying, harmonising and quantifying the processes, facilitating qualitative improvement and validation. The framework is now set for the coming years.

2025 was the year of further digitalising and improving HR services. The basic structure of the HR service desk was re-established, with a second line of HR advisors that support the development, implementation and monitoring of HR policy. Internal processes were streamlined and codified, and HR business partners focused on the provision of services by operational and corporate units.

In 2025, the HR archive of Heraklion was reassessed and transferred to Athens, personal files were digitalised to increase the digitalisation of systems, and smart system use led to the collection of more and better HR data, which will form the backbone of HR dashboards to be created in 2026 to further professionalise services.

The workforce was assessed, taking into account the limited resources and growing mandate of the agency. Three posts were reprofiled (meaning post profiles were adapted and staff members holding the post were supported with on-the-job training and learning to enter their new role. Six posts were restructured, meaning that existing contracts were either not renewed or ended, to address critical and high-priority business needs that demanded new profiles. The rate of fulfilment of plans was 97 %.

The agency increased its efforts to improve staff engagement through the introduction of a user-friendly staff engagement tool, that is, a jointly developed roadmap for promoting staff engagement with the involvement of senior leadership, management, staff and the Staff Committee. The tool increased participation in ENISA's staff satisfaction survey to 80 % and improved satisfaction over the six areas covered by the survey.

Staff well-being was closely monitored and supported by training, unit away days, an open-door policy and roadmap update sessions.

Overall, in 2025, ENISA welcomed 21 new staff members: 6 temporary agents, 11 contract agents (out of which 5 were hired under various contribution agreements) and 3 SNEs.

Seven vacancy notices were published by ENISA in 2025, which resulted in the compilation of seven applicant reserve lists, expected to cater for emerging staffing needs in the next two years.

The sharing of reserve lists through EUAN has become common practice. In 2025, this sharing will result in the signing of a memorandum of understanding in the context of EUAN, further professionalising efficient and (cost-)effective recruitment of staff, and promoting EUIBAs as employers of choice, while supporting the geographical balance of EUIBAs.

The following table presents the performance of HR services in relation to their KPIs in 2025.

AREA	OBJECTIVE	2024 PERFORMANCE	2025 PERFORMANCE	2025 TARGET
Efficient management of selection procedures	Time taken to hire (in line with the standard EU HR definition, this is the time frame from the deadline set in the vacancy notice for candidates to submit applications until the signing of the reserve list by the Executive Director)	≤ 5 months (4.8 months)	4.1 months	≤ 5 months
Staff turnover	Reduced turnover rate of statutory staff (temporary agents and contract agents)	4.49 %	6.42 %	< 5 %
Management of staff performance	Implementation and monitoring of the appraisal and reclassification exercises	100 %	100 %	100 %

Implementing rules adopted in 2025

In response to the Commission decision of 12 December 2023 on the prevention of and fight against psychological and sexual harassment, and repealing Decision C(2006) 1624/3, the agency asked the Commission for a derogation, awaiting the draft model decision for agencies that will be negotiated by the Standard Working Party. The agency expected the model decision for agencies to be ready for adoption in 2025; however, the negotiations took longer and no common ground was found on the draft. In 2026, the Standard Working Party will aim to draft a service-level agreement that could be used in addition to the Commission decision by analogy, which may provide a way forward.

In July 2025, the agency decided to change its course with regard to the applicable rules on administrative inquiries and disciplinary proceedings, as the then-applicable MB Decision No MB/2020/13, applying, by analogy, the Commission decision of 2019 laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings, was not deemed appropriate for the agency owing to its small size. As the Commission reached an *ex ante* agreement on the possibility of adopting a draft model decision tailored to agencies under Commission Decision C(2022) 497 of 25 January 2022, the MB decided to adopting this decision by analogy, ensuring that there is no legal vacuum in applying provisions on the conduct of administrative inquiries and disciplinary proceedings, as requested by ENISA's staff regulations.

Brief description of the results of the screening/ benchmarking exercise

In 2025, ENISA continued to apply a benchmarking exercise following the methodology of the Commission. The third table in Annex IV depicts the results of the exercise based on the type of post: administrative support and coordination, operational or neutral. The proportion of posts described as involving administrative support and coordination increased slightly, to 24.5 %. A slight decrease can be observed in posts classified as operational, estimated to account for 68.9 % of posts. The remaining 6.6 % of posts were defined as neutral posts. For the purpose of this exercise, staff posts were counted, including staff financed by contribution agreements, along with interim appointments and *intra muros* posts.

2.7. Strategy for efficiency gains

The agency continued its efforts to improve efficiency gains in 2025. Actions included ENISA's collaboration with EIT and EFSA to develop shared service capabilities at the EU agencies network level. The three agencies agreed to dedicate resources and provide services to each other on the basis of a service catalogue including cybersecurity (ENISA), legal support (EIT) and HR (EFSA). The EUAN Shared Support Office EU agencies network shared support office was assigned as project manager for this pilot initiative. In the event of successful outcomes, it is envisaged that shared service capabilities will be upscaled and opened up to more EU agencies.

In addition, the agency's annual work programme was implemented with the support and guidance of ENISA's statutory bodies, such as the NLO network and the Advisory Group, including specialised expert groups. These bodies support the agency to build synergies and avoid duplicating Member States' activities.

2.8. Assessment of audit and *ex post* evaluation results during the reporting year

Internal Audit Service

In March 2025, the IAS shared its strategic audit plan, which outlines the agency's main risks and determines the prospective audit topics for 2025–2027. No audits were carried out in 2025.

European Court of Auditors

In October 2025, the ECA issued its report on the 2024 annual accounts of the agency [39]. According to the court, the accounts of the agency for the year ending 31 December 2024 fairly present (a) the financial position of ENISA on this date; (b) the results of its financial operations; (c) its cash flows; and (d) changes in its net assets for that year, in accordance with the applicable financial regulation and with the accounting rules adopted by the Commission's accounting officer. Moreover, revenue and payments for accounts in the year ending 31 December 2024 are legal and regular in all material respects.

Moreover, ECA's 2024 report issued five non-critical observations related to (a) the lack of proper financing decisions prior to launching procurement procedures for operational expenditure, (b) weaknesses in the organisation of conferences, (c) a lack of sufficient documentation to justify the estimated contract value of procurement procedures, (d) high rates of carrying over amounts committed from 2024 to 2025 and (e) an above-threshold rate of late payments. These five observations have been addressed by the agency and the effectiveness of associated measures will be assessed by the ECA in its 2025 report.

Ex post evaluation results

In 2025, ENISA started its *ex post* checks of financial transactions made during the 2024 financial year, in accordance with Article 45(8) and (9) of the agency's financial regulation. The checks were finalised in early 2026. A total of 119 financial transactions were scrutinised, representing 5.97 % of the agency's transactions and 7.33 % of the its budget (excluding salaries and related staff expenditure, as per the *ex post* control methodology). The results identified non-critical weaknesses, further confirming the issue of late payments (10 payments out of 119, or 8.4 %). Other weaknesses included a lack of proper documentation, *a posteriori* (legal or financial) commitments and other non-critical weaknesses. It is important to note that most of these clerical weaknesses did not have any adverse impacts on ENISA's finances and did not alter the effective delivery of services/goods by the agency's contractors.

2.9. Follow-up on recommendations and action plans for audits and evaluations

Internal Audit Service

At the end of 2025, one important recommendation was still unactioned. The recommendation is related to the delayed implementation of the newly adopted policy on remunerated experts, for which a new call for interest is expected to take place in 2026. Only then will ENISA be able to provide sufficient evidence to verify the effective implementation of the principles and rules established in the policy.

European Court of Auditors

Out of five recommendations arising from previous ECA audits (prior to financial year 2024), two were formally closed by the ECA in 2025.

The three recommendations that are still open are related to (a) the usage of non-staff actors to initiate financial transactions, (b) the incompatible and overlapping responsibilities between the roles of accounting officer and internal control coordinator and (3) the high rate of late payments.

ENISA is confident that the observation on late payments was fully addressed in 2025, while the role of the internal control coordinator was further clarified. Regarding the usage of non-staff actors, ENISA is addressing the observation with great diligence, but a long-term solution must be found to fully tackle the root of the problem, partially explaining the postponement of the resolution of this particular audit observation.

[39] https://www.eca.europa.eu/ECAPublications/SAR-AGENCIES-2024/SAR-AGENCIES-2024_EN.pdf#page=98.

2.10. Follow-up on recommendations issued following investigations by the European Anti-Fraud Office

The agency has carried out all actions previously requested by the European Anti-Fraud Office, and no obligations, follow-up actions or recommendations are pending.

2.11. Follow-up of observations from the discharge authority

In response to observations and comments made by the European Parliament in its discharge of 2024, the agency provided further information on actions taken to address previously identified areas for improvement, in particular corrective actions to address the weaknesses identified by the ECA (as described in Section 2.9.2), and highlighted actions it had taken that are of interest to the European Parliament (related to efficiency gains, important achievements during the year, public procurement, fulfilment of the staff establishment plan and the underlying gender and nationality balance, diversity and inclusion, etc.)

On 29 April 2026, the Parliament granted 'the Executive Director of ENISA discharge in respect of the implementation of the Agency's budget for the financial year 2024' and approved 'the closure of the accounts of ENISA for the financial year 2024[40].

2.12. Environmental management

In 2025, ENISA consolidated its position on environmental management. In February 2025, the agency concluded its development of its first environmental statement and its evaluation of an external verification.

In September 2025, ENISA submitted its environmental declaration for 2024 to the Hellenic Competent Authority in view of the agency's addition to the EMAS register, validated by the verification body TÜV Austria. In January 2026, the agency's EMAS registration was completed (registration number EL-000124)

2.13. Assessment by management

The agency's operational and corporate activities were implemented in accordance with the 2025 work programme, with the necessary guidance and support of the MB. ENISA conducts its operations openly in compliance with relevant legal requirements through the management team, which monitors the implementation of operational and corporate projects on a weekly basis through team meetings.

The agency regularly monitors the implementation of its action plans based on ECA and IAS recommendations. In 2025, ENISA implemented corrective actions addressing all recommendations from previous years, and a review of ENISA's internal control framework did not reveal any significant shortcomings. The budget was implemented in accordance with the principles of sound financial management, in particular with regard to the checks and control procedures performed by agency staff and supported by an assessment of the effectiveness of the internal control framework (presented in Part III). ENISA's management has reasonable assurance that the components and principles of internal control have been followed.

(40) https://www.europarl.europa.eu/doceo/document/TA-10-2026-0136_EN.html

II

PART II (b)

EXTERNAL EVALUATIONS

The European Commission performed an evaluation ([40]) of ENISA and the European Cybersecurity Certification Framework (ECCF) and published its findings on the 20 January 2026. The findings, conclusions and recommendations are presented in the following sections.

2.14. ENISA

The main findings of the evaluation of ENISA focused on its effectiveness, efficiency, relevance, coherence and the added value it brings to the EU's cybersecurity landscape. Additionally, a closer examination of the internal governance and practices of the agency were provided to shed light on its operational dynamics and areas for improvement (see the conclusions and recommendations below).

In terms of effectiveness, the evaluation report highlighted that ENISA has fulfilled its mandate by delivering nearly all planned outputs. During the evaluation period, from 2017 to 2023, ENISA demonstrated efficient operations under its existing governance structure. ENISA's relevance within the cybersecurity domain was underscored by its responsiveness to evolving stakeholder needs and its flexibility to adapt to the changing landscape. In assessing ENISA's coherence, the evaluation highlighted both strengths and areas for improvement. In terms of added value, ENISA significantly contributed to enhancing the EU's cybersecurity ecosystem, although there are ways in which its impact could be amplified.

Conclusions and recommendations

The evaluation of ENISA highlighted its crucial role in working towards a cohesive cybersecurity landscape across the EU. ENISA has shown effectiveness and generated valuable outputs.

- As demands on ENISA continue to grow, it is important to reassess and streamline its operations to better align resources and priorities, with continued emphasis on supporting Member States to address cybersecurity threats and enhance their cybersecurity infrastructures.

- By refining its report production process, ENISA could make outputs more user-friendly and accessible through visual aids, and concise summaries could enhance the agency's effectiveness and relevance in the current threat landscape.

- Strengthening communication channels is essential to ensure ENISA's activities and services are clearly

[40] Report from the Commission to the European Parliament and the Council on the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework, COM(2026) 9 final of 20 January 2026, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2026:9:FIN.

visible to stakeholders, including industry players. A well-defined communication strategy could aid in fostering stronger connections and cooperation within existing cybersecurity networks such as ISACs.

- ENISA could improve its efficiency by placing a more strategic focus on task prioritisation, enabling a more streamlined approach to managing workload pressures.

- To improve relevance among stakeholders, ENISA's central role in supporting Member States should continue to be elevated by strengthening its capacity to provide timely insights into emerging threats and strategic tools for addressing them.

- Moreover, as indicated by a number of stakeholders, ENISA could establish more structured and transparent methods of engaging with private entities, including SMEs.

- Clarity should be sought regarding ENISA's role in policy implementation alongside other EU institutions, ensuring that collaboration with Member States is at the forefront of efforts to reinforce the cohesion of the EU's unified cybersecurity strategy. This would include strengthening cooperation with other EU agencies and seeking synergies with other cybersecurity bodies to implement joint actions to enhance operational coherence across Europe.

Overall, maintaining ENISA's status as a specialised agency within the EU is important, as it ensures continued focus on cybersecurity priorities. These recommendations aim to enhance ENISA's capacity to effectively manage its responsibilities and reaffirm its role as a leading entity in the area of cybersecurity.

2.15. European cybersecurity certification framework

This section provides the main findings of an evaluation regarding the ECCF, focused on its effectiveness, efficiency, relevance, coherence and the added value it brings to the EU's cybersecurity landscape. Additionally, it summarised the main strengths and weaknesses of the framework, identified based on a SWOT (strengths, weaknesses, opportunities and threats) analysis.

In terms of effectiveness, a significant shortcoming of the current ECCF is its inability to effectively address the fragmentation of certification schemes across the EU, mainly due to procedural limitations. This fragmentation has persisted despite the framework's intention to harmonise certification processes, leading to inconsistency and inefficiency in cybersecurity assurance.

The efficiency of the ECCF has been subject to scrutiny, given the extended timelines for the adoption of cybersecurity certification schemes and the myriad complexities involved. Despite its strategic intention to streamline the certification process across the EU, the ECCF's efficiency was notably hampered by drawn-out discussions and preparation phases that culminated in significant delays; the first scheme was only adopted in early 2024, nearly five years after its implementation. These protracted timelines can be attributed to multifaceted challenges encompassing both political and technical dimensions.

The ECCF emerges as a crucial response to the growing complexity and sophistication of cyber threats across the EU, aspiring to establish harmonised cybersecurity certification schemes that assure trust and foster a secure digital market. Despite the framework's promising premise, its relevance is still considered more potential than practical, with certification schemes only recently becoming operational.

The ECCF's coherence is also affected by the lack of clear accountability mechanisms, which has led to difficulties in aligning its objectives with other legislative measures. This misalignment risks creating overlaps and inefficiencies in the cybersecurity landscape. The complete coherence of the ECCF with other EU legislative instruments, including the NIS 2 Directive and the CRA, is crucial to ensuring a unified cybersecurity approach.

Despite the potential of the ECCF, the framework struggled to deliver its added value in fostering a unified and effective cybersecurity environment across the EU. The ECCF sought to significantly enhance the EU's cybersecurity landscape by introducing an unprecedented development procedure and governance structure for certification processes.

Conclusions and recommendations

The evaluation of the ECCF produced several strategic recommendations.

Despite ENISA's pivotal role in fostering cooperation and operational cohesiveness among Member States and other stakeholders, constraints on the efficiency and effectiveness of the ECCF have been evident, mainly due to the complexities of scheme adoption processes. These issues highlight the need

for substantial revision of governance structures to enhance operational clarity and accountability at all levels. To address these findings, several actions are recommended to optimise ENISA's contribution to the ECCF.

- There should be a concerted effort to ensure the consistent and adequate distribution of financial and human resources across ENISA and other stakeholders within the ECCF.
- Stabilising employment arrangements is essential to reduce turnover and enhance institutional memory, thereby facilitating efficient scheme implementation and ongoing maintenance.
- Developing streamlined decision-making processes within the ECCF, which clarify roles and responsibilities, will promote transparency and efficiency, particularly in enhancing collaborative efforts among Member States, the Commission and ENISA. This will foster accountability and reduce inefficiencies.
- A commitment to setting and adhering to realistic timelines for the development and implementation of certification schemes is essential. This involves supporting detailed technical analysis and bolstering preparatory efforts to effectively anticipate and mitigate political influences.
- Actively investing in the training and retention of skilled personnel within ENISA is crucial to ensuring continuity and expertise when navigating complex cybersecurity challenges. Long-term workforce stability will be vital to maintaining the ECCF's operational efficacy.
- Industry and consumer awareness should be increased through targeted campaigns and strategic involvement, emphasising the value of certified products and services. A proactive approach to garnering stakeholder support is critical to boosting demand and trust in ECCF initiatives.

The agency acknowledges and welcomes the findings of the external evaluation, including its conclusions and recommendations. ENISA is committed to giving these due consideration and to undertaking appropriate, concrete and time-bound actions to address the areas identified for improvement.

The agency notes that a number of the issues highlighted had already been recognised internally, and steps had already been taken to address them prior to the evaluation. In this regard, the evaluation provides valuable external validation that these efforts were appropriately targeted and that ENISA is progressing in the right direction.

Moving forward, the agency will build on these ongoing efforts to ensure that the evaluation's recommendations are integrated into its planning and implementation processes.

III

PART III

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

3.1. Effectiveness of internal control systems

Internal control is established in the context of ENISA's fundamental budgetary principles and associated with sound financial management. Internal control is broadly defined in the agency's financial regulation as a process designed to provide reasonable assurance of achieving objectives. This definition very much mirrors the standard definition of internal control adopted by the Committee of Sponsoring Organizations of the Treadway Commission (https://www.coso.org).

In this context, ENISA adopted its internal control framework by MB Decision No MB/2019/12 and amending MB Decision No MB/2022/11. It is based on the relevant framework of the Commission (which follows the Committee of Sponsoring Organizations of the Treadway Commission framework) and includes 5 internal control components and 17 internal control principles. The five internal control components are the building blocks that underpin the structure of the framework; they are interrelated and must be present and effective at all levels of ENISA for internal control over operations to be considered effective. Each component comprises one or more internal control principles. Applying these principles helps to provide reasonable assurance that ENISA's objectives have been met. The principles specify the actions required for the internal control to be effective.

To assess the components and principles of the internal control framework, a set of 66 indicators was adopted (as amended by MB Decision No MB/2022/11). The indicators are assessed individually and supported by the relevant evidence. The assessment of the internal control is an important part of ENISA's internal control framework, and it is conducted on an annual basis. For 2025, this assessment was based on the indicators of the framework, and also on additional information from specific (risk) assessment reports, audit findings and other relevant sources. The assessment also followed the related guidance and templates developed through the EU agencies' Performance Development Network.

Assessment of control environment component

The control environment component consists of five principles, as described below.

Principle 1 – ENISA demonstrates commitment to integrity and ethical values

The assessment concluded that this principle is present and functioning, but some improvements are needed, mainly in the area of training sessions on ethics and integrity for staff, in order to attain a sufficient rate of participation in these training sessions.

Principle 2 – ENISA's management exercises responsibility for overseeing the development and performance of its internal control systems

The assessment concluded that this principle is present and functioning well but some improvements are needed. ENISA's management is regularly updated on the result of its internal controls; however, the recommendations should be more actively and formally followed up, in order to improve the overall effectiveness of ENISA's internal control systems. A need to strengthen the internal control resources is observed.

Principle 3 – ENISA's management establishes structures, reporting lines and appropriate authorities and responsibilities in pursuit of the agency's objectives

The assessment concluded that this principle is present and functioning well, and only minor improvements are needed. On a regular basis, the agency publishes on its intranet the adopted and updated organisation charts. Delegation of authority is clearly documented and regularly updated by means of various Executive Director decisions, notably on specifying the roles and responsibilities of ENISA's structural entities and on a framework for the financial delegation of the Authorising Officer.

Principle 4 – ENISA demonstrates commitment to attracting, developing and retaining competent individuals in alignment with its objectives

The assessment concluded that this principle is present and functioning well. One minor improvement is needed, in the area of learning opportunities for ENISA's staff, which should be more comprehensive to ensure that all needs are catered for. The planned training and competency development as reported in the annual career development assessment of each staff member should be better followed up in order to ascertain that staff members develop the agreed skills and competencies in alignment with their objectives.

Principle 5 – ENISA holds itself accountable for its internal control responsibilities in pursuit of the agency's objectives

The assessment concluded that this principle is present and functioning well. The agency has defined clear roles and responsibilities and holds individuals and entrusted entities accountable for the performance of internal control responsibilities across the organisation and for the implementation of corrective action as necessary. Moreover, as part of its internal controls, the agency regularly reviews and monitors its annual objectives to ensure that preset objectives will be reached.

Assessment of risk assessment component

The risk assessment component consists of four principles, as presented below.

Principle 6 – ENISA specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives

The assessment concluded that this principle is present and functioning well. Predefined targets for annual objectives are set in the SPD. ENISA's SPD is drafted based on input from all units and teams across the agency, and in consultation with stakeholders, before it is formally adopted by the agency's MB. Throughout the year, the agency's outputs are planned, reviewed and finalised in close consultation with stakeholders, including ENISA's MB, the advisory group and the NLO network. ENISA uses its objectives as a basis for allocating resources to achieve policy, operational and financial performance goals.

Principle 7 – ENISA identifies risks to the achievement of its objectives across the organisation and analyses risks as a basis for determining how the risks should be managed

The assessment concluded that this principle is present and functioning well, but improvement is needed in the follow-up of implementation of mitigating measures. An enterprise risk assessment, based on the Commission's risk assessment guidance, and a dedicated IT security risk assessment are performed on an annual basis. As regards these assessments, no critical risks were identified in 2025. The identified risks are reported in a corporate risk register, and high-priority risks are reported to ENISA's management team to take the relevant corrective actions. However, due to lack of resources, corrective actions are not always properly followed up to ascertain that their implementation is sufficiently effective to significantly reduce the identified risk(s).

Principle 8 – ENISA considers the potential for fraud in assessing risks to the achievement of objectives

The assessment concluded that this principle is present and functioning well. The revised anti-fraud strategy for 2025–2027 was adopted by MB Decision 2025/03. A dedicated anti-fraud web page is available on ENISA's intranet, where all staff can access relevant regulations, documents and training material. Training in fraud prevention, which forms part of training in ethics and integrity, is delivered regularly (however, the participation rate should be improved).

Principle 9 – ENISA identifies and analyses significant change

The assessment concluded that this principle is present and functioning well and that only minor improvements are needed. Change is managed through various processes within the agency. At the operational level, continuous monitoring of the work programme activities in the weekly management team meetings enables the identification and analysis of any significant change (thus enabling further reflection of this change in internal activities). This allows ENISA to identify new challenges and to quickly react by adapting itself to best meet the underlying objectives and to best deliver additional tasks entrusted to ENISA.

Assessment of control activities component

The control activities component consists of three principles, as presented below.

Principle 10 – ENISA selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to an acceptable level

The assessment concluded that this principle is present and functioning; however, following up on identified deficiencies has been slow, while deeper assessments of and awareness raising on internal controls in specific areas cannot be performed in a comprehensive way due to lack of resources.

In this context, one failure of internal controls was observed with the publication of the ENISA's Threat Landscape 2025 report without proper content validation. In this case, AI-generated and hallucinated links to existing content were not captured within the Agency before publication. As a follow-up measure, ENISA adopted its AI policy in early 2026 and further internal controls have been put in place to ensure compliance and alignment on the use of AI across the Agency

Principle 11 – ENISA selects and develops general controls on technology to support the achievement of objectives

The assessment concluded that this principle is present and functioning, but some improvements are needed. Efforts to mitigate IT risks yielded results in 2025, leading to the partial mitigation of certain identified risks. However, some IT risks are of a continuous nature, such as the risks stemming from cybersecurity threats, which are constantly evolving. The agency's cybersecurity maturity plan is the response to these risks; the plan's efficiency still needs to be demonstrated.

Principle 12 – ENISA deploys control activities through policies that establish what is expected and through procedures that put policies into action

The assessment concluded that this principle is present and functioning, but some improvements are needed. In particular, recurrent weaknesses identified by internal control tools (e.g. the registry of exceptions) in previous years have not yet been effectively addressed. For example, from the analysis of the 2025 register of exception, out of 21 non-compliant events (i.e. exceptions), the majority (12) concerned a posteriori transactions (i.e. the budgetary and/or legal commitment(s) was (were) not compliant with EU financial rules at the moment of the processing of the financial transaction). Although these exceptions are mainly related to minor errors and did not adversely (financially or operationally) impact ENISA, this weakness had already been identified by control activities in previous years, but no specific procedure had been introduced to further mitigate this usually minor risk.

Moreover, on the registry of exceptions, one exception was assessed as high risk. This exception is related to the participation (financially and physically) of ENISA in a conference in an EU neighbouring country, for which an explicit financing decision was missing. This was an *ex ante* exception that was endorsed in order to support the security of the neighbouring country. Additionally, three other material risks have been identified and reported as exceptions to ENISA's legal frameworks: two are related to the erroneous use of budget carried forward from 2024 to 2025, and the last one is an ineligible cost reimbursement, which was granted in an exceptional context.

Assessment of information and communication component

The information and communication component consists of three principles, as presented below.

Principle 13 – ENISA obtains or generates and uses relevant high quality information to support the functioning of its internal control systems

The assessment concluded that this principle is present and functioning, and only minor improvements are needed. For example, internal information sharing and the mapping of information could be improved, and compliance with the need-to-know principle (to access internal information) needs further monitoring.

Principle 14 – ENISA communicates information internally, including objectives and responsibilities for internal control, that is necessary to support the

functioning of its internal control systems

The assessment concluded that this principle is present and functioning well. Through the minutes of the weekly management team meeting which are made available by email to all staff, ENISA's management essentially communicates internally and regularly about its objectives, challenges, actions taken and results achieved. In addition, frequent Q & A sessions for all staff on various relevant topics were held during 2025. Moreover, there is a separate communication line for whistleblowing arrangements, to ensure information flow when normal channels are ineffective.

Principle 15 – ENISA communicates with external parties about matters affecting the functioning of its internal control systems

The assessment concluded that this principle is present and functioning well. ENISA communicates its activities in a transparent way and in line with internal control principles. In particular, ENISA regularly communicates with external parties on the functioning of its internal controls.

Assessment of monitoring activities component

The monitoring activities component consists of two principles, as presented below.

Principle 16 – ENISA selects, develops and conducts ongoing and/or separate assessments to ascertain whether the components of internal control are present and functioning

The assessment concluded that this principle is present and functioning, but some improvement is needed, mainly in the area of timely follow-up of recommendations issued by internal controls (as mentioned in previous sections).

Principle 17 – ENISA assesses and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management as appropriate

The assessment concluded that this principle is present and functioning, but the effectiveness of the monitoring of mitigation measures remains to be demonstratedonclusions of the assessment of internal control systems

The overall assessment shows that the internal controls at ENISA provide reasonable assurance that policies, processes, tasks and behaviours of the agency, taken together, facilitate its effective and efficient operation, help to ensure the quality of internal and external reporting, and help to ensure compliance with its regulations. That being said, some improvements are needed in certain principles, in order to increase effectiveness and ensure proper implementation of the internal controls in the future. In particular, ENISA should further strengthen the internal control capacity of the agency, focus on deeper internal control assessments in specific areas and address internal controls at operational level beyond financial controls.

3.2. Statement of the Manager in charge of risk management and internal control

I, the undersigned,
Andreas MITRAKAS,

in charge of risk management and internal control within **ENISA**,

In my capacity as Head of Unit for Executive Directors Office in charge of risk management and internal control, I declare that in accordance with ENISA's Internal Control Framework, I have reported my advice and recommendations on the overall state of internal control in the Agency to the Executive Director.

I hereby certify that the information provided in the present Consolidated Annual Activity Report and in its annexes is, to the best of my knowledge, accurate, reliable and complete.

Andreas Mitrakas
Head of Unit for Executive Directors Office

Qualified electronic signature by: ANDREAS MITRAKAS

Date 2026-06-25 06:08:09 UTC

IV

PART IV

MANAGEMENT ASSURANCE

4.1. Review of the elements supporting assurance

The declaration of assurance, provided by the Authorising Officer, is mainly based on the following three pillars:

1. regular monitoring of the KPIs set for operational, administrative and financial tasks through the formal periodical management reporting,
2. effectiveness of the internal controls and processes to detect weaknesses and to identify areas for improvement,
3. assessment and reports from independent bodies (external evaluators, financial auditors (ECA, complemented by a private audit firm), internal auditors (IAS), etc.).

As highlighted in the previous sections, by the operational, administrative and financial KPIs, and by the positive opinion of the ECA on the reliability of the accounts and on the legality and regularity of the transactions underlying the accounts, and as no critical observations have been formulated by the IAS, the management has sufficient assurance that ENISA is adequately managed so as to safeguard its financial resources and to pursue the tasks with which it was entrusted.

4.2. Reservations

Considering the results of the 2025 annual audits performed by the ECA and the IAS, the 2025 results of the internal controls (*ex post* controls, review of the register of exceptions, the internal controls framework assessment) and the 2025 results of the key financial and operational indicators, the Authorising Officer can conclude that ENISA operated in 2025 in such a way as to manage the risks appropriately.

In addition, the Authorising Officer has reasonable assurance that the allocated resources were used for their intended purpose, in compliance with the legal framework and in accordance with the principle of sound financial management.

V

PART V

DECLARATION OF ASSURANCE

I, the undersigned,
Juhan LEPASSAAR,

Executive Director of the European Union Agency for Cybersecurity,

in my capacity as Authorising Officer,

Declare that the information contained in this report gives a true and fair ([42]) view of the state of the agency's affairs, and state that I have reasonable assurance that the resources assigned to the activities described in this report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

This reasonable assurance is based on my own judgement and on the information at my disposal, such as the results of the self-assessment, *ex post* controls, the work of the internal audit capability, the observations of the IAS and the lessons learned from the reports of the ECA for years prior to the year of this declaration.

I confirm that I am not aware of anything not reported here that could harm the interests of the agency.

Athens,
Qualified electronic signature by: JUHAN

LEPASSAAR

Date 2026-06-29 10:46:32 UTC

Juhan Lepassaar
Executive Director

[42] True and fair in this context means reliable, complete and accurate.

A

ANNEX I

CORE BUSINESS STATISTICS

Activity 1

ACTIVITY 1 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
1.1.	Stakeholders receive technical advice with the evidence needed for policymaking activities and the definition of implementation measures.	EU institutions (European Commission, European Parliament, Council of the European Union) NIS CG, including relevant workstreams NLOs, including relevant subgroups	Develop and pilot a peer review framework, including a code of conduct.	Biennial survey, annual dialogue and annual desktop research	By the end of 2025, both endorsed.	ENISA developed all peer review documentation and guidance, including the code of conduct, and all were endorsed by workstream 9.
1.2.			Assessment of ENISA advice on EU policy.		> 90 % stakeholder satisfaction	Survey planned for 2026.
1.3.			Assessment of timeliness of advice provided during policy development.		> 70 % stakeholder satisfaction with timeliness	100 % – fully achieved, as all Member States and the various EU networks have agreed with the consolidated findings. ENISA has also reviewed and validated them as part of its activities.

Activity 2

ACTIVITY 2 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
2.1. Support Member States in their implementation of the NIS 2 Directive.	The NIS 2 frameworks for risk management, security measures and incident reporting achieve harmonisation.	Directorate-General for Communications Networks, Content and Technology NIS CG	Framework usage.	Annual (internal count)	10 Member States to adopt, use or endorse the frameworks.	Parts of the 2 NIS 2 frameworks are adopted/ endorsed by the NIS CG.
			EUDIR used by all Member States.	Annual (report)	20 Member States to use EUDIR.	18 Member States use EUDIR.
			Alignment between DORA and the NIS 2 Directive.	Satisfaction survey	> 80 %	> 80 % of Member States say DORA is aligned with the NIS 2 Directive. 77 % of the finance sector use the NIS 2 Directive-implementation guidelines, which means better DORA–NIS 2 Directive alignment.
2.2. Support Member States with EU toolboxes, EU-coordinated risk evaluations and EU-coordinated preparedness tests.	Support is given to EU-wide risk evaluations and risk scenarios and their follow-up (5G, Nevers call). Coordinated risk assessment of critical supply chains is undertaken.	Directorate-General for Communications Networks, Content and Technology NIS CG	Risk assessment framework for critical supply chains.	Annual (internal count)	1 coordinated risk assessment per domain or sector.	2
			Number of sectoral situational awareness reports.	Annual (internal count)	12	12

2.3. Improve the cybersecurity and resilience of the NIS sectors.	Stakeholders use the NIS service packages to improve sectoral security and resilience.	Directorate-General for Communications Networks, Content and Technology NIS CG Sectoral EU ISACS Sectoral EU agencies	Number of critical sectors increasing in maturity (from build to sustain or involve – *NIS360*).	Annual (internal count)	5	8 sectors recorded improvements in maturity (3 advancing to the next band; 5 evolving within their existing band).
			Number and frequency of services or workflows delivered to NIS sectors according to the maturity of the sector.	Annual (internal count)	24	30 services were delivered to 10 NIS subsectors.
2.4. Perform an annual check on policy implementation.	Member States and EU institutions (both general and sectoral stakeholders) use the NIS Investments, the *NIS360* and the cyber posture briefs as reference documents for policymaking.	Directorate-General for Communications Networks, Content and Technology NIS CG Sectoral EU ISACS Sectoral EU agencies	Number of critical or essential sectors covered by NIS Investments.	Annual (internal count)	12 subsectors covered.	14 subsectors were covered (22 sectors and subsectors in total).
			Number of critical sectors assessed by the *NIS360* and cyber posture briefs.	Annual (internal count)	12	22 sectors and subsectors were covered by the *NIS360*; 3 sectors covered by cyber posture briefs.
			Implementation tracker.	Annual (internal count)	5 requests stemming from the implementation of the NIS 2 Directive in Member States.	N/A (initiative incorporated into 2026 NIS 2 hub).

Activity 3

ACTIVITY 3 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
3.1. Support the adoption and uptake of the ECSF.	Review and update the ECSF in line with the Cybersecurity Skills Academy Communication. Measure and report the skills gap, including developing indicators to be used for the cybersecurity index. Promote the adoption of the ECSF in Member States, in training organisations and academia. Regularly update the ECSF.	AHWG on Cybersecurity Skills ECCC WG 5 on Skills	Number of Member States endorsing the ECSF.	Annual	10	18
			Number of training organisations endorsing the ECSF in their training programmes.	Annual	15	26
3.2. Organise targeted exercises and support stakeholders to plan and execute their own exercises.	Organise a limited number of large-scale exercises to increase the level of preparedness and cooperation of targeted stakeholders. Develop, deploy and promote exercises, tools and frameworks that enable stakeholders, in particular in sectors impacted by the NIS 2 Directive, to independently execute their own cybersecurity exercises. Develop a community to 'train the trainers that leverages the tools, platforms and frameworks developed by ENISA.	CERT-EU CSIRTs network (as applicable) EU ISACs (as applicable) EU-CyCLONe members (as applicable) NIS CG (as applicable) NLO network (as necessary) NLO subgroup of cyber Europe planners (as applicable)	Number of people impacted directly and/or indirectly by exercises organised by ENISA.	Annual (report)	> 7 000	> 9 000
			Number of sectoral authorities, including EUIBAs, using ENISAs exercise solutions and frameworks.	Annual	5	7
			Number of Member States participating in the community of 'train the trainers.	Annual	10	27

3.3. Organise targeted training and awareness programmes and support stakeholders to plan and execute their own training/ programmes.	Develop, deploy and promote training and awareness-raising tools, frameworks and content that enable stakeholders, in particular those in sectors impacted by the NIS 2 Directive, to independently execute their own training or awareness-raising programmes. Develop a community to 'train the trainers' that leverages the tools, platforms and frameworks developed by ENISA. Harmonise training activities sponsored by Cybersecurity Support Action.	CSIRTs network (as applicable) EU ISACs (as applicable) EU-CyCLONe members (as applicable) NIS CG (as necessary) NLO network (as necessary) NLO subgroup of Cyber Europe planners (as necessary)	Number of participants in ENISA online training sessions.	Annual (report)	4 000 (depending on the Support Action contribution).	> 4 800
			Number of participants in ENISA's train-the-trainer and train-the-planner events.	Annual (report)	> 250	> 300
			Number of professionals impacted by ENISA's AR in a box.	Annual (report)	10 000	> 26 000
3.4. Organise and support cybersecurity challenges, including the ECSC.	Deliver the ECSC final. Form and train an elite team representing Europe at the ICC. Create challenges and a platform with access to new potential cybersecurity professionals.	ECSC Steering Committee NLO subgroup	Number of countries represented in the Team Europe cohort.	Annual (report)	26	32
			Number of users participating in ECSC and national capture the flags, who potentially are new cybersecurity professionals.	Annual (report)	20 000	35 000

Activity 4

ACTIVITY 4 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
4.1. Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs network and EU-CyCLONe members, the HWPCI and the NIS CG.	Enhanced information sharing and cooperation among the CSIRTs network and EU-CyCLONe members and enhanced interaction with the HWPCI and the NIS CG.	CSIRTs network EU-CyCLONe HWPCI NIS CG	Continuous use and durability of platforms (including prior to and during large-scale cyber incidents).	Annual (report)	> 60 % use of platforms.	CNW 81.3 % EU-CyCLONe 63.4 %
			Number of joint sessions established.	Annual (report)	2 joint sessions per year with operational outcomes.	5 joint sessions.
4.2. Maintain, develop and promote the ENISA cyber partnership programme to enable the exchange of information to support the agency's understanding of threats, vulnerabilities, incidents and cybersecurity events.	Operationalisation of the cyber partnership programme.	CSIRT network EU-CyCLONe EUIBAs HWPCI MB	Number of new and total partners in the ENISA partnership programme.	Annual (report)	6	1 new in 2025 and 9 entities in total.
			Percentage of RFI answered by members of partnership programme.	Annual (report)	65 %	67 %
4.3. Implement ENISA's international strategy and outreach.	EU values recognised by international stakeholders. International cooperation supports ENISA's objectives.	European Commission EEAS MB (as required ENISA Management team	Staff satisfaction with international coordination.	Annual (survey)	3.5	3.9 (survey revised to use a 1–5, where 1 means very dissatisfied and 5 means very satisfied).
4.4. Develop comprehensive coordinated vulnerability disclosure platforms by operationalising the EUVD and designing the CRA Single Reporting Platform.	The EUVD is deployed. The CRA Single Reporting Platform is being developed.	CSIRTs network				

4.5. Develop and maintain IT systems and platforms for operational activities.	Consolidation of operational IT with a view to supporting ENISA operations.	Business owners of ENISA's operational IT systems CSIRTs network EU-CyCLONe HWPCI NIS CG	IT architecture for external operational IT services.	Biennial update	End of 2025.	Completed on time.
			ENISA operational IT.	Annual (report)	All operational IT systems are consolidated under one IT operational manager by 2025.	All IT operational assets are consolidated and streamlined on time.
					One third of current systems are updated every year to reach 100 % in 2027.	One third of current IT assets were updated and systems upgraded based on need.
			EUVD.	Annual (report)	EUVD is produced and users are trained.	EUVD is live and provides services to the EU.
			CRA Single Reporting Platform.	Annual (report)	Technical specifications of the CRA Single Reporting Platform are available and the service provider is contracted to start implementation.	The design and the development of the CRA started. The contactor is delivering milestones according to plan.
4.6. Development of stakeholder and knowledge management systems and frameworks.			Stakeholder satisfaction with knowledge management and stakeholder management system.	Biennial (survey)	> 60 % by 2026.	The results will be attained at the end of 2026 after a full year of implementation.

Activity 5

ACTIVITY 5 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
5.1. Collect, organise and consolidate information (including from the general public) on common cyber situational awareness, technical situational reports, incident reports and threats, and support the consolidation and exchange of information on the strategic, operational and technical levels [43].	Establishment of a threat information management platform. Production of briefings, reports and summaries of incidents, threats and vulnerabilities. Increased understanding and timely access to information regarding the latest threats, incidents and vulnerabilities.	CSIRT network EU entities EU-CyCLONe National authorities within Member States subscribed to the products	Timeliness and accuracy of reports.	Annual (survey)	> 85 %	Overall accuracy score of 3.8 out of 5 and an overall timeliness score of 3.9 out of 5 (based on responses from 49 respondents out of 660 surveyed).
5.2. Provide analysis and risk assessment jointly with other operational partners, including EUIBAs, Member States, industry partners, and non-EU partners.	EU joint assessment and reports, sectoral analysis and threat analysis [44]. Recipients receive accurate and timely assessments of threat actors and associated risks to the EU internal market.	CSIRT network EU entities EU-CyCLONe HWPCI MB	Number of contributing Member States to the JCAR.	Annual (report)	> 40 %	24 Member States contributing (an increase of 13).
5.3. Collect and analyse information to report on cyber threat landscapes.	Mapping threats. Generating recommendations for stakeholders to take up.	Advisory group and Cybersecurity Threat Landscape AHWG CSIRTs network NLOs	Number of downloads of *ENISA Threat Landscape*.	Annual (report)	> 5 % increase year on year	6 195 downloads in a five-week period

[43] Advisory group proposal for standby emergency incident analysis team provisioned within Output 5.1.

[44] Including the JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation and EC3 Cooperation and Directorate-General for Communications Networks, Content and Technology Situation Centre.

5.4. Analyse and report on incidents as required by Article 5(6) of the CSA and other sectoral legislation (e.g. DORA, eIDAS Article 10, etc.).	Analysing incidents. Generating recommendations for stakeholders to take up.	European Competent Authority for Secure Electronic Communications European Competent Authority for Trust Services Expert Group NIS CG workstream 3				
5.5. Develop the CRA Single Reporting Platform and operationalise the EUVD.	CRA Single Reporting Platform work is scoped, and implementation is initiated. Operational and business processes are defined together with primary stakeholders.	CSIRT network	Opera-tioanal processes expected for 2025 are defined. Implemen-tation work in progress.	Survey	80 % of the stakehold-ers agree on the es-tablished process and score them > 4 (Scale 1 to 5).	100 % of respondents gave a satisfaction score of ≥ 4 for the platform so far.

Activity 6

ACTIVITY 6 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
6.1. Provide penetration testing and threat-hunting services for selected entities within Member States (45).	Penetration testing and threat-hunting services are delivered in a timely and accurate manner to Member States.	Beneficiaries Directorate-General for Communications Networks, Content and Technology Member States	Percentage of Member States requesting the service. Satisfaction score.	Annual	50 % > 4	82 % requested services (22 out of 27 Member States). Overall satisfaction score of 4.65.
6.2. Provide customised exercises and training for selected entities within Member States.	Customised exercise and training services are delivered in a timely and accurate manner to Member States.	Beneficiaries Directorate-General for Communications Networks, Content and Technology Member States	Percentage of Member States requesting the service. Satisfaction score.		50 % > 4	100 % requested. Overall satisfaction score of 4.
6.3. Support risk monitoring and assessment for selected entities within Member States.	ENISA provides regular risk monitoring of specific targets or at the national level, including by leveraging commercial off-the-shelf platforms, as well as providing specific risk assessment and threat landscapes as requested by Member States.	Directorate-General for Communications Networks, Content and Technology Member States Other beneficiaries	Percentage of Member States requesting the service. Satisfaction score.		50 % > 4	48 % requested. Overall satisfaction score of 4.3.
6.4. Support incident response and incident management for selected entities within Member States.	ENISA provides 24/7 incident-response support to Member States.	Directorate-General for Communications Networks, Content and Technology Member States Other beneficiaries	Percentage of Member States requesting the service. Support provided in a timely manner. Satisfaction score.		50 % > 4	100 % requested. Overall satisfaction score of 5.0.

(45) The beneficiaries of Activity 5 services are specified in the contribution agreement.

Activity 7

ACTIVITY 7 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
7.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes.	Scheme meets stakeholder requirements, notably those of the Commission and Member States. Take-up of schemes by stakeholders. Timely delivery by ENISA of all schemes requested in cooperation with the Commission. Statutory bodies and AHWGs actively involved.	AHWGs on certification ECCG European Commission	Number of opinions of stakeholders managed.	Annual (report)	100 opinion items per scheme.	370 opinions of stakeholders managed for the EU5G NESAS draft candidate scheme.
			Number of people or organisations engaged in the preparation of certification schemes.	Annual (report)	At least 20 AHWG members from third-party experts; at least 15 Member States joining AHWGs.	25 experts in EUDIW AHWG. 23 Member States in EUDIW AHWG. 30 experts in EUMSS AHWG. 22 Member States in EUMSS AHWG.
7.2. Implementation and maintenance of established schemes, including evaluation of adopted schemes, participation in peer reviews etc., and monitoring the dependencies and vulnerabilities of ICT products and services.	Review schemes to improve efficiency and effectiveness. Take-up of schemes by stakeholders.	ECCG European Commission	ECCG's satisfaction with ENISA's efforts on schemes adopted.	Triennial (survey)	75 %	To be assessed in 2027.
			Satisfaction with ENISA's role in NCCA peer reviews.	Triennial (survey)	75 %	To be assessed in 2027.
7.3. Supporting statutory bodies in carrying out their duties with respect to governance roles and tasks.		ECCG European Commission SCCG	Feedback from statutory bodies, including NCCAs, on ENISA's role.	Annual (survey)	75 %	Rescheduled to 2027

7.4. Developing and maintaining the necessary provisions, tools and services concerning the ECCF (including the certification website and supporting the Commission in relation to the core stakeholders service platform, CEF, for collaboration, publication and promotion of the implementation of the cybersecurity certification framework etc.).	Transparency and trust in supporting ICT products, services and processes. Stakeholder engagement in promotion of certification.	ECCG European Commission SCCG	User satisfaction with the services on the certification website.	Annual (survey)	75 %	Rescheduled to 2027
			Use of the certification website.	Annual (report)	75 %	Rescheduled to 2027

Activity 8

ACTIVITY 8 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
8.1. Collect and analyse information on new and emerging ICT, and provide strategic advice to the ECCC on the EU agenda on cybersecurity research, innovation and deployment.	Identifying current and emerging ICT gaps, trends, opportunities and threats. Advising EU funding programmes, including the ECCC and its strategic agenda and action plan.	Academia Entities, including NCCs and EUIBAs European Commission, including the Directorate-General for Communications Networks, Content and Technology and the Joint Research Centre (JRC) and the ECCC as appropriate Industry Member States' market authorities National R & I	Findings endorsed by Member States (NCCs and market authorities).	Annual	> 60 %	No updates in 2025 on the ECCC strategic agenda and action plan.
			Alignment with the ECCC strategic agenda and action plan.	Annual (survey with ECCC)	> 60 %	No updates in 2025 on the ECCC strategic agenda and action plan.
8.2. Conduct market analysis of the main trends in the cybersecurity market on both the demand and supply sides, and evaluations of certified products, services and processes; prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements.	Improved understanding of the market and industry.	Advisory group AHWGs for cybersecurity market analysis ECCG (as necessary) Member States' market authorities NLO (as necessary) SCCG	Cybersecurity market analysis; cybersecurity products and services.	Annual (report)	All reports produced as planned (Y out of Y reports).	1 ENISA cybersecurity market analysis framework (version 3) completed and validated by NLO and the advisory group.

			Member States' endorsement of the report on emerging trends regarding cybersecurity risks in products with digital elements.	Biennial (report)	27 Member States endorse report.	First report expected in 2028 as per the CRA.
8.3. Support the activities of market surveillance authorities and the identification of categories of products for simultaneous coordinated control actions and, upon request, conduct evaluations of products that present a significant cybersecurity risk.	Produce a catalogue of market surveillance authorities; survey market surveillance authorities' requirements; identify categories of products; produce a methodology on market sweeps; carry out market sweeps. Evaluations to be carried out ideally on the basis of input from market sweeps; rely on external expertise.	European Commission NLO/NCCA SCCG (as appropriate)	Collection of requirements. Matching requirements with deliverables. Time to carry out market sweeps. Methodology for evaluations. Profiles of experts.	Catalogue, survey and categories of products in 2025–2026. Market sweeps as from 2027 (3-year transition) or earlier if requested. Method to evaluate products. Guidance and criteria to accept evaluation results.	Stakeholder satisfaction above 60 %	The CRA enters into force in December 2027, hence criteria cannot be assessed.
8.4 Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification.	Alignment with standards.	Advisory group NLO (as necessary) SCCG	Reports on analysis of standardisation aspects on cybersecurity, including cybersecurity certification.	Annual (report)	All reports produced as planned (Y out of Y reports).	1/1 ENISA cybersecurity standardisation repository report completed. Report to be published in 2026.

Activity 9

ACTIVITY 9 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
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 the SPD. Annual assessments of risk and internal controls performed and reported. Legal and regulatory compliance monitored; issues and areas for improvement identified. Outcomes are included in the annual assessments of risk and internal controls. Streamlined IT system management across the agency and in accordance with ENISA's IT strategy under the ITMC. Streamlined budget management across the agency, under the Budget Management Committee. A plan to reduce CO2 emissions at ENISA's headquarters.	Budget Management Committee External and internal audits IT Management Committee Management team Statutory bodies	Number of high risks identified in annual risk assessment.	Annual	≤ 3	6 high risks (0 critical, 6 medium and 4 low).
			Effective monitoring of high risks and critical recommen-dations to follow up on timely implemen-tation of mitigation measures by business owners.		Quarterly status reporting to the management team. Internal controls assessment, including reporting on implementation for year N-1. Risk assessment.	Completed. Completed. Completed.
			Percentage of identified deficiencies in internal controls addressed within timelines.		100 % for critical, 80 % for major, 60 % for moderate risks.	No critical weakness has been identified in the 2025 ICF assessment. While improve-ments have been noted, out of six recommendations issued in the 2025 ICF assessment , three important and two desirable recommendations remains to be fol-lowed up from the previous year while one important recommendation has been newly introduced on the implementation of specific and/or horizontal internal controls going above and beyond financial transac-tions.

			Timely follow-up and resolution of internal and external audits recommendations and findings (in particular from the IAS and the ECA).		Monitoring audit action plans. Results of corrective actions taken during year N-1 are reported in the current year AAR.	Audit plans were monitored as appropriate. Completed.
			Number of identified regulatory breaches.		≤ 3	No regulatory breach identified in 2025.
			Percentage of revised and up-to-date corporate rules (Managing Board decisions, Executive Director decisions, policies, processes).		Review 50 % of corporate rules that have not been reviewed in the last 4 years and 60 % of corporate rules that have not been reviewed in the last 5 years. Provide or confirm motivation for non-revision, as a baseline requirement.	60 active Management Board decisions from before 2022.
			Annual report on ARES maintenance and actions.		80 % resolution of identified open issues, incorporating lessons learned.	100% resolution of identified issues
			Efficiency and effectiveness of ITMC and Budget Management Committee (survey).		> 60 %	Satisfaction rate of 69% for the BMC

9.2. Maintain and enhance ENISA's cybersecurity position.	Compliance with new regulations on a high common level of cybersecurity within EU entities. Timely identification and response to cybersecurity risks.	External and internal audits Management team and relevant committees Statutory bodies	Percentage of identified high-risk mitigation measures addressed within timelines.	Annual	90 %	100 % (all the previously identified risks are being addressed).
	Continuous monitoring of the cybersecurity of IT systems and timely identification of issues and areas for improvement (first-level and second-level controls).		Annual risk assessment and risk treatment plan with the relevant business owners.		Implement annual risk assessment follow-up actions.	Implemented and in progress; follow-up with the risk owners.
			Implement action plan for implementation of cybersecurity risk management measures in line with Regulation (EU, Euratom) 2023/2841.	Annual	Report on the level of accomplishment of action plan.	Initial risk review was submitted in due time, and 60 % of identified actions are in progress.
			Address all potential cybersecurity incidents.	Annual	Respond to > 90 % of tickets submitted to the ticketing system.	100 %; all potential incidents were addressed in due time and without impact.
			Cybersecurity training for staff and managers.	Annual	At least 2 training sessions a year.	100 % achieved (first session by CERT-EU for managers and the second session for staff by the ISO team).

9.3. Provide support services to EUAN in key areas of the agency's expertise and chair EUAN in 2025.	Cybersecurity advisory on implementation of the new regulation on a high common level of cybersecurity within EU entities and in cooperation with CERT-EU. Shared services in the area of data protection, legal services and accounting.	Agencies receiving ENISA's support Budget Management Committee EUAN Management team	Satisfaction within EUAN with ENISA support services.	Annual	> 80 %	100 % satisfaction from all EU entities that have received services from ENISA.
9.4. Ensure the implementation of single administration processes across the agency.	Streamlined document management practices.	Management team Staff Committee	Percentage of staff considering that the information they need to do their job is easily available or accessible within ENISA.	Annual	55 %	As per the 2025 Staff Satisfaction Survey, 53 % of respondents agree and 17 % strongly agree with this statement; ≥ 70 %.
			Response timeliness to external parties (internal reporting).	Annual	Rate according to rules of procedures	Response rates in accordance with ENISA's procedures

Activity 10

ACTIVITY 10 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
10.1. Review and implement the multiannual communications strategy and support the stakeholders strategy, including corporate outreach.	Enhanced transparency and outreach. Engaged communities. Increased impact of ENISA activities. Relevant and easily accessible information provided to stakeholders. Successful EUAN leadership, communications and EUAN yearly meetings.	Agency stakeholders Management team	Number and types of activities at each engagement level (stakeholder strategy implementation).	Annual (internal report)	Stakeholder strategy under review.	109 events and meetings, involving 63 national entities, 23 private-sector entities, 8 EUIBAs, 6 civil-society organisations, 5 academic institutions and 4 international organisations.
			Number of social media engagements.	Annual (media monitoring)	> 80 000	83 000
			Number of total ENISA website visits.	Annual (website analytics)	> 2.5 million	~ 1.3 million
			Website availability.	Annual (website analytics)		> 97 %
10.2. Implement internal communications strategy.	Engaged staff.	Management team Staff Committee	Staff satisfaction with ENISA's internal communications.	Annual (survey)	> 60 %	64 %

10.3. Manage and provide the secretariat for statutory bodies (i.e. the Executive Board, the MB, the advisory group and the NLOs (excluding certification)).	Support for the operation and organisation of ENISA statutory bodies. Support the effectiveness of the implementation of work programmes (validation of operational outputs). Provide administrative support for the day-to-day workings of the MB's decisions and recommendations from the NLO network and advisory group.	Committees Management team Statutory bodies	Number of feedback instances received per NLO consultation.	Annual (internal report)	> 6	9
			Number of feedback instances received per advisory group consultation.	Annual (internal report)	> 8	10
			Satisfaction of statutory bodies with ENISA's support to fulfil their tasks as described in the CSA.	Annual (survey)	> 80 %	89 % (very) satisfied and 11 % neutral.
			Satisfaction of statutory bodies with ENISA's portals.	Annual (survey)	> 80 %	74 % (very) satisfied, 24 % neutral and 2 % unsatisfied.

Activity 11

ACTIVITY 11 OUTPUTS						
DESCRIPTION	**EXPECTED RESULTS OF OUTPUT**	**VALIDATION**	**OUTPUT INDICATOR**	**FREQUENCY (DATA SOURCE)**	**2025 TARGET**	**2025 RESULTS**
11.1. Manage and provide general recurrent administrative services in the area of resources for ENISA staff and partners.	Services such as payroll, recruitment, learning and development, budget planning and execution are performed efficiently. Implementation of the Executive Director decision on the annual workforce review (adopted in April 2024).	Budget Management Committee ITMC Management team Staff Committee	Turnover rates (statutory staff and seconded national experts (SNEs)	Annual	< 5 %	6.4 %
			Turnover rates (staff under contribution agreements).		N/A	7.4 %
			Establishment plan posts filled.		> 95 %	99 %
			Lag between vacancy announcement to candidate selection (offer out).		< 300 days median across all posts.	Range between 14 days and 200 days.
			Percentage implementation of the approved recruitment plan.		> 90 %	98 %
			Percentage implementation of the approved procurement plan.		> 90 %	96 %
			Percentage procurement procedures launched via e-tool.		> 90 %	100 %
			Percentage budget implementation.		> 95 %	99.96 %
			Average time to initiate a transaction by financial initiating agent.		< 7 days	7 days
			Average time for verifying a transaction by financial verification agent.		< 3 days	0.17
			Number of budget transfers.		< 4	2
			Late payments resulting in interest payments.		< 10 %	0.97 %

11.2. Implement the agency's corporate strategy, including the HR strategy, with an emphasis on talent development, growth and welfare.	Objectives and goals set out in the corporate and HR strategy are met.	Budget Management Committee EUAN Management team MB Staff Committee	Number of policies reviewed.	Annual	> 1	17
			Number of processes revised.		> 1	25
			Percentage of staff satisfaction with talent development.		> 50 %	60 %
			Percentage of actions implemented as follow up on Staff Satisfaction Survey results and implemented on time.		> 95 %	97 %
			Number of implemented competency-driven training and development activities.		> 1	200
			Number of multisource feedback evaluations implemented and followed up.		> 5	43
11.3. Manage and provide general, recurrent support services in the area of facilities, security and corporate IT for ENISA staff and partners.	Services such as corporate IT, facilities and security are performed efficiently with minimal disruption. Upgrade of meeting rooms.	Budget Management Committee ITMC Management team Staff Committee	Staff satisfaction with working environment.	Annual	> 70 %	81 %
			Time to respond to safety and security incidents.		< 1 day to acknowl-edge and < 3 days to respond.	KPI met.
			Average time to respond to facilities management requests.		< 1 day to acknowl-edge and < 3 days to respond.	KPI met.
11.4. Enhance operational excellence and digitalisation through modern, safe, secure and streamlined ways of working, and introduce self-service functionalities.	Services such as access management, meeting room facilities, equipment renewals, cloud-based solutions and data availability are efficient.	ITMC Management team	Critical systems uptime and downtime.	Annual	99 %	99.95 %
			Staff satisfaction with IT resolution.		85 %	93 %

A

ANNEX II

STATISTICS ON FINANCIAL MANAGEMENT

Budget out turn and cancellation of appropriations (EUR)

BUDGET OUT-TURN	2023	2024	2025
Reserve from the previous years' surplus (+)			
Revenue actually received (+)	25 293 935	42 473 035	54 955 252
Payments made (–)	–21 118 392	–25 690 066	–28 674 472
Carryover of appropriations (–)	–4 228 452	–16 945 798	–38 608 030
Cancellation of appropriations carried over (+)	149 739	154 797	110 160
Adjustment for carry-over of assigned revenue appropriation from previous year (+)	53 469	163 909	12 337 348
Exchange rate differences (+/–)			
Adjustment for negative balance from previous year (–)			
Total	**150 299**	**155 877**	**120 258**

Execution of commitment appropriations in 2025

	CHAPTER	COMMITMENT APPROPRIATIONS AUTHORISED (*)	COMMITMENTS MADE	COMMITMENT RATE (%)
A-11	Staff in active employment	13 917 087	13 917 087	100.00
A-12	Recruitment/departure expenditure	216 784	216 784	100.00
A-13	Socio-medical services and training	842 978	842 778	99.98
A-14	Temporary assistance	517 953	517 953	100.00
TITLE I		15 494 802	15 494 602	100.00
A-20	Buildings and associated costs	1 097 800	1 081 300	98.50
A-22	Current administrative expenditure	703 208	703 208	100.00
A-23	ICT	2 599 803	2 578 219	99.17
TITLE II		4 400 811	4 362 727	99.13
B-30	Activities related to outreach and meetings	1 203 592	1 198 272	99.56
B-36	Core operational activities	5 681 179	5 672 247	99.84
B-37	CSA core operational activities	39 422	39 247	99.56
TITLE III		6 924 193	6 909 766	99.79
B-40	Activities related to externally funded projects	40 472 795	14 123 736	34.90
TITLE IV		40 472 795	14 123 736	34.90
Total		**67 292 601**	**40 890 831**	**60.77**

(*) Commitment appropriations authorised include the budget voted by the budgetary authority, budget amendments, transfers by the Executive Director and miscellaneous commitment appropriations for the period (fund sources C1, C4, R0).

Execution of payment appropriations in 2025 (EUR)

N EUR	CHAPTER	PAYMENT APPROPRIATIONS AUTHORISED (*)	PAYMENT MADE	% PAYMENT RATE
A-11	Staff in active employment	13 917 087	13 917 087	100.00
A-12	Recruitment/departure expenditure	216 784	213 784	98.62
A-13	Socio-medical services and training	842 978	478 550	56.77
A-14	Temporary assistance	517 953	237 782	45.91
TITLE I		15 494 803	14 847 204	95.82
A-20	Buildings and associated costs	1 097 800	743 846	67.76
A-22	Current administrative expenditure	703 208	367 811	52.30
A-23	ICT	2 599 803	1 841 073	70.82
TITLE II		4 400 810	2 952 729	67.10
B-30	Activities related to outreach and meetings	1 203 592	918 710	76.33
B-36	Core operational activities	5 681 179	3 911 736	68.85
B-37	CSA core operational activities	39 422	39 247	99.56
TITLE III		6 924 192	4 869 693	70.33
B-40	Activities related to externally funded projects	40 472 795	6 004 846	14.84
TITLE IV		40 472 795	6 004 846	14.84
Total		**67 292 600**	**28 674 472**	**42.61**

Carry forward to 2025 (open amounts as of 31 December 2025) (EUR)

IN EUR	CHAPTER	COMMITMENTS MADE (*)	PAYMENTS MADE (**)	AMOUNT TO BE PAID IN 2023	% AMOUNT TO BE PAID
A-11	Staff in active employment	13 917 087	13 917 087	—	0.0
A-12	Recruitment/departure expenditure	216 784	213 784	3 000	1.4
A-13	Socio-medical services and training	842 778	478 550	364 228	43.2
A-14	Temporary assistance	517 953	237 782	280 171	54.1
TITLE I		15 494 603	14 847 204	647 399	4.2

(*) Payment appropriations authorised include the budget voted by the budgetary authority, budget amendments, transfers by the Executive Director and miscellaneous commitment appropriations for the period (fund sources C1, C4, R0).

A-20	Buildings and associated costs	1 081 300	743 846	337 454	31.2
A-22	Current administrative expenditure	703 208	367 811	335 397	47.7
A-23	Information and communication technologies	2 578 219	1 841 073	737 146	28.6
TITLE II		4 362 727	2 952 729	1 409 997	32.3
B-30	Activities related to outreach and meetings	1 198 272	918 710	279 562	23.3
B-36	Core operational activities	5 672 247	3 911 736	1 760 511	31.0
B-37	CSA Core operational activities	39 247	39 247	—	0.0
TITLE III		6 909 766	4 869 693	2 040 073	29.5
B-40	Core operational activities – assistance funds	14 123 736	6 004 846	8 118 890	57.5
TITLE IV		14 123 736	6 004 846	8 118 890	57.5
Total		**40 890 832**	**28 674 472**	**12 216 360**	**29.9**

Revenue and income during 2025 (EUR)

TYPE OF REVENUE	ENTITLEMENTS ESTABLISHED	REVENUE RECEIVED	OUTSTANDING AT THE END OF THE YEAR
Subsidy from the EU budget	26 714 332	26 714 332	0
Other contributions	28 066 718	28 066 718	0
Revenue from administrative operations	174 805	174 202	603
Total	**54 955 855**	**54 955 252**	**603**

(*) All fund sources C1, C4, R0 are included in the figures.

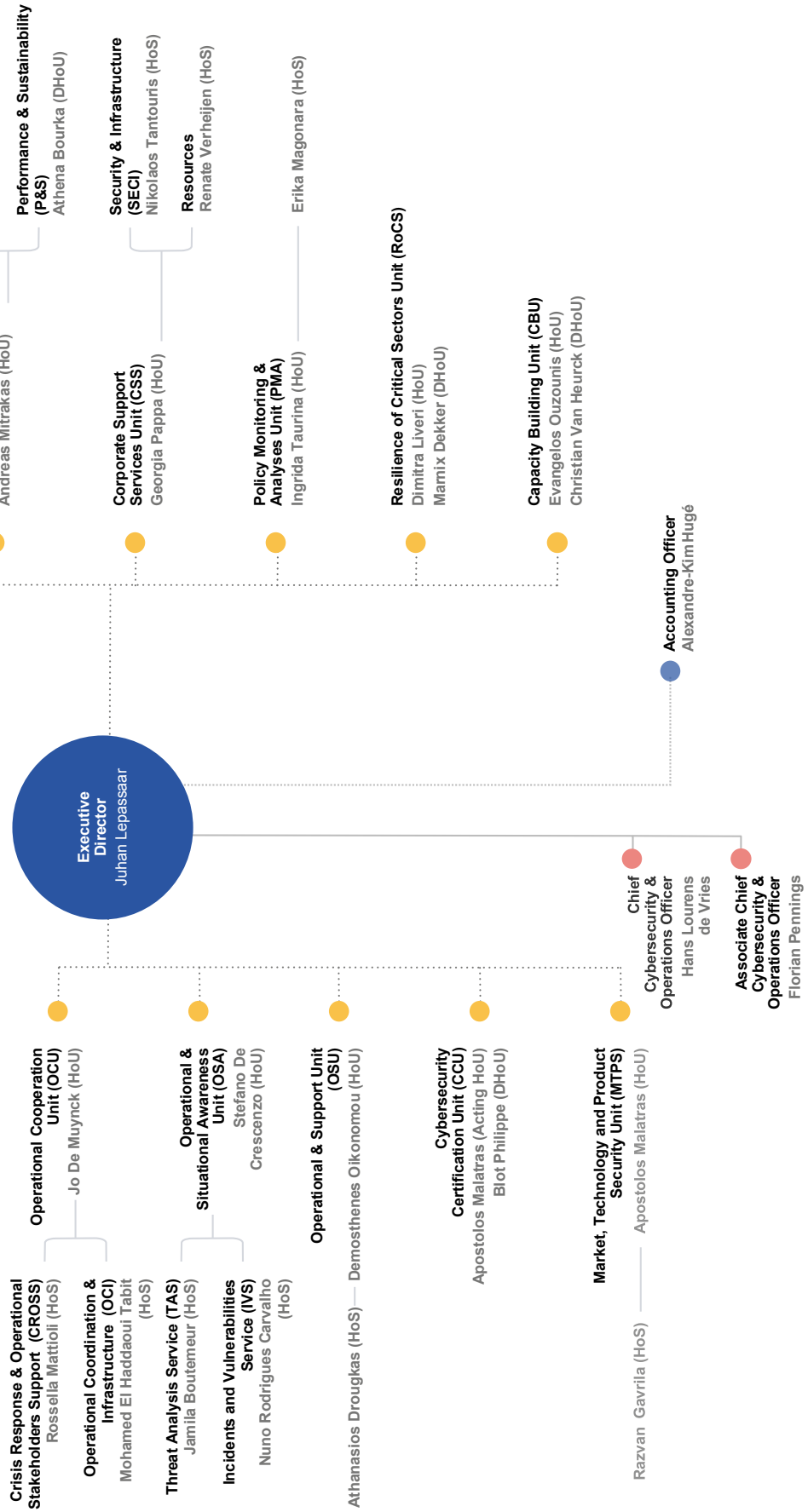
(*) All fund sources are included in the figures.

Total revenue may differ from commitment appropriations authorised, as total revenue is based on actual income whereas commitment appropriations may use estimates for other, minor administrative revenue.

A

ANNEX III

ORGANISATIONAL CHART


Executive Director
Juhan Lepassaar
Executive Director's Office
Andreas Mitrakas (HoU)
Reputation & Trust (R&T)
Laura Heuvinck (HoS)
Performance & Sustainability (P&S)
Athena Bourka (DHoU)
Corporate Support Services Unit (CSS)
Georgia Pappa (HoU)
Security & Infrastructure (SECI)
Nikolaos Tantouris (HoS)
Resources
Renate Verheijen (HoS)
Policy Monitoring & Analyses Unit (PMA)
Ingrida Taurina (HoU)
Erika Magonara (HoS)
Resilience of Critical Sectors Unit (RoCS)
Dimitra Liveri (HoU)
Marnix Dekker (DHoU)
Capacity Building Unit (CBU)
Evangelos Ouzounis (HoU)
Christian Van Heurck (DHoU)
Accounting Officer
Alexandre-Kim Hugé
Operational Cooperation Unit (OCU)
Jo De Muynck (HoU)
Crisis Response & Operational Stakeholders Support (CROSS)
Rossella Mattioli (HoS)
Operational Coordination & Infrastructure (OCI)
Mohamed El Haddaoui Tabit (HoS)
Operational & Situational Awareness Unit (OSA)
Stefano De Crescenzo (HoU)
Threat Analysis Service (TAS)
Jamila Boutemeur (HoS)
Incidents and Vulnerabilities Service (IVS)
Nuno Rodrigues Carvalho (HoS)
Operational & Support Unit (OSU)
Athanasios Drougkas (HoS)
Demosthenes Oikonomou (HoU)
Cybersecurity Certification Unit (CCU)
Apostolos Malatras (Acting HoU)
Biot Philippe (DHoU)
Market, Technology and Product Security Unit (MTPS)
Razvan Gavrila (HoS)
Apostolos Malatras (HoU)
Chief Cybersecurity & Operations Officer
Hans Lourens de Vries
Associate Chief Cybersecurity & Operations Officer
Florian Pennings

A

ANNEX IV

2025 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT

2025 Establishment Plan

FUNCTION GROUP AND GRADE	ESTABLISHMENT PLAN IN 2025 VOTED EU BUDGET [11]		POSITIONS FILLED AS OF 31 DECEMBER 2025	
	OFFICIALS	TEMPORARY AGENTS	OFFICIALS	TEMPORARY AGENTS
AD 16				
AD 15		1		1
AD 14				
AD 13		2		1
AD 12		4		4
AD 11		3		3
AD 10		4		4
AD 9		14		13
AD 8		16		12
AD 7		13		12
AD 6		7		14
AD 5				
Total number of ADs		**64**		**64**
AST 11				
AST 10				
AST 9		1		2
AST 8		3		1
AST 7		3		0
AST 6		6		7
AST 5		4		4
AST 4		2		2
AST 3				1
AST 2				1
AST 1				
Total number of ASTs		**19**		**18**

11

AST/SC 6				
AST/SC 5				
AST/SC 4				
AST/SC 3				
AST/SC 2				
AST/SC 1				
Total number of AST/SCs				
Total		**83**		**82**

AD, administrator; AST, assistant; AST/SC, assistant/secretary.

Information on entry level for each type of post

NO	JOB TITLE	TYPE OF CONTRACT (OFFICIAL, TA, CA OR SNE)	FUNCTION GROUP / GRADE OF RECRUITMENT	FUNCTION (ADMINISTRATIVE SUPPORT OR OPERATIONS)
	Executive Director	TA	AD 14	Top operations
	Adviser	TA	AD 12	Administrative
	Head of Unit	TA	AD 9	Administrative/operations
	Head of Sector	TA	AD 6	Administrative/operations
	Team leader	TA	AD 7	Operations
	Senior cybersecurity expert	TA	AD 9	Operations
	Cybersecurity expert	TA	AD 6	Operations
	Cybersecurity officer	CA	FG III/IV	Operations
	Officer	CA	FG IV	Administrative
	Assistant	CA	FG III	Administrative/operations
	Assistant	CA	FG I	Administrative/operations
	Coordinator	TA	AST 6	Administrative
	Cybersecurity officer	TA	AST 6	Operations
	Officer	TA	AST 3	Administrative/operations
	Assistant	TA	AST 2	Administrative
	Lead certification expert	TA	AD 12	Operations

	Legal adviser on cybersecurity	TA	AD 6	Operation
	Spokesperson	TA	AD 6	Administrative
	Legal adviser	TA	AD 7	Administrative
	Data Protection Officer	TA	AD 7	Administrative
	Information security officer	TA	AD 7	Administrative
	Administrator	TA	AD 8	Administrative
	Accounting	TA	AD 8	Administrative
	SNE	SNE	N/A	Operations

AD, administrator; AST, assistant; FG, function group.

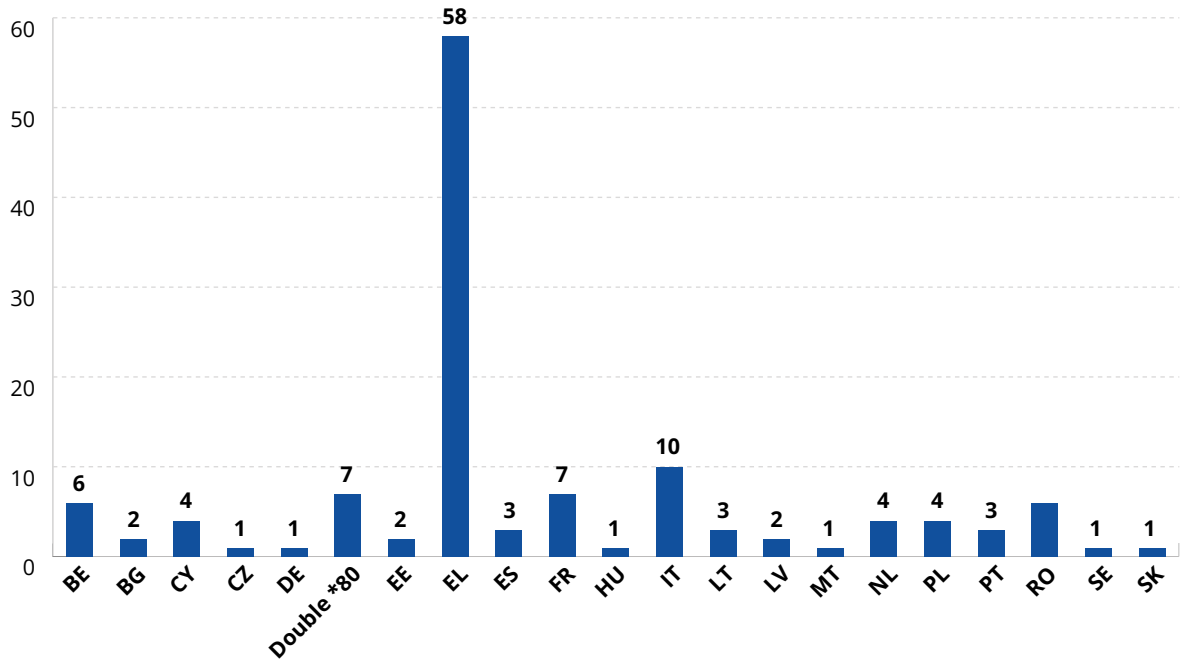
Information on benchmarking exercise (%)

JOB TYPE	2023	2024	2025
TOTAL ADMINISTRATIVE SUPPORT AND COORDINATION	25.76	23.69	24.51
Administrative support	19.05	17.69	18.00
Coordination	6.72	6.00	6.51
TOTAL OPERATIONAL	66.55	70.25	68.91
Total operational coordination	11.27	9.69	11.54
Programme management and implementation	53.64	56.06	56.80
General operational activities	1.64	4.50	0.57
TOTAL NEUTRAL	7.69	6.06	6.58
Finance and control	7.31	5.75	6.29
Linguistic activities	0.37	0.31	0.29

Human resources statistics

On 31 December 2025, the agency had a total of 127 statutory staff members (temporary agents and contract agents) in-house.

Nationalities of statutory staff as of 31 December 2025

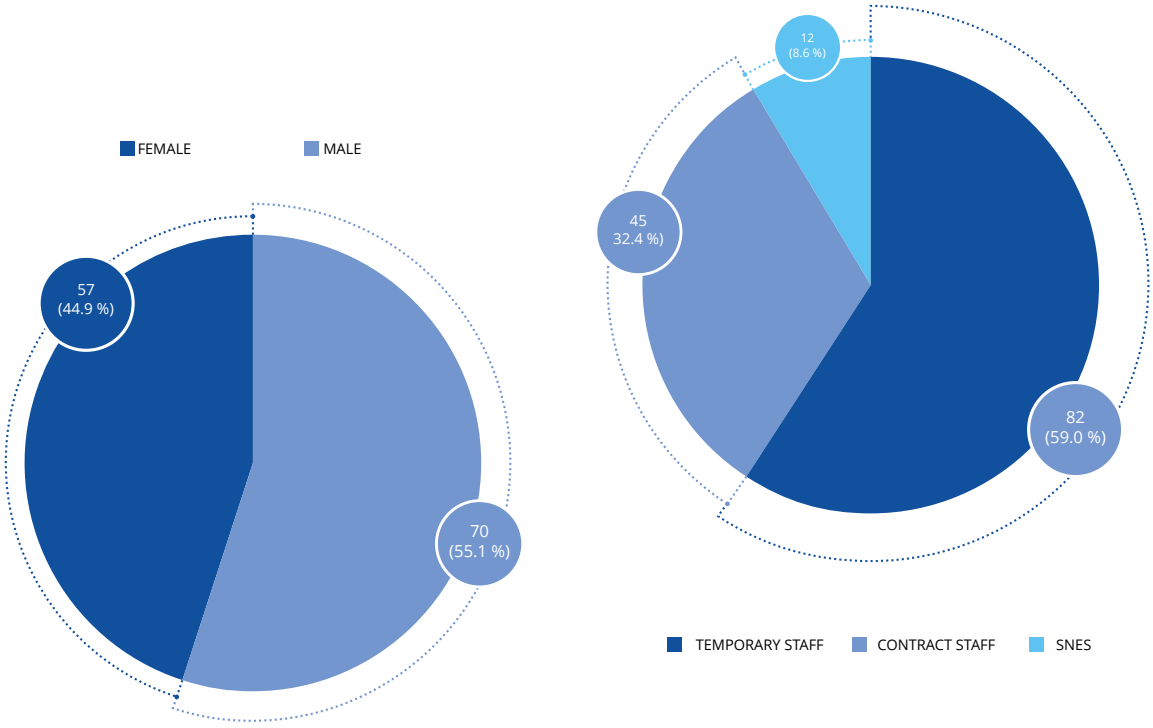


*double refers to dual nationality

Most represented nationality

MOST REPRESENTED NATIONALITY	2024		2025	
	Number	%	Number	%
Greek	52 out of 121	43.0	58 out of 127	45.6

Gender distribution of statutory staff as of 31 December 2025



Staff distribution by contract type as of 31 December 2025

MANAGEMENT	2024		2025	
	NUMBER [48]	%	NUMBER [49]	%
Female managers	2	29	3	30
Male managers	5	71	7	70

IMPLEMENTING RULES

Decision No MB/2025/12	On laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings

[48] The managers are the Executive Director (1), Heads of Unit (6) and team leaders (3).

[49] Statistics include the Executive Director (1) and Heads of Unit (6). Team leaders are not included.

Appraisal and reclassification/promotions

Implementing rules in place

		YES	NO	IF NO, WHICH OTHER IMPLEMENTING RULES ARE IN PLACE
Reclassification of temporary agents	Model decision C(2015)9560	x		
Reclassification of contract agents	Model decision C(2015)9561	x		

Reclassification of temporary agents

GRADES	2021 (REFERENCE YEAR 2020)	2022 (REFERENCE YEAR 2021)	2023 (REFERENCE YEAR 2022)	2024 (REFERENCE YEAR 2023)	2025 (REFERENCE YEAR 2024)	ACTUAL AVERAGE OVER 5 YEARS	AVERAGE OVER 5 YEARS (ACCORDING TO DECISION C(2015)9563)
AD 5	—	—	—	—	—	—	2.8
AD 6	1	1	1	2	2	4.02	2.8
AD 7	—	2	1	3	2	4.26	2.8
AD 8	1	3	1	2	1	3.71	3
AD 9	—	—	2	—	2	3.13	4
AD 10	—	2	—	—	1	7.83	4
AD 11	—	—	—	—	—	—	4
AD 12	1	—	—	—	—	10	6.7
AD 13	—	—	—	—	—	—	6.7
AST 1	—	—	—	—	—	—	3
AST 2	—	—	—	—	—	—	3
AST 3	—	1	—	—	—	8.5	3
AST 4	—	—	1	1	—	5.65	3
AST 5	1	—	1	—	1	3.47	4
AST 6	1	—	—	—	1	4	4
AST 7	1	1	1	—	—	3.97	4
AST 8	—	—	—	2	—	3.5	4
AST 9	—	—	—	—	—	—	N/A
AST 10 (senior assistant)	—	—	—	—	—	—	5

AD, administrator; AST, assistant; N/A, not applicable.

Reclassification of contract agents

CONTRACT AGENTS	GRADE	STAFF IN ACTIVITY AT 31.12.2025	STAFF MEMBERS RECLASSIFIED IN 2025 (REFERENCE YEAR 2024)	AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS	AVERAGE NUMBER OF YEARS IN GRADE OF RECLASSIFIED STAFF MEMBERS ACCORDING TO DECISION C(2015)9561
FG IV	18	1	—	—	
	17	—	1	7.8	Between 6 and 10 years
	16	15	—	—	Between 5 and 7 years
	15	4	1	2.6	Between 4 and 6 years
	14	13	2	3.5	Between 3 and 5 years
	13	5	—	—	Between 3 and 5 years
FG III	12	3	—	—	
	11	1	—	—	Between 6 and 10 years
	10	2	—	—	Between 5 and 7 years
	9	—	—	—	Between 4 and 6 years
	8	0	—	—	Between 3 and 5 years
FG II	6	0	—	—	Between 6 and 10 years
	5	—	—	—	Between 5 and 7 years
	4	—	—	—	Between 3 and 5 years
FG I	3	1	—	—	N/A
	2	—	—	—	Between 6 and 10 years
	1	—	—	—	Between 3 and 5 years

Schooling

AGREEMENT IN PLACE WITH THE EUROPEAN SCHOOL OF HERAKLION	
Contribution agreements signed with the Commission on type I European schools	No
Contribution agreements signed with the Commission on type II European schools	Yes

A

ANNEX V

HUMAN AND FINANCIAL RESOURCES BY ACTIVITY

Human resources by activity

The allocation of financial and human resources for 2025 for the operational and corporate activities described in Part I of this consolidated AAR is presented in the table below. The allocation was determined according to the direct budget and number of FTEs reported for each activity, with the indirect budget being assigned to all activities based on drivers such as direct FTEs.

The following assumptions were used in the simplified activity-based costing methodology.

- The budget granted to ENISA through the contribution agreements signed in 2023–2025 is not included in the calculations, as the activities (as well as the budget) defined in those agreements cover multi-year periods.
- The FTEs granted to ENISA through the contribution agreements signed in 2023–2025 are not included in the calculations, as their direct and indirect costs should be fully covered by those contribution agreements.
- The budget allocation for each activity includes the direct and indirect costs attributed to each activity.
- The direct budget is the actual cost under each of the eight operational activities described in Part I, which covers services, goods, missions and large-scale events.
- The indirect budget is the actual cost for salaries and allowances, buildings, IT, equipment and miscellaneous operating costs attributable to each activity. The indirect budget was allocated to activities based on drivers. The main driver for cost allocation was the number of direct FTEs spent for each operational and administrative activity in 2025.
- In order to estimate the full costs of operational activities, all corporate activities (Activities 9, 10 and 11) should be distributed accordingly to all the operational activities based on defined drivers.

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES	ACTIVITIES AS REFERRED TO IN PART I	BUDGET ALLOCATION (EUR)	FTE ALLOCATION
Support for policy monitoring and development	Activity 1	1 328 804.07	5.25
Cybersecurity and the resilience of critical sectors	Activity 2	2 199 534.79	9.56
Capacity building	Activity 3	2 866 110.94	10.95
Enabling operational cooperation	Activity 4	3 867 184.26	11.72
Provide effective operational cooperation through situational awareness	Activity 5	3 676 632.95	11.61
Provide services for operational assistance and support	Activity 6	659 569.79	3.60
Supporting the development and maintenance of the EU cybersecurity certification framework	Activity 7	2 095 873.88	8.06
Supporting the European cybersecurity market, research and development, and industry	Activity 8	2 144 577.34	8.51
Performance and sustainability	Activity 9	2 287 122.45	9.52
Reputation and trust	Activity 10	1 307 268.64	6.12
Effective and efficient corporate services	Activity 11	4 271 904.93	15.36
Total		**26 704 584.04**	**100.26**

A

ANNEX VI

GRANTS, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS

ENISA does not receive any form of grant.

Income-generating SLAs

SLA PARTNER(S) AND PURPOSE	DATE OF SIGNATURE	TOTAL AMOUNT FORECAST (EUR)	DURATION	COUNTERPART	SHORT DESCRIPTION	COMMENTS
ECCC (Activity 9)	20.12.2022	54 604	Automatic renewal on an annual basis.	ECCC	Covers support services offered by ENISA to the ECCC, namely a data protection officer and an accounting officer.	
eu-LISA (Activity 3)	8.5.2024	120 000	31.12.2025 (with option to renew).	eu-LISA	Covers support services offered by ENISA to eu-LISA on the planning, execution and evaluation of upcoming annual security and business continuity exercises.	Valid until 31.12.2025; a new SLA is pending, currently awaiting Executive Director-level signature.
DORA inter-agency agreement between ENISA, ESMA, the European Banking Authority and the European Insurance and Occupational Pensions Authority	4.7.2024	89 963		ESMA European Banking Authority European Insurance and Occupational Pensions Authority	This agreement lays down the terms and conditions under which ENISA shall develop, deliver, deploy in a pre-production environment and make available to the ESAs the DORA IR tool, against payment from the ESAs to ENISA.	Either party may terminate the present agreement by giving the other party at least 30 calendar days' prior written notice.

Non-income-generating SLAs with other EU entities that were active in 2025

SLA PARTNER(S) AND PURPOSE	DATE OF SIGNATURE	END DATE	DURATION	TOTAL AMOUNT FORECAST IN 2025 (EUR)	COUNTERPART	SHORT DESCRIPTION
European Centre for the Development of Vocational Training (Cedefop) for legal services	30.10.2023	14.7.2025		N/A	Cedefop	This SLA sets out the general terms and conditions (the 'terms') under which the providing agency shall provide its services in the field of legal expertise to the receiving agency as described in the annex ('the legal services').
Cedefop for possible cooperation and synergies	30.10.2023		Automatic renewal on an annual basis.	N/A	Cedefop	The 2 agencies aim to continue fruitful cooperation; realise efficiency gains; support the effort to shift resources from administration to their core business; and share knowledge, expertise and best practices.
CERT-EU for structured cooperation	15.2.2021		Automatic renewal on an annual basis.	N/A	CERT-EU	Structured cooperation is established on the basis of Article 7.4 of the CSA to allow ENISA and CERT-EU to benefit from synergies and to avoid the duplication of activities provided for in their respective mandates, with respect to operational cooperation within the CSIRTs network.
CISA regarding working arrangements	6.12.2023		Cooperation may continue until participants conclude that the objectives have been achieved.	N/A	CISA	Cooperation to benefit from synergies as derived from their respective mandates.
ECCC regarding increasing cooperation	8.6.2023	8.6.2025	The agreement was signed for an initial period of 2 years and may be renewed by mutual agreement between ENISA and the ECCC.	N/A	ECCC	The parties cooperate with each other and ensure synergies across relevant parts of their respective mandates.

The European Defence Agency (EDA) for establishing structured cooperation	16.3.2017		No specific duration is stated in the agreement.	N/A	EDA	Structured cooperation between ENISA and EDA.
EDA, EC3 and CERT-EU for cooperation supported by all the parties' respective mandates	23.5.2018		The present agreement will stay in force between the remaining parties until such a time as they submit their own written notice of termination.	N/A	EDA European Union Agency for Law Enforcement Cooperation (Europol) (EC3) CERT-EU	Cooperation framework between all parties by identifying the areas of cooperation based on common interest.
European Railway Agency for increasing cooperation	23.10.2023	23.10.2025		N/A	European Railway Agency	The parties cooperate with each other and ensure synergies across relevant parts of their respective mandates.
EUIPO for disaster recovery services	1.1.2022		The agreement shall remain valid for an indefinite period.	46 171.46	EUIPO	Disaster recovery services.
eu-LISA regarding working arrangements	10.1.2018		No specific duration is stated in the agreement.	N/A	eu-LISA	Cooperation framework between the parties by identifying the areas of cooperation based on common interest.
Europol for cooperative relations to support Member States	26.6.2014		No specific duration is stated in the agreement.	N/A	Europol	Structured cooperation between ENISA and Europol in order to support the Member States in preventing and combating cybercrime and other forms of related crime with a view to ensuring a high and effective level of NIS.
Europol for the EC3 Working Group on security and safety online	16.3.2017		No specific duration is stated in the agreement.	N/A	Europol (EC3)	Establishment of a forum, where experts have an opportunity to discuss, assess and contribute to solutions to counter the criminal abuse of encryption and anonymity, while respecting and protecting security and safety online.

EASA for a permanent secretariat	20.5.2016		The agreement is signed for an indefinite period.	N/A	EASA	EUAN has agreed to set up a secretariat to facilitate the coordination of the network by providing administrative, operational and secretariat support.
European Food Safety Authority for shared office support under the EUAN shared support office	1.3.2018		The agreement is signed for an indefinite period.	8 277.21	EFSA	The SSO is the office designated to assist the network chair in facilitating coordination among network members and with the EU institutions.
EDPS on increasing cooperation	30.11.2022	30.11.2027	This agreement is signed for an initial period of 5 years and may be renewed by mutual agreement between ENISA and the EDPS.	N/A	EDPS	Establishment of strategic cooperation in areas of common interest.
JRC regarding the EU Academy	2.8.2023		The agreement is signed for an indefinite period.	17 106.00	JRC	The agreement sets out the modalities of cooperation and defines the conditions under which the JRC provides services related to the delivery, operation and use of the EU Academy platform.
The Ukrainian national cybersecurity coordination centre regarding working arrangements	9.11.2023		Cooperation may continue until the participants conclude that the objectives have been achieved or until 1 participant discontinues its participation in this working arrangement.	N/A	Ukraine's national cybersecurity coordination centre	Cooperation activities.

REA regarding the provision of validation services	19.11.2024			101 001.34	This agreement defines the conditions under which REA ('the service provider') provides services ('services') to ENISA ('the client').	Valid for a period of 1 year and will be renewed automatically unless specified otherwise.

GENERAL INFORMATION						FINANCIAL AND HR IMPACTS				
CONTRIBUTION AGREEMENTS	DATE OF SIGNATURE	TOTAL AMOUNT EURO	DURATION	COUNTERPART	SHORT DESCRIPTION		N–1		N	
						Amount	CA	PA	CA	PA
Support Action fund	21.12.2023	20 000 000.00	31.12.2026	Directorate-General for Communications Networks, Content and Technology	To implement the 'preparedness and incident response support for key sectors' action under the DEP. This contribution agreement covers Support Action ex ante / ex post and SitCen (2024–2026).		5 204 461.11	3 843 160.01	8 021 903.51	3 527 790.33
						Number of CAs	12		12	
						Number of SNEs	N/A		N/A	
CRA Single Reporting Platform	9.12.2024	400 000 00.00	31.7.2026	Directorate-General for Communications Networks, Content and Technology	To conduct a feasibility study on a single reporting platform under the CRA that will inform the future steps of the platform development.	Amount	N/A	N/A	239 409.38	132 935.93
						Number of CAs	N/A		N/A	
						Number of SNEs	N/A		N/A	
Support for incident and vulnerability response and reporting and implementation of the CRA (LC-03708221 with amendments)	19.12.2024	23 350 000.00	18.12.2028	Directorate-General for Communications Networks, Content and Technology	To implement the 'incident and vulnerability response support and reporting' action under the DEP. The action will be developed through the 'ENISA cybersecurity support action programme', composed of 3 activities.	Amount	N/A	N/A	5 543 164.76	2 137 669.69
						Number of CA	N/A		3	
						Number of SNEs	N/A		N/A	

EU Cybersecurity Reserve and Cyber Situation and Analysis Centre	31.7.2025	36 670 000.00	30.7.2028	Directorate-General for Communications Networks, Content and Technology	To financially contribute to the implementation of the EU Cybersecurity Reserve and the Cyber Situation and Analysis Centre.	Amount	N/A	N/A	130 150.00	114 400.00
						Number of CA	N/A		N/A	
						Number of SNEs	N/A		N/A	
European cybersecurity support centre for hospitals and healthcare providers	16.12.2025	6 000 000.00	28.2.2029	Directorate-General for Communications Networks, Content and Technology	To finance the implementation of the action 'European cybersecurity support centre for hospitals and healthcare providers'.	Amount	N/A	N/A	N/A	N/A
						Number of CA	N/A		N/A	
						Number of SNEs	N/A		N/A	
						AMOUNT	**5 204 461.11**	**3 843 160.01**	**1393462765**	**5912795.95**
TOTAL CONTRIBUTION AGREEMENTS						**NUMBER OF CAS**	**12**		**15**	
						NUMBER OF SNES	**N/A**		**N/A**	

A

ANNEX VII

ENVIRONMENTAL MANAGEMENT

ENISA is progressively integrating environmental considerations into its operations alongside its core focus on cybersecurity. This includes adopting practices such as the use of certified cloud hosting and promoting environmentally responsible solutions.

The agency places strong emphasis on environmental awareness and training for staff, while encouraging active participation in its environmental management system.

Responsibility for achieving environmental objectives extends to staff, suppliers, partners and visitors, with policy principles communicated to all relevant stakeholders.

The agency's main objectives include compliance with national and EU environmental legislation, full implementation and continuous improvement of the environmental management system, monitoring environmental performance, reducing environmental impacts and ensuring efficient use of resources and energy. The agency also promotes waste reduction, lower emissions, circular economy practices, biodiversity support and increased agency awareness and engagement.

To achieve these goals, ENISA implements structured actions such as aligning with EMAS standards, allocating necessary resources, adopting environmentally friendly technologies and conducting continuous training and communication.

In its supply chain and infrastructure planning, including the planned phase-out of office building in Heraklion, ENISA prioritises environmentally sustainable services, contingent on the availability of suitable options in its operational locations.

A

ANNEX VIII

ANNUAL ACCOUNTS

Statement of financial position

IN EUR	31.12.2025	31.12.2024
I. Non-current assets	989 813	977 984
Intangible fixed assets	0	0
Tangible fixed assets	989 813	977 984
II. Current assets	41 356 571	17 647 925
Short-term receivables	41.356.571	17.647.925
Cash and cash equivalents	0	0
TOTAL ASSETS (I. + II.)	**42 346 384**	**18 625 909**
III. Non-current liabilities	14 945 468	6 078 420
Long-term Commission pre-financing received	14 945 468	6 078 420
IV. Current liabilities	22 605 865	7 341 690
Short-term Commission pre-financing received	19 482 166	6 234 297
Accounts payable	476 788	66 136
Accrued liabilities	2 646 911	1 041 257
TOTAL LIABILITIES (III. + IV.)	**37 551 333**	**13 420 110**
V. Net assets	4 795 051	5 205 799
Accumulated result	5 205 799	1 791 102
Surplus/(deficit) for the year	−410 748	3 414 697
TOTAL LIABILITIES AND NET ASSETS (III. + IV. + V.)	**42 346 384**	**18 625 909**

Statement of financial performance

IN EUR	2025	2024
Revenue from the Union Subsidy	26 594 074	29 063 924
Revenue from administrative operations	6 126 970	4 067 815
Total operating revenue	32 721 044	33 131 739
Administrative expenses	−23 503 769	−19 453 036
Staff expenses	−16 650 128	−14 354 476
Fixed asset related expenses	−314 071	−675 054
Other administrative expenses	−6 539 570	−4 423 506
Operational expenses	−9 628 023	−10 264 006
Total operating expenses	−33 131 792	−29 717 042
Surplus/(deficit) from operating activities	−410 748	3 414 697
Financial revenue	0	0
Financial expenses	0	0
Exchange rate loss	0	0
Surplus/(deficit) from non-operating activities	0	0
Surplus/(deficit) from ordinary activities	−410 748	3 414 697
Surplus/(deficit) for the year	−410 748	3 414 697

A

ANNEX IX

LIST OF ACRONYMS, INITIALISMS AND ABBREVIATIONS

AEV	Adversarial Exposure Validation
CCTF	Cyber Coordination Task Force
CDT	Cyber Diplomacy Toolbox
CIRAS	Cybersecurity Incident Reporting and Analysis System
CIRAS 2	Cybersecurity Incident Reporting and Analysis System v2
CSAT	Customer Satisfaction Score
HCs	
IL-HAM	Israel Hamas
IPCR	Integrated Political Crisis Response
ISAA	Integrated Situational Awareness and Analysis
IVS	Incidents and Vulnerabilities Services
JRRs	Joint Rapid Report
MITRE	The MITRE Corporation
OpenCTI SaaS	OpenCTI Software as a Service
ORAS	Openssam Retrieval and Analysis System
SitCen	Cyber Situational Awareness and Analysis Center
Stratcom	Strategic Communications
TAS	Threat Analysis Services
UA-RU	Ukraine - Russia
URSA	Union Regular Situational Awareness
AAR	Annual Activity Report
AD	Administrator
AHWG	Ad hoc Working Group
AST	Assistant
AST/SC	Assistant/Secretary
CA	Contract Agent
Cedefop	European Centre for the Development of Vocational Training
CEF	Connecting Europe Facility
CERT-EU	Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CG	Cooperation Group
CISA	Cybersecurity and Infrastructure Security Agency
CNA	CVE Numbering Authority
CNW	CSIRTs Network
COO	Chief Cybersecurity and Operations Officer
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
CSOA	Cyber Solidarity Act
CSS	Corporate Support Services
CVE	Common Vulnerabilities and Exposures

DEP	digital Europe programme
DORA	Digital Operational Resilience Act
EC3	European Cybercrime Centre
ECA	European Court of Auditors
ECCC	European Cybersecurity Competence Centre
ECCF	European cybersecurity certification framework
ECCG	European Cybersecurity Certification Group
ECSC	European Cybersecurity Challenge
ECSF	European cybersecurity skills framework
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EFSA	European food Safety Authority
eIDAS	Electronic Identification and Trust Services Regulation
EIT	European Institute of Innovation and Technology
EMAS	eco-management and audit scheme
ENISA	European Union Agency for Cybersecurity
ESMA	European Securities and Markets Authority
EU	European Union
EU-CSI	EU cybersecurity index
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
EUAN	EU Agencies Network
EUCC	EU cybersecurity certification scheme on common criteria
EUDI	European digital identity
EUDIR	EU Digital Infrastructure Registry
EUDIW	EU Digital Identity Wallet
EUIBAs	European Union institutions, bodies and agencies
EUMSS	European Union cybersecurity certification for managed security services
Europol	European Union Agency for Law Enforcement Cooperation
EUVD	European Union Vulnerability Database
FTE	full-time equivalent
HWPCI	Horizontal Working Party on Cyber Issues
IAS	Internal Audit Service
ICC	International Cybersecurity Challenge
ICT	information and communications technology
ISAC	information-sharing and analysis centre
IT	information technology
ITMC	IT Management Committee

JCAR	Joint Cyber Assessment Report
JRC	Joint Research Centre
KPI	Key Performance Indicator
MB	Management Board
NCAF	National Capabilities Assessment Framework
NCCs	network of National Coordination Centres
NCCA	National Cybersecurity Certification Authority
NESAS	Network Equipment Security Assurance Scheme
NIS	Network and Information Security
NLO	National Liaison Officer
Q & A	Question and Answer
R & I	Research and Innovation
REA	European Research Executive Agency
REU	REGULATION (EU, Euratom) 2023/2841 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
SBOMs	Security Bill of Materials
SCCG	Stakeholder Cybersecurity Certification Group
SLA	Service-level Agreement
SME	Small and Medium-sized Enterprises
SNE	Seconded National Expert
SOCs	Security Operations Centers
SOPEx	Standard Operating Procedures Exercise
SPD	Single Programming Document
TA	Temporary Agent
ITIL	Information Technology Infrastructure Library

TP-01-26-013-EN-N

ABOUT ENISA

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