EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2024 Consolidated Annual Activity Report

JUNE 2025

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONTACT

To contact the European Union Agency for Cybersecurity (ENISA) or for general enquiries, use info@enisa.europa.eu or www.enisa.europa.eu.

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2025

COPYRIGHT NOTICE

PDF Web **ISBN** 978-92-9204-715-3 **ISSN** 2314-9434 **DOI** 10.2824/2824042 **TP**-01-25-020-EN-N

2024 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 2025

I2024 marked a significant milestone for the Agency on its 20-year anniversary. Since 2004, ENISA has been dedicated to pursuing and to a great extent, achieving a high common level of cybersecurity across the European Union. I would like to thank the ENISA Management Board, all ENISA stakeholders and particularly its staff, past and present, for their important contributions to 20 years of making Europe more cybersecure.

In 2024, the Agency marked several significant achievements over the year, with the following milestones standing out:

- **First State of the Union Cybersecurity Report:** This report provides an evidence-based overview of the state of play of cybersecurity and an assessment of cybersecurity capabilities across Europe. Since its establishment, ENISA has been steadfast in its commitment to providing expertise and strategic support to EU Member States. This report has been made possible by means of input sourced from the ENISA Cybersecurity Index, that provides a baseline for the State of the Union Cybersecurity Report, the NIS Investment Report and both the ENISA Threat Landscape 2024 and the updated Foresight 2030 Threats Report, all of which provide long term strategic guidance on cybersecurity challenges. The State of the Union Cybersecurity Report provides policy recommendations to address shortcomings identified and bolster cybersecurity, cooperation and resilience.

- **CVE Numbering Authority:** ENISA has been authorised as a Common Vulnerabilities and Exposures (CVE) Numbering Authority, which has enhanced the support that ENISA renders to EU CSIRTs in terms of Coordinated Vulnerability Disclosure. Under this light, the EU has been equipped with an essential tool designed to substantially improve the management of vulnerabilities and the risks associated with it. ENISA progressed with the implementation of the vulnerability database requirement from the NIS 2 Directive. The database will provide aggregated, reliable, and actionable information on cybersecurity vulnerabilities affecting ICT products and services. The database ensures transparency to all users and will stand as an efficient source of information to find mitigation measures.

- **NIS2 Directive Support:** ENISA continued to work closely with EU Member States to support them with implementing the NIS2 Directive. ENISA provided expertise and guidance to

build up cybersecurity resilience and deploy comprehensive, purpose-made, awareness material.

- **Certification:** In early 2024, the Implementing Regulation on the EU cybersecurity certification scheme on Common Criteria (EUCC), was published on the Official Journal marking a significant achievement. Furthermore, a new Commission request for a cybersecurity certification scheme on the certification of the EU Digital Identity Wallets has been received and met with the acceptance of the Agency and the establishing of a dedicated Ad Hoc Working Group, to complement ongoing work on EUCS and EU5G.

- **Cyber Europe Exercise:** The 7th edition has been one of the largest cybersecurity exercises in Europe ever and it focused on the resilience of the EU energy sector. This exercise is evidence of the commitment of ENISA to advancing preparedness and response capacities to protect critical infrastructure, a building block of the digital single market. This pan-European exercise brought together 30 national cybersecurity agencies, several EU agencies, bodies and networks and over 1000 experts supporting a broad range of areas including incident response, decision-making etc. In addition, the exercises performed by ENISA currently map to the roles identified in the European Cybersecurity Skills Framework (ECSF), thus allowing actors across sectors and Members States to foster a resilient and skilled workforce capable of addressing evolving threats.

- **ENISA Cybersecurity Support Action:** By implementing and delivering ex-ante and ex-port services via the Agency's Cybersecurity Support Action, ENISA contributed to further developing cyber preparedness and response capabilities at the EU and MS level. All 27 Member States participated in the programme, which consolidated a total of 482 requests for services.

- **Situational Awareness:** The Agency established a Threat Information Management system, thus contributing to the cooperative response by further strengthening its situational awareness capabilities. It also consolidated and leveraged the ENISA Cyber Partnership Programme, which onboarded 10 companies to embed the private sector contribution primarily within the EU Joint Cyber Assessment Report (EU-JCAR). The number of contributing MS also increased and the CSIRTs Network and EU-CyCLONe contributed to the cooperative response through effective situational awareness. ENISA provided 8 briefings to HWPCI which contributed to increased situational awareness at Council level.

In 2024, the revised strategic objectives adopted by the ENISA Management Board and restructuring of ENISA's operational services will likely empower the Agency to remain agile and ahead of cybersecurity challenges. In early 2025, a comprehensive survey of operational activities highlighted the strong added value of ENISA's deliverables in the past two years, with 88% of stakeholders reporting significant benefits from our outputs. Significantly 89% of stakeholders confirmed that ENISA's work does not duplicate, or it only partially duplicates, albeit at very small proportions, Member States efforts—underscoring the Agency's alignment with the needs of Member States. Finally, 96% of respondents had trust in ENISA's ability to achieve its mandate. The survey results will shape our future processes, ensuring that we continue meeting stakeholder needs and delivering high-value results in a timely fashion.

I would like to thank all contributors to the survey for their invaluable feedback provided. I am immensely grateful to the broader cybersecurity community, including experts, advisors, partners, and staff, alike, for all their contributions throughout 2024. Together, we continue keeping Europe cyber secure.

Juhan Lepassaar
Executive Director

ENISA MANAGEMENT BOARD ASSESSMENT

The Management Board (MB) extends its congratulations for the significant milestone of ENISA's 20th anniversary in 2024. For the past two decades, ENISA has been a steadfast supporter of the EU and its Member States (MS) in their pursuit of a high common level of cybersecurity across Europe. In recent years, new legislation has expanded the scope of actions, further reinforcing and strengthening the EU's cybersecurity posture. ENISA has built up momentum by scaling up its operations to support the implementation of not only the Cybersecurity Act (CSA) but also other key legislation, including the NIS2 Directive and the Cyber Resilience Act (CRA). Finally, the MB extends its gratitude to ENISA for its valuable support in the revision of ENISA's strategy that was adopted in 2024 and admires the growth of importance of ENISA over the years.

Please find below the MB assessment of the 2024 annual activity report (AAR).

1. In 2024 ENISA made significant strides in supporting the development of cybersecurity policies and regulations, particularly through the release of the first State of the Cybersecurity in the Union report, as all other reports produced by ENISA contribute to and feed into this report. The MB congratulates ENISA on the high level of satisfaction of all 27 MS that actively participated in the Cybersecurity Index, that forms a baseline for the report and encourages the agency to follow up on the policy recommendations identified to increase the level of cybersecurity in the EU.

2. The MB takes note of the publication of ENISA's annual NIS Investments report, providing a pre-NIS2 implementation snapshot of the sectorial maturity for new NIS 2 sectors, which is expected to serve as a baseline to assess the impact of the Directive in the following years. The MB recognizes the importance of the NIS Investment Report and the success of the both the ENISA Threat Landscape 2024 and the updated foresight 2030 threats report, both of which provide long term strategic guidance on cybersecurity challenges and opportunities.

3. The MB acknowledges the successful execution of the 'Cyber Europe' exercise in 2024 and its importance in helping to improve and develop the capabilities of MS and EU institutions, bodies and agencies (EUIBAs) to respond to cyber threats and incidents and increase preparedness across the EU. The MB calls on the agency to focus on impactful exercises, taking on board learning outcomes, and to develop its exercises and training platforms to support stakeholders with organising their own exercises and trainings ('exercises as a service'), with the support of ENISA via the ENISA exercises platform 'Blueroom'.

4. The MB congratulates the agency on the success of the European cybersecurity skills framework (ECSF) in 2024 and its further adoption by a total of 14 MS, including its recognition by the European skills, competences, qualifications and occupations (ESCO) framework. The MB calls on ENISA to further enhance the concept of attestation of skills using the ECSF profiles together with the European Cybersecurity Competence Centre (ECCC).

5. With regards to policy implementation, the MB appreciates the support provided to MS for the implementation of the NIS2 Directive (NIS2 security measures and adoption of coordinated vulnerability disclosure (CVD) guidelines) and calls on the agency to continue its focus of supporting the MS with best practices and by providing a greater overview of solutions. In addition, the MB acknowledges the significance of the ENISA NIS360 2024 report in identifying areas for improvement and process tracking across NIS2 Directive sectors, thus supporting critical sectors in overcoming challenges. The MB calls on ENISA to give recommendations that are as horizontal as possible across sectors, in order to streamline approaches to challenges and work towards convergence and simplification.

6. The MB appreciates the support provided to MS for the implementation of the NIS2 Directive, especially the technical advice to support the European Commission with adopting the implementing rules for the NIS2 security measures. The MB congratulates ENISA on the development of EU-wide NIS2 security measures, its valuable contribution to all the NIS Cooperation Group (NIS CG) workstreams and its role and input to the Commission's EU health action plan, adopted in early 2025.

7. The MB acknowledges the support provided to operational communities (computer security incident response team (CSIRTs) network and EU-CyCLONe, the EU's cyber crisis liaison organisation network) and congratulates the agency on receiving recognition for its contribution to the overall ecosystem by the December 2024 Council conclusions. The MB calls on the agency to take additional measures to raise the maturity and trust of operational communities going forward.

8. The MB recognises the finalisation of the first phase of the European Union Vulnerability Database (EUVD) and ENISA's new role as a Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA), and calls on the agency to ensure a high level of coordination of vulnerability disclosure services within the EU.

9. The MB acknowledges the increased cooperation with external operational entities, such as MS through the CSIRTs network, EU-CyCLONe and EU entities such as the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU) and the European Union Agency for Law Enforcement Cooperation's (Europol) European Cybercrime Centre (EC3) in contributing to cooperative response via the 'EU Joint Cyber Assessment Report' (EU-JCAR). In addition, the MB takes note of the developments of ENISA's cyber partnership programme (CPP). The MB calls on the agency to step up its effort with MS to build a common situational awareness, also in preparation for the new cyber blueprint to be finalised during the Polish Presidency of the Council.

10. The MB appreciates ENISA's contribution to further developing preparedness and response capabilities at the EU and MS levels via the ENISA support action and recognises the results of the ongoing programme in 2024, with all 27 MS participating. The MB looks forward to the final results of the ENISA support action by the end of 2026 and to the successful rollover and continuation of support via the Cyber Reserve as from 2026.

11. The adoption of the first implementing act on the EU cybersecurity certification scheme on Common Criteria (EUCC) is a significant landmark in the certification field that paves the way for certified products in the EU. The MB recognises ENISA's support of managed security services (MSS) with a view to engage the MS and selected service providers across the EU, and acknowledges the significance of the Commission request to ENISA to provide support for the certification of European Digital Identity (EUDI) Wallets. The MB calls on the agency to prioritise the development of the EUDI Wallets and to perform all adjustments deemed necessary to make this a priority in the work programme.

12. The MB recognises the support provided by ENISA in 2024 concerning the CRA. This includes the processing of specific requests from the Commission on product catalogues. Such processing broadens the scope of the support of the agency to the Commission and MS, along with cybersecurity market analysis. The MB would like to emphasise the importance of the

CRA and therefore requests the agency to build the necessary internal capabilities to engage in the relevant activities.

13. The MB calls on the agency to strengthen its role and to focus on addressing emerging technologies such as quantum technology, encryption and AI.

14. The MB values the agency's continued support to the EU's external actions and outreach. This is notably the case with Ukraine, the United Kingdom, the United States and Indo-Pacific countries, and the establishment of actions with neighbouring regions such as the Western Balkans. The MB looks forward to the review and update of ENISA's international strategy in 2025, taking on board lessons learned from the past three years.

15. The MB recognises the importance of strong and sustained cooperation between MS and ENISA across all areas of the work programme. To enhance effectiveness and impact, the MB encourages both ENISA and MS to invest additional time and resources into strengthening the National Liaison Officers (NLO) network. In addition, the MB calls on MS to increase the number of seconded national experts (SNEs) to ENISA, as they play a vital role in building links, sharing expertise and promoting mutual understanding, all of which are essential for long-term success.

16. The MB thanks the ENISA stakeholders for responding to the 2nd stakeholder satisfaction survey, with over 186 respondents (15% increase from 2023 survey) and over 250 comments. The results of the second stakeholder satisfaction survey shed much important light on how stakeholders perceive the added value of ENISA's work.

17. On aggregate the results demonstrate high added value of ENISA's deliverables with 88 % of stakeholders finding significant added value in the outcome / results of ENISA's work and 82% of stakeholders rating the likelihood of taking up the results of ENISA work in support of their tasks in the immediate to medium term. Although the results are slightly lower than 2021-2022 results, they remain at significantly high levels, supported by the results of the ENISA support action and knowledge on emerging cybersecurity challenges and opportunities. The MB recognizes that the Agency has already taken measures to improve both stakeholders take up and added value with the implementation of structural adjustments in 2025.

18. The mandate of the agency requires that the agency carry out its tasks while avoiding the duplication of Member State activities, therefore the result that 89% of stakeholders (6% increase from 2023 survey) find that ENISA deliverables do not duplicate or only somewhat duplicate Member State activities is tantamount to ENISA's effort to involve stakeholders in all stages of its work and ensure that the outcomes / results are fit for purpose. The MB notes that duplication in some areas is unavoidable due to the nature of the work and the need for MS to have their own capacities, however congratulates the Agency on this result.

19. The MB commends the agency on the successful execution of its internal restructuring. By aligning the internal structure of the agency with its operational activities, the restructuring further strengthens ENISA's commitment to implementing its strategy and enables the agency to effectively navigate the increasing complexity of the cybersecurity policy landscape. In addition, the MB congratulates the agency on the reinforcement of its senior management and on ensuring business continuity with the appointment of Hans de Vries, Chief Cybersecurity and Operations Officer.

20. The MB acknowledges the positive strides made by the agency to meet the obligations of the regulation on a high common level of cybersecurity at EUIBAs. The MB calls on the agency to further strengthen its internal cybersecurity posture by increasing its information technology (IT) cybersecurity investments according to the minimum set by its corporate strategy.

21. The MB reiterates its call to the agency to streamline functions and tasks within its two corporate units (the Executive Director's Office and the Corporate Support Services Unit) where possible, to better address the agency's evolving needs. This could be achieved by outsourcing administrative and technical support functions and by allocating staff posts to functions which would ensure business continuity and that objectives are met as outlined in the corporate strategy.

22. During 2024, ENISA committed a total amount of EUR 26 218 721, representing 100 % of the total budget for the year. Payments made during the year amounted to EUR 21 775 888, representing 83.05 % of the total budget. Overall payment execution very slightly decreased to 83.05 %, compared with 83.86 % in 2023. The target of 95 % for commitment rate set by the Commission (DG Budget) was reached. The agency cancelled a total of EUR 154 797, which represents 3.81 % of the total amount carried forward. Compared with 2023, there is a minor increase in payment execution for implementation of the C8 funds: 96.19 % in 2024 compared with 96.14 % in 2023. The MB calls on the agency to take measures to lower the amount of cancelled budget from the C8 budget carried forward.

23. The MB welcomes the 26 new staff members who joined the agency in 2024, along with the reserve lists of cybersecurity experts established by the agency to be used in the coming years to cover new needs. Staff turnover decreased slightly compared with 2023, from 4.9 % to 4.49 % in 2024, and the ratio remains low (below 5 %), showing the satisfactory ability of the agency to retain staff members.

24. The 2024 AAR also provides extensive information on the 2024 assessment of the internal control framework. Whereas improvements and further fine-tunings are needed in certain areas in order to increase their effectiveness, the assessment confirmed that the internal controls at ENISA provide sufficient and reasonable assurance that policies, processes, tasks and behaviours of the agency, 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 risk and weakness were identified in 2024. Moreover, 15 non-compliant events (i.e. exceptions) were identified in 2024 via internal checks. None of the 15 identified exceptions were assessed as high risk (13 were assessed as low risk and two as medium risk) and only four exceptions were deemed to be of material relevance (set at EUR 10 000). Based on the above, the MB concludes that necessary actions were undertaken within 2024 to ensure the overall efficiency of the internal controls at the agency in order to comply with ENISA's legal and regulatory framework, and further congratulates ENISA for all the efforts engaged to that end.

25. The annexes complete the AAR with a declaration of assurance of the Executive Director, 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 the successful achievements of ENISA in 2024.

26. The MB reiterates that the insufficient resources of the agency are detrimental to the agency's ability to achieve a high common level of cybersecurity across the EU and to fulfil all its tasks as prescribed by EU law. In this context, the MB repeats its call to the Commission (2023 letter to the commissioner from incoming and outgoing MB chairs and vice-chairs) to ensure adequate resources for the agency to be able to undertake any new tasks and take this onboard during the CSA.2 proposal.

27. The MB expresses its deep appreciation to the staff of ENISA and to the Executive Director for their commitment and the 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 Commission, the European Court of Auditors (ECA) and the Permanent Representations of the Member States.

EXECUTIVE SUMMARY

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

ENISA aims to establish a high level of cybersecurity across the EU in collaboration with the broader community. As a center of expertise, it provides independent, high-quality technical guidance and support to MS and EU bodies, and plays a key role in shaping and implementing the EU's cybersecurity policies.

In line with the Cybersecurity Act, the agency remained committed to strengthening Europe's cybersecurity through a transparent and resilient approach. It continuously adapted its operations to evolving challenges, ensuring it effectively fulfilled its mandate by supporting the EU through the following activities.

ENISA supported the development of cybersecurity policies and regulations via its annual NIS Investments report, providing a pre-NIS2 implementation snapshot of the sectorial maturity for new NIS2 sectors, which can serve as a baseline to assess the impact of the directive in the coming years. Findings from the report have also supported the Commission's initiatives in relation to the EU action plan for the cybersecurity of hospitals and healthcare providers and preparatory work for the CRA and the Cyber Solidarity Act (CSOA). The agency provided strategic long-term analysis, guidance and advice on the cybersecurity threat landscape, emerging technologies and cybersecurity challenges via the first *2024 report on the state of cybersecurity in the Union,* delivered to the Parliament in December 2024. The report provides an evidence-based overview of the cybersecurity maturity state of play and an assessment of cybersecurity capabilities across Europe. The report also includes policy recommendations to address identified shortcomings and increase the level of cybersecurity in the EU. Finally, ENISA's evidence-based policy support work is becoming increasingly referenced in EU policy initiatives, such as the European action plan on the cybersecurity of hospitals and healthcare providers.

In terms of policy implementation, ENISA delivered technical advice to support the Commission with adopting the implementing rules for the NIS2 security measures, in close collaboration with the NIS CG. Additionally, ENISA developed a full technical guideline for the EU-wide NIS2 security measures. ENISA's support for policy implementation was highlighted by the Council. In the 2024 conclusions on ENISA, the Council highlighted ENISA's valuable contribution to all the NIS CG workstreams. In addition, ENISA sustained a community of experts on election security. The Nevers risk assessment process was further underlined by the Commission recommendations on subsea cables, and on ENISA's work for the health sector, promoting the EU Health-ISAC (information sharing and analysis centre). Sustaining an EU community of national health authorities, the EU Health-ISAC directly led to ENISA gaining a principal role in the Commission's EU health action plan, which was adopted in early 2025. Supporting the rapid implementation of NIS2 by the MS remains one of the agency's highest priorities,

when many MS are still transposing the legislation in 2025. ENISA will continue to push for consolidation of the many NIS CG workstreams, and to improve coordination, implement an MS NIS implementation issue tracker.

The agency executed its biennial Cyber Europe flagship exercise in 2024, helping to improve and develop the capabilities of MS and EUIBAs, as well as various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the EU. The agency successfully mapped its capacity-building services to the ECSF, which was developed to address Europe's growing need for a unified approach to defining roles and skills in the cybersecurity field. The ECSF was endorsed or adopted as is by 14 MS and more than 500 European companies use it for recruitment purposes. Aligning exercises with competency-based training approaches leads to more targeted and effective skill development and cybersecurity maturity. Finally, the agency trained more than 2 000 cybersecurity professionals in critical sectors and national cybersecurity authorities, thus contributing to directly upskilling the workforce and addressing the growing demand for skilled professionals.

In terms of enabling operational cooperation among MS, EUIBAs and across operational activities, the agency supported the coordination of operational stakeholders during key cybersecurity events. This was the case for high-profile vulnerabilities, when ENISA enabled everyday information-sharing during incidents, specific targeted campaigns and situations of EU interest, such as elections and the Paris Olympic Games. The role of the agency and its contribution to the overall ecosystem were acknowledged by the Council in its December 2024 conclusions, stressing 'that ENISA fulfils an important role as secretariat of the two EU-level Member States driven cyber cooperation networks, the CSIRTs network and EU-CyCLONe'.

Finally, ENISA successfully finalised the first phase of the EUVD. The role of ENISA further strengthened when it became a CNA, thus ensuring a high level of coordination of the vulnerability disclosure services within the EU.

The agency established a Threat Information Management system, thus contributing to the cooperative response by further strengthening its situational awareness capabilities. In doing so, ENISA improved its processes and procedures and increased its cooperation with external operational entities, primarily in MS through the CSIRTs network, and EU entities such as CERT-EU and Europol EC3.

It also consolidated and leveraged the ENISA CPP to embed the private sector contribution primarily within the EU-JCAR. ENISA exited the pilot phase of the EU-JCAR quarterly report in 2024. Produced jointly with CERT-EU, Europol EC3, ENISA formalised the report after engaging in the preparation lifecycle. The number of contributing MS also increased and the CSIRTs Network and EU-CyCLONe were heavily involved in the process, thus contributing to the cooperative response through effective situational awareness.

By implementing and delivering ex ante and ex post services via the agency's cybersecurity support action, ENISA contributed to further developing preparedness and response capabilities at the EU and MS levels to large-scale cross-border incidents or crises related to cybersecurity.

The agency fully met the forecast figures for 2024 in terms of execution of the programme, with the successful participation of all 27 MS. By consolidating a total of 482 requests for services, 157 of which were completely finalised during the reporting year, ENISA contributed to increasing preparedness and the ability to respond to cyber threats across the EU.

In the key area of certification, ENISA celebrated the adoption of the first implementing act on the EUCC and its subsequent amendment on cybersecurity certification by the MS, on a Commission proposal. In addition, the adoption of the amendment to the CSA, concerning MSS, was supported by a feasibility study. The study focused on cybersecurity certification for MS and was carried out swiftly, with a view to engage the MS and selected service providers across the EU. Finally, the Commission requested ENISA to provide support for the certification of European Digital Identity (EUDI) Wallets, including the development of a candidate European cybersecurity certification scheme. Thus in 2024, ENISA launched the ad hoc working group (AHWG) on the EUDI Wallet to support the certification schemes across the MS, along with the EU certification scheme on the EUDI Wallets.

ENISA made positive steps in 2024 concerning the CRA by processing specific requests of the Commission regarding products catalogues broaden the scope of the support of the agency to the Commission and the MS which is also the case of cybersecurity market analyses. ENISA supported its market outputs with a report on the market for MSS, under the CSA amendment, thus further underpinning certification and providing rich contextual information to better understand cybersecurity market dynamics.

The agency strengthened cooperation with a number of stakeholders during the course of 2024, such as with the signing of an MoU with the European Supervisory Authorities (EBA, EIOPA, and ESMA) and with the European Cybersecurity Competence Centre in the area of research and innovation, building on ENISA's status as a trusted ECCC partner.

The agency made positive strides to meet the obligations of Regulation (EU, Euratom) 2023/2841 on a high common level of cybersecurity at EUIBAs, including by conducting risk assessments and a horizontal cybersecurity audit that will form the basis for the agency's long-term cybersecurity strategy and planning.

In 2024, the agency implemented measures to optimise its operational activities and support structure, focusing on enhancing efficiency and fostering synergies. To ensure the effective execution of its expanding tasks and functions (CRA, CSOA), the MB decided to align the agency's operational structure more closely with its work programme. This included the creation of eight dedicated units, each responsible for one of the work programme's eight operational activities.

Finally, the agency supported the MB with the revision of the ENISA strategy, adopted by the MB in November 2024. The updated strategy refines the seven existing objectives and provides indicators to measure their success.

I

PART I

ACHIEVEMENTS OF THE YEAR

The following sections of the AAR are based on the structure of the **ENISA Programming Document 2024–2026.** The achievements of each activity are described, including details of the outcome of each output undertaken during the course of 2024.

ACTIVITY 1:

Providing assistance on policy development

Under Activity 1, ENISA provides evidence-based technical advice to EU policymakers to support the development of cybersecurity policies and regulations. The agency also collects evidence on the effectiveness of existing policy frameworks and identifies synergies and gaps between existing initiatives under implementation. In doing so, the activity contributes to the fulfilment of the strategic objective of cybersecurity as an integral part of EU policies. Under this activity, the following was achieved in 2024.

- **Policy recommendations for the 'Article 18' report.** Activity 1 contributed to the work of Activity 8 on the development of the first-ever report on the state of cybersecurity in the EU, as foreseen in Article 18 of NIS2 (Article 18 report), by correlating the evidence collected and developing policy recommendations for EU policymakers. The policy recommendations were validated following extensive consultations with the Commission and the NIS CG. In total, six policy recommendations were developed, intended to address identified shortcomings and to strengthen the state of cybersecurity in the EU.

- **The NIS Investments 2024 report.** The agency produced its annual NIS investments report, and in doing so analysed data from 1 350 operators, from all sectors of high criticality defined in NIS2 and the manufacturing sector. In covering both existing NIS1 sectors and new NIS2 sectors, the report provides a pre-NIS2 implementation snapshot of the sectorial maturity for new NIS2 sectors, which can serve as a baseline to assess the impact of the directive in the coming years. Findings from the report have also supported the Commission's initiatives in relation to the EU action plan for the cybersecurity of hospitals and healthcare providers and preparatory work for the CRA and CSOA, the Article 18 report, the EU Cybersecurity Index (EU-CSI) and the 'NIS360' network and information security (NIS) project.

- **Contributions to the policy work of the G7 Cybersecurity Working Group (WG).** In 2024, ENISA was invited to contribute to policy developments under the G7 Cybersecurity WG via the EU delegation. This made it possible for ENISA to extend its role in the EU policy and regulatory framework. Specifically, ENISA had an active supporting role in two work streams established under the WG, namely on the topics of AI and cybersecurity and security of critical infrastructures. ENISA contributed to the respective policy work via consultations and technical opinions.

The impact of ENISA's work in supporting policy development has been acknowledged by stakeholders in several ways. ENISA remained engaged in supporting the preparatory work for

key EU policy files such as the CRA and CSOA, and was also invited to contribute to the policy work of the G7 Cybersecurity WG. At the same time, ENISA's evidence-based policy support work is becoming increasingly referenced in EU policy initiatives, such as the European action plan on the cybersecurity of hospitals and healthcare providers. The Article 18 report, which notably called for the drafting of policy recommendations to address shortcomings, is another key example of the agency's positioning as a trusted advisor for policymakers in matters of cybersecurity.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 1 moving forward:

- Activity 1 could benefit from stronger synergies with the work conducted for national cybersecurity strategies and, by extension, the EU-CSI in the future;
- an increased focus of Activity 1 on monitoring policy implementation over the coming years could allow the agency to maximise its impact via targeted policy advice, as the focus across the EU shifts from policy development to policy implementation;
- the Article 18 report could serve as a strategic aggregator of knowledge, connecting the dots of ENISA's expert knowledge and setting a strategic roadmap for the EU and ENISA.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO2. Cybersecurity as an integral part of EU policies	• Uptake of policy recommendations adopted within the biennial report on the state of cybersecurity in the EU [1] • Effectiveness of EU relevant policy initiatives taking cybersecurity into consideration

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

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
Improve the effectiveness and consistency of EU cybersecurity policies	Article 5 of the CSA	2026	Assessment of ENISA advice and its influence on EU policy (stakeholder-centric survey)	75 % stakeholder satisfaction from ENISA's advice and influence (among EU policymakers)

OUTPUTS	OUTCOME
1.1 Advise the Commission and MS on reviewing the effectiveness of current cybersecurity policy frameworks	• ENISA published the 5th NIS investments report, which provided policymakers with insights into the cybersecurity budgets of entities in scope of NIS2. The report showed how these budgets were influenced by the NIS directive and were expected to further develop in light of the implementation of NIS2, in order to inform future policy decisions. Data from the report were also used to support policy discussions, such as the development of the EU action plan for the cybersecurity of hospitals and healthcare providers, as well as several ENISA activities, such as the *2024 report on the state of cybersecurity in the Union,* the EU-CSI and the NIS360 sectorial assessments. • Following up on the preparatory work conducted in 2023, the agency developed a business intelligence dashboard to enable NIS investments data to be easily reused across ENISA's activities.
1.2 Assist and advise the Commission and MS on new policy developments, and carry out preparatory work	ENISA followed a holistic approach, with internal coordination of contributions from all relevant agency activities. Expertise across the agency was used as needed, and technical advice was coordinated and consolidated to provide comprehensive input in the policy development process. • ENISA supported the Commission via contributions to preparatory work in relation to the CRA. This included extensive consultations on priorities for guidance, based on analysis of NIS investments data concerning manufacturers in the scope of the CRA, analysis of datasets to provide expert opinion on skills gaps among manufacturers for compliance and collection, and analysis of data concerning the awareness of CRA among manufacturers and other NIS2 entities developing relevant products to provide advice to DG Communications Networks, Content and Technology (Connect). • ENISA supported the Commission via contributions to preparatory work in relation to the CSOA. This included advice to Connect on MSSP maturity assessment using NIS investments data, and technical advice on implementation aspects of the Cyber Reserve. • In the area of the digital euro, the agency had technical consultations with Connect, DG Financial Stability, Financial Services and Capital Markets Union and the European Central Bank, providing opinions on cybersecurity requirements, standards, certification and related areas, including EUDI Wallets. • In the area of AI, ENISA provided technical advice to the Commission on the AI Act via meetings and technical workshops. The agency also contributed to the EU–US cyber dialogue workstream on AI concerning multilayer framework for cybersecurity in AI systems and security measures for adversarial AI.

OUTPUTS	OUTCOME
1.2 Assist and advise the Commission and MS on new policy developments, and carry out preparatory work	• ENISA contributed to the work of the G7 Cybersecurity WG, which was created following a proposal of the Italian Presidency of the Council. Two work streams were established, namely AI and cybersecurity and security of critical infrastructures. ENISA was invited to join both streams and actively contribute to their respective work. Specifically for the work stream on security of critical infrastructures, ENISA has provided feedback/technical opinions, through the EU delegation represented by the Commission, to the 10-principle paper 'Supply chain principles – energy sector', proposed by the United States. On the workstream on AI and cybersecurity, ENISA provided technical feedback to the rest of the G7 members via coordination with the Commission on two papers. • In the area of health, ENISA provided a sectorial policy mapping to Work Stream 12 of the NIS CG, which also covers aspects of the European Health Data Space, and held a relevant workshop with Work Stream 12 and the Commission.
1.3 Monitor and analyse new and emerging policy areas	• Activity 1 contributed to the work of Activity 8 on the first-ever report on the state of cybersecurity in the Union (Article 18 report), foreseen under Article 18 of NIS2. Activity 1 developed six policy recommendations to address the shortcomings identified in the report and validated them with the Commission and the NIS CG. • A new policy landscape report will offer a comparative analysis of the cybersecurity provisions within key adopted policy files. Its objective is to identify synergies and gaps in cybersecurity legislation. Additionally, through policy foresight, the report highlights emerging areas that may require policy intervention. These insights serve as a valuable resource for policymakers, supporting the development of secondary legislation or new policy initiatives in the future. The report is expected to be published in Q2 2025. • ENISA, in collaboration with Connect and under the auspices of the Belgian Presidency of the Council, organised the second EU Cybersecurity Policy Conference. This event, which took place on 17 April 2024, focused on key EU policy files with cybersecurity provisions and bringing together the relevant communities.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction [2]	Biennial (survey)	> 90 %	90 %
1.1	Stakeholders will use evidence to understand how implemented policies have affected the targeted entities	Connect NIS CG NLOs	Nº of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	30	37

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

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
1.2	Stakeholders will use ENISA's advice to develop effective and consistent EU cybersecurity policies	Connect and other DGs or EUIBAs, depending on the policy file owner	N° of EU policies supported by ENISA	Annual (internal report)	5	6
			N° of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	30	37
1.3	Stakeholders are informed in a timely manner about gaps, overlaps and inconsistencies across EU policy initiatives under development	NLOs NIS CG Connect and other DGs or EUIBAs, depending on the policy file owner				

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	4.25	N° OF FTES ACTUALLY USED	3.23
PLANNED BUDGET (EUR) [3]	357 135.00	BUDGET CONSUMED (EUR) [4]	348 775.60
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	17 961.28

[3] Direct costs only.

[4] Direct costs only.

ACTIVITY 2

Supporting implementation of Union policy and law

Under Activity 2, ENISA supports the implementation of Union cybersecurity policy, particularly the revised NIS directive (NIS2).

Under this activity, ENISA:

- supports the NIS CG and its work programme;
- develops the technical framework underpinning the EU-wide implementing rules for the NIS2 security measures;
- implements the NIS2 EU Digital Infrastructure Registry (EUDIR);
- supports the EU-coordinated risk evaluations and toolboxes, such as the 5G toolbox, Nevers, Cyber posture, information and communications technology (ICT) supply chain;
- supports the EU's critical sectors, such as telecoms, energy, health, rail, etc.;
- particularly works to ensure alignment between NIS2 and sectorial policies, such as the Digital Operational Resilience Act (DORA) regulation and the network code for cross-border electricity flows.

In addition, ENISA supports the implementation of other policies with cybersecurity provisions, such as the EU's digital identity framework, the EUDI Wallets and the cybersecurity aspects of personal data protection rules.

Under this activity, the following was achieved in 2024.

- **ENISA delivered, on schedule, the technical advice to support the Commission with adopting the implementing rules for the NIS2 security measures, in close collaboration with the NIS CG.** Additionally, ENISA developed a full technical guideline for the EU-wide NIS2 security measures, which was initially planned for 2025, and kicked off a broad industry consultation about this important NIS2 guideline.
- **Following the delivery of an NIS360 pilot edition in 2023, ENISA further improved the NIS360 product to cover many more NIS sectors, including the most critical ones.** The new NIS360 methodology uses datapoints directly collected from 1 400 EU companies in the critical sectors, resulting in an NIS sector maturity/criticality quadrant.
- **The EUDIR was developed and released in production at the end of the year.** It aims to help national authorities across the EU implement the NIS2 'main establishment principle', by enabling cross-border supervision of entities in the NIS2 digital infrastructure sector.

The Council highlighted ENISA's valuable contribution to all the NIS CG workstreams in its December 2024 conclusions, showcasing the importance of ENISA's support for policy implementation. In the run up to the Parliament elections, ENISA sustained a community of experts on election security, coordinating multiple actions, delivering an updated compendium of good practices and feeding situational awareness to the community (in collaboration with Activity 4). The importance of the Nevers risk assessment process was further underlined by the Commission recommendations on subsea cables, adopted at the start of 2024, which will ensure action to address subsea cable risks. The contribution of ENISA to health is another example of the agency's impactful sectorial work. By promoting the EU Health-ISAC, sustaining an EU community of national health authorities, ENISA took a principal role in the Commission's EU health action plan, which was adopted in early 2025.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 2 moving forward:

- **Supporting the rapid implementation of NIS2 by the MS remains a high priority, when many of them are still transposing the legislation in 2025.** ENISA will continue to push for consolidation of the many NIS CG workstreams, and to improve coordination, implement an MS NIS implementation issue tracker. Under Activity 4, ENISA will coordinate across the EU CSIRTs network, Cyclone and the NIS CG, to exploit synergies between these three groups and to facilitate joint sessions on specific cybersecurity topics, such as elections and incident reporting.
- **The EU risk evaluations and toolboxes have become a top priority for the Council and the new Commission, for example the recommendations of the Niinistö report and the subsea cable recommendation.** ENISA will prioritise supporting these EU risk evaluation processes, and to streamlining them to speed up delivery. Additionally, to better support the technical aspects of these processes, the activity will explore synergies with the new ENISA unit for product security, technology and markets (Activity 8).
- **The sectorial focus of 2024 was adequate and will remain largely the same in 2025.** Supporting the NIS2 implementation in these sectors, and the implementation of sectorial rules, will remain a priority. Additionally, ENISA will support the finance sector stakeholders with implementing DORA, and the energy sector stakeholders with implementing the network code for cross-border electricity flows. A major new sectorial policy is the newly launched EU health sector cybersecurity action plan, which will be financed by Connect and will need to be implemented by multiple ENISA units and across multiple activities. Support for EUDI Wallets and EU's trust service authorities will continue under Activity 7 and Activity 8, respectively.
- **In 2025, to support the main objective of building resilience across the EU critical sectors, this activity will have a dedicated output for annual checking of the implementation of NIS2 in the critical sectors, grouping the policy implementation products:** the annual ENISA NIS investments report and the annual ENISA NIS360 report, which provide important input to the NIS2 Article 18 report.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO2. Cybersecurity as an integral part of EU policies	Level of maturity of cybersecurity capabilities and resources across the EU at the sector level [5]

[5] As part of the Article 18 report.

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGE
2.A Effective implementation of the NIS directive (NISD)	Article 5 of CSA and NIS2	First target: end of 2024 and then continuously	Cybersecurity index area **'Policy'** – indicator 2.3 'Implementation of cybersecurity related directives'	75 % of MS have implemented NIS2 by the end of 2024 RESULT: 25% for 2 months of 2024
2.B Improve maturity of NIS sectors	Article 5 of CSA and NIS2	2026	Average maturity of critical sectors Average maturity of less critical sectors – source NIS360.	One immature NIS1 sector increases maturity score One mature NIS1 sector increases maturity score
2.C Improve alignment between NIS2 and DORA	Article 5 of CSA	2026	Level of alignment between main NIS2 provisions (incident reporting and security measures) and DORA provisions in survey of JC-DOR and NIS CG	75 % of respondents say NIS2 and DORA are aligned on these topics

OUTPUTS	OUTCOME
2.1 Support MS and the Commission in the implementation of the NIS CG work programme and the NIS Directive	• In supporting the NIS CG, ENISA is the secretariat for six workstreams and supports four additional workstreams, including the 5G workstream, the ICT supply chain workstream, the elections workstream and the workstream for EU coordinated risk evaluations. • In supporting the Commission with publishing NIS2 implementing regulations, ENISA participated in the three comitology meetings of the NIS2 Cybersecurity Committee on the implementing act for NIS2 security measure and incident reporting. • In supporting the NIS2 transposition by MS, ENISA organised three 'NIS101' risk management training sessions for national authorities from the financial, energy and rail sectors, to help build up knowledge with the new authorities for the NIS2 implementation. ENISA also handled 15 individual MS requests for advice on NIS2 transposition. • In developing and hosting the EUDIR, ENISA managed to deliver the project on time (in Q4 2024), and before the NIS2 deadline for populating the Registry (17 January 2025). • The agency developed an NIS2 tool enabling dedicated sectorial NIS2 webpages on the ENISA website. This tool is pending data collection in 2025 from the MS that are still transposing the NIS2 at the national level.
2.2 Support MS with EU-wide risk evaluations and EU toolbox scenarios	• To respond to the Council conclusions on ICT supply chain security, ENISA supported the work of the NIS CG to create an EU ICT Supply Chain Security Toolbox. The toolbox includes possible risk scenarios against EU ICT supply chains, accompanied by a set of strategic and technical recommendations in order to mitigate the impact of these risk scenarios. The toolbox is expected to be adopted by the NIS CG in Q2 2025. • Stemming from the Council conclusions on the EU's cyber posture, the EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors report was adopted by the NIS CG, delivering a risk assessment and a set of cyber risk scenarios for the two sectors, along with key recommendations in areas such as resilience, improvement of cyber posture, crisis management and supply chain security.

OUTPUTS	OUTCOME
2.2 Support MS with EU-wide risk evaluations and EU toolbox scenarios	• EU-coordinated risk assessments have become a top political priority in 2025. ENISA continues to support the Commission and the MS in the recently merged NIS CV workstreams on risk assessments and ICT supply chain risks, to be able to fulfil the multiple different requests for EU risk evaluations. • ENISA delivered a guide on good practices for cyber resilience stress testing, which collects and identifies good practices and includes a step-by-step approach for cyber resilience stress testing. ENISA also began supporting the Commission's subsea cable expert group and is engaged to support future subsea cable stress tests. • The NIS360 methodology was improved in 2024. ENISA delivered a second version, which includes all critical sectors under NIS2 (22 sectors and subsectors in total). The new NIS360 methodology used data from 1 480 experts and changed from a self-assessment to an indicator-based evaluation. The outcomes were validated by both authorities and industry stakeholders. The outcomes feed into the EU-CSI, the Article 18 report and ENISA's sectorial work (Output 2.3). • ENISA delivered six bimonthly reports with sectorial situational awareness information for the NIS2 health, energy, transport and digital Infrastructure sectors. Regarded by stakeholders as a key piece of information for regular updated situational awareness, this report is now delivered to an audience that spans over 500 recipients, including Cyclone officers. • The Nevers action plan entered its second and last year, and ENISA keeps supporting relevant stakeholders (e.g. the European Competent Authorities for Secure Electronic Communications (Ecasec) group and the Body of European Regulators for Electronic Communications. Four out of the 10 technical recommendations in the action plan that ENISA is responsible for have been concluded. In 2025, two of the remaining four recommendations are planned to be discussed during ENISA's Telecom Forum. • ENISA continued to support the Commission's situation centre.
2.3 Improve cybersecurity and resilience of the NIS sectors	In 2024, under the ENISA NIS strategy, ENISA supported key NIS sectors with targeted packages/bundles of services: **Build,** to improve immature sectors; **Sustain,** for the continued support to already mature sectors and to ENISA leadership; **Involve,** for mature sectors where sectorial stakeholders take the lead; **Prepare,** for new NIS sectors which ENISA may support in the future. Some highlights from these packages/bundles are shown below. • **Health** (Build package) – the ENISA eHealth cybersecurity conference took place in Budapest. ENISA acted as secretariat for the NIS CG Workstream 12 on health, supported the EU Health-ISAC and mapped security requirements in the health regulatory frameworks. • **Rail** (Build package) – the 4th ENISA–European Union Agency for Railways conference for cybersecurity in the rail sector took place in Lille. ENISA also organised a cybersecurity essential and NIS2 workshop for the railway authorities who will supervise the sector and how entities comply with the NIS2 requirements. ENISA also mapped security requirements in the rail regulatory frameworks and relevant standards. ENISA supported the Landsec Working Party on Rail Security and engaged with expert groups like Rail CISO Forum, UIC CSSP, UITP, the European Committee for Electrotechnical Standardisation (CENELEC), ER-ISAC, ERJU System Pillar, and also supported the creation of IEC standard 63452 on railway cybersecurity with the Market Certification & Standardisation Unit.

OUTPUTS	OUTCOME
2.3 Improve cybersecurity and resilience of the NIS sectors	• **Telecoms and digital infrastructures** (Sustain package) – ENISA acts as the secretariat for both the Ecasec group of EU telecom authorities and NIS CG Workstream 10 on digital infrastructures, organising meetings and supporting NIS2 implementation. Within Ecasec, ENISA launched two NIS2 task forces on security measures and incident reporting. The agency also works closely on the Nevers process (Output 2.2), the EUDIR and NIS2 provisions on the "WHOIS" database (Output 2.1). The ENISA Telecom Forum, a flagship conference, took place in Helsinki. Key reports on smishing and internet modems, prepared in 2024, will be published in 2025. • **Trust** (Sustain package) – the ENISA Trust Forum 2024 took place in Heraklion. ENISA supported the ECATS group of EU trust services security authorities as a secretariat, by hosting ECATS meetings and supporting ECATS task forces. • **Energy** (Sustain package) – ENISA co-organised the Energy Cybersecurity Conference, together with ENTSO-E, E.DSO and ENCS, in Brussels. ENISA is also the secretariat of the NISCG workstream on Energy and organised a meeting in Brussels. ENISA also supports the EU Energy ISAC with situational awareness updates. ENISA also organised a cybersecurity essential and NIS2 workshop for the energy authorities. • **Finance** (Involve package) – ENISA signed a memorandum of understanding (MOU) with the three European supervisory authorities (ESAs), which are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA). ENISA is a member of the Joint Committee on DORA and supports the ESAs providing technical advice. In 2024, together with Activity 8, ENISA prepared a finance threat landscape, and organised a cybersecurity essential workshop for ESAs. In addition, ENISA supported FI-ISAC and hosted its meeting in Athens in May 2024. • **Space** (Involve package) – ENISA prepared the space threat landscape in collaboration with Activity 8 (to be published in 2025). • **Public administrations** (Involve package) – ENISA analysed MS approaches to public administrations, focusing on their scope, definitions, identification processes, and the application of risk-based assessments. • **Aviation** (Involve package) – ENISA supports the main aviation stakeholders, by participating in their groups and giving advice. ENISA is an observer in the Part-IS implementation task force.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction [6]	Biennial (survey)	> 90 %	92 %
2.1	MS will use ENISA advice to implement the NISD	Connect, NIS CG	EU register for digital entities is used by all MS	Biennial (survey)	Used by all MS	N/A – in production from 2025
			CVD guidance is implemented by MS and all MS are on the CVD map	Biennial (survey)	Used by all MS	N/A – map pending ENISA website update

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

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
2.2	• Support EU-wide risk evaluations and risk scenarios • Follow-up of previous EU-wide risk assessments (5G, Nevers) • Sectorial situational awareness reporting	Connect, NIS CG	N° of stakeholders involved in the NIS360	Annual (internal count)	120	1 480
			N° of sectorial situational awareness reports	Annual (internal count)	12	24
2.3	Stakeholders use the NIS service packages to improve security and resilience of the sectors	Connect, NIS CG, sectorial DGs, sectorial EU agencies	N° of critical sectors with a high level of cybersecurity maturity (NIS sector 360)	Annual (internal count)	4	4 (electricity, banking, telecom, core internet)
			N° and frequency of services delivered to NIS sectors according to the maturity of the sector	Annual (internal count)	24	28 services + 8 workflows

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	12.5	N° OF FTES ACTUALLY USED	9.72
PLANNED BUDGET (EUR) [7]	720 268.00	BUDGET CONSUMED (EUR) [8]	814 407.38
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	196 266.08

[7] Direct costs only.

[8] Direct costs only.

ACTIVITY 3

Building capacity

Under Activity 3, ENISA seeks to improve and develop the capabilities of MS, EUIBAs and various sectors to respond to cyber threats and incidents, and to increase resilience and preparedness across the EU. In parallel, the activity seeks to raise the overall awareness of cybersecurity risks and practices. Actions to support this activity include the organisation of large-scale exercises, sectorial exercises, 'capture the flag' competitions, trainings and attack defence competitions. In addition, the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem, including across borders, and assist in reviewing and developing national and EU level cybersecurity strategies.

Under this activity, the following was achieved in 2024.

- **Service mapping and framework development.** Successfully mapped capacity-building services to the ECSF and developed the cyber exercise framework, ensuring structured exercise planning, execution, and assessment. This achievement provides a foundation for aligning exercises with competency-based training approaches, leading to more targeted and effective skill development and cybersecurity maturity.
- **Exercise planning and execution.** Planned and conducted five cyber exercises, including a very successful Cyber Europe, enhancing organisational preparedness and resilience. The successful test of ENISA's technical 'Blueroom' solution, in the most complex exercise setup yet offered by the agency, also demonstrates a significant advancement in exercise realism and complexity. These exercises provide crucial opportunities for participating organisations to test their defences, identify vulnerabilities and improve their incident response capabilities, but also for EU-wide coordination.
- **Cybersecurity skills training.** Trained more than 2 000 cybersecurity professionals in critical sectors and national cybersecurity authorities, using the ENISA self-paced operational trainings platform, on hands-on cybersecurity topics and skill validation exercises. This significant contribution to upskilling the workforce directly addresses the growing demand for skilled professionals in the face of evolving cyber threats.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 3 moving forward.

- **Scalability.** Training a large number of professionals and conducting complex exercises highlighted the challenges of scaling these activities effectively while maintaining quality and personalised capacity-building.

Influence on future work: future training and exercise programmes will give priority to coordination, synergy and empowerment of stakeholders. This will involve maximising the use of online platforms like self-paced operational trainings, EU Academy, EU Learn etc. for broader reach and accessibility, combined with targeted in-person training for key stakeholders (like learning and training events) using complex exercise scenarios and Cyber Europe for high-impact, hands-on experience. In addition, cross-activity synergies should be strengthened (e.g. Activity 6). Empowering stakeholders to use ENISA's existing frameworks (e.g. Cyber Exercises Framework or solutions (e.g. Blueroom) to perform their own exercises would increase scalability. Developing communities of these stakeholders to share good practices and lessons learnt will generate more impact and value for them. This approach will optimise resource allocation while ensuring both reach and depth of learning. Investment in the Blueroom solution to support complex exercise design, delivery and evaluation will be prioritised.

- Practical skills focus and realism. The success of hands-on training and the demand for increasingly realistic exercises reinforces the critical need for practical skills development and immersive exercising experiences.

  Influence on future work: future exercise development will focus on hands-on exercises and realistic and real-world case studies. This includes investing in extensions of the Blueroom that facilitate skills acquisition, using ECSF as a basis. Exercise design will include current threat intelligence and simulating realistic attack scenarios, to maximise the transfer of learning to real-world situations. Collaboration with stakeholders and industry experts will be sought after, to ensure exercise scenarios reflect the latest attack techniques and defensive strategies.

- Framework integration. The development of the Cyber Exercises Framework emphasised the importance of standardised frameworks and procedures in driving consistent cybersecurity exercise practices and skills development.

  Influence on future work: future capacity-building outputs will be explicitly aligned with relevant internal and external frameworks (Cyber Exercises Framework, ECSF, Cyber Skills Academy attestation etc.) to ensure that the EU cyber workforce develops the skills and knowledge needed to address the skill gap and meet legal requirements.

To consolidate focus and maximise the impact of the above changes, certain actions will be taken, such as:

- ensuring that one-off training contribute to a sustained learning process;
- developing the exercises as a service model and platform;
- supporting the community with the Cybersecurity Challenge and International Challenge so that the community can build on the momentum from previous years and take more of a leading role in driving the challenges going forward.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO4: Cutting-edge competences and capabilities in cybersecurity across the EU	• Aggregated assessment of the level of cybersecurity capabilities in the public and private sectors across the EU [9] • Aggregated assessment of the level of maturity of national cybersecurity capabilities and resources, and the extent to which MS national cybersecurity strategies are aligned [10]

[9] As part of the Article 18 report.

[10] As part of the Article 18 report.

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET / RESULTS
3.A Increase the level of alignment and cooperation within and between MS, sectors and EUIBAs	Articles 6 and 9 of the CSA	2024	Nº of MS that use ENISA support and tools for the implementation, review and update of their national cybersecurity strategy (NCSS)	TARGET: All MS that have reviewed their NCSS using ENISA support and tools. RESULT: 27 MS
3.B Prepare and test capabilities to respond to cybersecurity incidents	Article 6 of the CSA	2024	Proportion of beneficiaries who take part in relevant ENISA exercises and training sessions	TARGET: All MS participate in Cyber Europe 2024 RESULT: 1 970 learners from 26 MS used the self-paced operational trainings platform TARGET: > 80 % of EUIBAs have participated in JASPER exercises over three years (number of participants in 2024 increases compared with 2023) RESULTS: Accomplished TARGET: 90 % of participants see positive added value RESULTS: Accomplished
			• Added value of ENISA exercises and training sessions	TARGET: 90 % of participants see positive added value RESULTS: Accomplished
3.C Increase skill sets and align cybersecurity competencies	Article 6 of the CSA	2024	• Assessment of the average level of cybersecurity technical competences of participants in European cybersecurity challenge finals	RESULTS: N/A [11]
			• Nº of participants that take part in national competitions improving cybersecurity skills and capabilities	TARGET: More than 10 000 participants take part in the annual 'capture the flag' competitions that are organised prior to the European Cybersecurity Challenge (ECSC) final RESULTS: Accomplished
			• Level of alignment of cybersecurity competences across the EU	RESULTS: MS national competence frameworks are aligned with the ECSF

[(°°)] A relevant metric is being developed in the ENISA security index

OUTPUTS	OUTCOME
3.1 Assist MS to develop, implement and assess national cybersecurity strategies	The NIS CG adopted the peer review methodology, a significant achievement driven by NIS CG Workstream 9 and ENISA. A peer learning session on governance frameworks for NCSS implementation engaged 23 participants from 13 MS, facilitating the exchange of expertise and national approaches. Finally, the upgrade of the national cybersecurity strategies interactive map was successfully launched, aligning both with the new ENISA website requirements and style, and with ENISA's future vision for NCSS work.
3.2 Organise large-scale biennial exercises and sectorial exercises	1. Service mapping and framework development: • successfully mapped Exercise Services to the ECSF, aligning exercises with competency-based training approaches, • developed the Cyber Exercises Framework and use of the evaluation framework, ensuring structured exercise planning, execution, and assessment; 2. Exercise planning and execution: • planned and conducted five cyber exercises, including a very successful Cyber Europe, enhancing organisational preparedness and resilience, • laid the groundwork for National HealthEx (Cyber Europe replay exercise), scheduled for February 2025, demonstrating a commitment to iterative improvement and scenario refinement, • successfully tested the Blueroom solution in the most complex exercise setup offered by the agency.
3.3 Organise trainings and other activities to support and develop maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS CG, EU-CyCLONe and work streams, ISACs and other communities	• Organised three learning and training physical events (11 days total). Two of them focused on CSIRT teams, providing hands-on training on technical topics and skills validation exercises, enhancing their incident response capabilities. The other one focused on the cybersecurity workforce in the public sector (national and EUIBA). • Provided access to over 344 CSIRTs network members from 10 MS to the full catalogue of the ENISA self-paced operational trainings platform with hands-on trainings on a variety of cybersecurity topics and skills. • Developed a bespoke CSIRTs network standard operating procedure (SOP) training module in the ENISA self-paced operational trainings platform, accessible by the aforementioned CSIRTs network members with licenses through the ENISA support action.
3.4 Organise and support cybersecurity challenges, including the ECSC	The ECSC 2024 in Turin, Italy, marked a pivotal moment in cybersecurity competitions, driving improvements in competition quality, international collaboration and diversity. The competition format saw significant advancements in technical infrastructure and stricter quality controls, ensuring a fairer and more transparent event. At the same time, Team Europe's success at the International Cybersecurity Challenge (ICC) in Chile reaffirmed the strength of European training programmes, demonstrating the high level of preparation and skill within the European cybersecurity community, yet highlighted the necessity of a structured, sustainable year-round preparation model from 2025 onwards. A key lesson learned was the need to extend these standards beyond ECSC, leading to efforts to convince the ICC Steering Committee to adopt similar measures for international competitions, ensuring consistency and integrity across global cybersecurity challenges. The first-ever all-female team was built and competed at the Kunoichi games in Japan, achieving a ground-breaking victory, demonstrating the impact of dedicated female mentorship and training. OpenECSC played a crucial role in 2024, serving as a training and selection platform for national teams, as well as the 'Compete with Team Europe' event. Given its success, plans for 2025 include expanding OpenECSC into a broader skills and reskilling platform, and transforming 'Compete with Team Europe' into a larger initiative, allowing more communities to participate in training events and fostering a stronger cybersecurity talent pipeline.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	90 %	92 %
3.1	• Increase the level of preparedness and cooperation • Prepare capabilities to respond to cybersecurity incidents • Increase skill sets • Align cybersecurity competencies • Improve national cybersecurity strategies	NLO subgroup on national cybersecurity strategies	Maturity of national cybersecurity strategies, ISACs, SOCs, etc.	Annual (report)	N/A	N/A
3.2	• Increase the level of preparedness and cooperation • Prepare and test capabilities to respond to cybersecurity incidents • Conduct stakeholder tests and improve capabilities and increase capacity	• NLO network (as necessary) • CSIRTs network (as applicable) • EU-CyCLONe members (as applicable) • NIS CG (as applicable) • EU ISACs (as applicable) • NLO subgroup of Cyber Europe planners (as applicable)	Stakeholder satisfaction	Biennial (survey)	90 %	**95.5 %**
			Evaluation of capacity-building measures by participants in exercises and training	Annual (report)	> 50 % high usefulness	**52.5 %**
			Nº of participants in training sessions organised by ENISA	Annual (report)	> 500 (including online exercises)	**~ 5 000**

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
3.3	• Increase the level of preparedness • Prepare capabilities to respond to cybersecurity incidents • Increase skill sets • Stakeholders improve capabilities and skill set	• NLO network (as necessary) • CSIRTs network (as applicable) • EU-CyCLONe members (as applicable) • NIS CG (as necessary) • EU ISACs (as applicable) • NLO subgroup of Cyber Europe planners (as necessary)	Nº of participants in training and in challenges organised by ENISA	Annual (report)	> 1 000 (including online training)	> 2 047 (1 970 self-paced operational trainings + 77 in three learning and training events)
3.4	Align cybersecurity competencies Increase skill sets	ECSC Steering Committee (NLO subgroup)				

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	12.45	Nº OF FTES ACTUALLY USED	10.62
PLANNED BUDGET (EUR) [12]	1 236 591.00	BUDGET CONSUMED (EUR) [13]	1 327 063.56
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	234 691.30

[12] Direct costs only.

[13] Direct costs only.

ACTIVITY 4

Enabling operational cooperation

Under Activity 4, ENISA supports operational cooperation among MS and EUIBAs and between operational activities. The main goal of the activity is to provide support and assistance in order to ensure the efficient functioning of EU operational networks and cyber crisis management mechanisms.

Under this activity, the following was achieved in 2024.

1. Effectively increased the trust and preparedness of the operational networks;
2. Successful finalisation of the first phase of the EUVD, and ENISA strengthened its role by becoming a CNA;
3. Enhanced scalability, resilience and security of the operational IT infrastructure.

Effectively increased the trust and preparedness of the operational networks. As per the provisions of NIS2, ENISA supports and ensures the functioning of both the technical layer (EU CSIRTs network) and the operational layer (EU-CyCLONe), in terms of powering every aspect of the network's operations, providing infrastructure and tools, and standing ready to support the networks in case of incidents and situation of EU interest. The year 2024 was pivotal for both networks, due to the NIS2 transposition and the challenging geopolitical environment that requires increased trust and preparedness. This culminated in the joint coordination of the CSIRTs network and EU-CyCLONe in response to the Romanian election interference in December 2024 that resulted in the first joint executive summary signed by both networks.

ENISA supported the coordination during key cybersecurity events in 2024, such as high-profile vulnerabilities, and enabled everyday information-sharing during incidents, vulnerabilities, specific targeted campaigns and situations of EU interest, such as elections and the Olympic Games. The agency showed its commitment to facilitating the seamless cooperation among the CSIRTs network and EU-CyCLONe, supporting them to be efficient EU operational networks. Through the support under this activity, the cooperation strengthened and these operational networks increased their maturity levels. The agency also focused on supporting the networks' preparedness and shared situational awareness in concert with Activity 5, while also building the trust that is needed during escalations and situations of EU interest. Through its secretariat role, ENISA facilitated the interaction within and across these networks, both in non-escalated and escalated modes.

ENISA drafted the 'First EU Cyclone report for the European Parliament and Council' and the 'First CSIRTs Network NIS2 Report to the Cooperation Group'. ENISA engaged in this work on behalf of the Council presidencies and with the contribution of network members, to further ensure and report on the cooperation among operational networks.

These reports outlined the successes and challenges of both networks and paved the way to future developments. In attestation to the agency's role and in recognition of its contribution to the overall ecosystem, the December 2024 Council conclusions stressed 'that ENISA fulfils an important role as secretariat of the two EU-level Member States driven cyber cooperation networks, the CSIRTs network and EU-CyCLONe'.

The activity achieved effective cooperation, seamless integration and robust and secure tooling/platforms via the final full deployment of the CSIRTs network central services (formerly known as MeliCERTes), where the CSIRTs network reached its next level of cooperation. The deployment enables the use of tools operated by the CSIRTs network members, allowing the network as a whole to easily scale and federate with any future service that its members want to offer to their peers.

Successful finalisation of the first phase of the EUVD and ENISA strengthening its role by becoming a CNA. ENISA made significant progress in consolidating operational IT asset management and enhancing vulnerability coordination across the EU. Among the most impactful achievements of the activity, the successful finalisation of the first phase of the EUVD stands out, with the proof of concept completed and the production environment launched, supported by robust security controls and outreach initiatives.

Enhancing the scalability, resilience and security of operational IT infrastructure. The automation of user management for the CSIRTs network significantly streamlined access control, improving operational efficiency and coordination. Another key milestone was the migration of EU-CyCLONe tools to Azure, enhancing scalability, resilience and security. These efforts contributed to a more secure and efficient cybersecurity ecosystem, reinforcing ENISA's role in coordinating cybersecurity efforts across MS.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 4 moving forward.

- First, to give further priority to the automation of security operations, which would enhance efficiency and allow for a more scalable approach to cybersecurity crisis management.
- Second, a critical gap was identified in ENISA's internal solution architecture capabilities. Integrating a solution architect within ENISA would provide a structured approach to system design, ensuring better alignment between technical requirements and strategic objectives while reducing dependency on external contractors.
- Finally, the operational role of IT was expanded, and therefore requires additional resources to widen the experience of the team. Addressing this gap through additional resources and targeted capacity-building efforts will be crucial in ensuring the team can effectively support the expanded mandate.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO3: Effective cooperation among operational stakeholder within the EU in case of massive cyber incidents	Level of cooperation and availability (disruptions) and use and trust of EU-level networks, tools and databases

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET / RESULTS
4.A Enable trust and effective cooperation and operations of CSIRTs network and EU-CyCLONe members.	Article 7 and NIS2	2024	Satisfaction with scalable ENISA support	TARGET: 80 % satisfaction of stakeholders RESULTS: • **CSIRTs network** Secretariat performance evaluation 8/10 • **EU-CyCLONe** Secretariat performance evaluation 9/10
			Maturity of operational communities	TARGET: Average overall level of maturity increases year by year RESULTS: • **CSIRTs network** Members added value 8/10 • **EU-CyCLONe** Members added value 8/10
4.B Ensure a high level of coordination of the vulnerability disclosure services within the EU.	Article 7 and NIS2	2026	EUVD usage and added-value	• EU vulnerability disclosure services are gradually becoming available (numbering services in place) and aligned with national mechanisms • EUVD is functional and aligned with national mechanisms
4.C Robust and secure tools/ platforms are established and actively used to facilitate seamless operational collaboration at the EU level.	Article 7 and NIS2	2024	Continuous operations and use of secure communication tools and platforms for EU-CyCLONe and Cooperation Network including the use of regular checks and controls	No significant disruption or incidents in the working of operational tools and platforms recorded against standard checks and controls Beneficiaries use the tools RESULTS IN 2024: No significant disruptions Increase in the use of tools by beneficiaries see results at output level indicators

OUTPUTS	OUTCOME
4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs network and EU-CyCLONe members.	In 2024, ENISA played a crucial role in empowering the CSIRTs network and EU-CyCLONe, facilitating their operations, information-sharing and coordinated response to cybersecurity threats. ENISA's efforts, as mandated by NIS2 Articles 15 and 16, focused on strengthening these networks and fostering collaboration between them. CSIRTs network. ENISA, through its secretariat team, powered every aspect of the network and provided continuous operational and information-sharing support to the CSIRTs network members. In terms of reporting, coordinated response and information sharing. The secretariat team enabled coordination during critical cybersecurity events, such as vulnerabilities and the Romanian election situation, as well as ongoing information-sharing related to incidents, vulnerabilities, campaigns and situations of EU interest (e.g. elections, Olympic Games). Moreover, the team facilitated interaction with the private sector during specific incidents and vulnerabilities. The secretariat team also drafted the network's first NIS2 report for the Cooperation Group, as mandated by NIS2 Article 15(4), on behalf of the relevant Council Presidencies and with the contribution of all WG leaders. The report outlines success and challenges of the network since the entry into force of NIS2. The ENISA secretariat team also worked on streamlining information-sharing by bolstering initiatives like the bi-weekly situational digests and reporting dashboards to simplify MS input. This was done alongside efforts for capability advancement, such as supporting updates to the SOP reporting template and empowering the discussions in the WGs focused on tools, SOPs, maturity, training sessions, reviewing NIS2 founding documents and the newly established topics. The ENISA secretariat team also supported the input related to CVD policies, the CRA single reporting platform (SRP), NIS2 procedure alignment, EU-CyCLONe coordination, CSIRT tools and peer review input. As part of its organisational and coordination role, and in concert with the Belgian and Hungarian Council Presidencies, the ENISA secretariat team organised the 22nd EU-CSIRTs network meeting in Brussels, the 23rd EU-CSIRTs network meeting in Ghent, the 24th EU-CSIRTs network meeting in Budapest and the annual workshop for CSIRTs and law enforcement. In concert with the infrastructure sector, the team also coordinated the full deployment of the CSIRTs network central services (formerly MeliCERTes), enabling scalable operations and federation with member-provided services. EU-CyCLONe. ENISA also powered every aspect of EU-CyCLONe and, through the secretariat team, supported the daily information-sharing and development of this network. In particular, in concert with the trio of Council Presidencies, the team drafted and supported the adoption of rules of procedure as mandated by NIS2 Article 16(4), and of the first report to Parliament and the Council, as mandated by NIS2 Article 16(7). In terms of preparedness and awareness, the ENISA secretariat team supported the WGs on SOPs and exercises, particularly regarding the coordination with the CSIRTs network and the orchestration of BlueOlex and other exercises. In this respect, the agency also organised BlueOlex, which was hosted in Rome by the Italian Cybersecurity Agency, under the Hungarian Presidency of the Council. The ENISA secretariat team also enabled enhanced information-sharing during elections and the Olympic Games, organised ad hoc calls with cybersecurity stakeholders and produced dedicated reports for EU-CyCLONe members to support their development. The year 2024 also saw EU-CyCLONe reaching the next step in terms of impact assessment and coordination, which resulted in coordination and reporting during situations of EU interest. This was the case in particular in the first EU-CyCLONe escalation in relation to the Romanian election situation and joint coordination with the CSIRTs Network. In terms of building trust and coordination, in concert with the Belgian and Hungarian Council Presidencies, ENISA coordinated the organisation of the 14th EU-CyCLONe officers' meeting in Namur, the 15th EU-CyCLONe officers' meeting in Ghent, the EU-CyCLONe executives' meeting in Ghent, the 16th EU-CyCLONe officers' meeting in Budapest and the 17th EU-CyCLONe officers' meeting in Brussels.

OUTPUTS	OUTCOME
4.1 Ensure essential operations to foster seamless cooperation and robust interaction among the CSIRTs network and EU-CyCLONe members.	Joint efforts. ENISA's focus for 2024 was on facilitating seamless cooperation among CSIRTs network and EU-CyCLONe members for efficient EU operational networks, prompt incident response and cyber crisis management. In this respect, the agency organised several cross-network activities to foster trust-building across the different communities, which resulted in the first shared EU-CyCLONe / NIS CG session in Namur and the first shared EU-CyCLONe / Horizontal Working Party on Cyber Issues (HWPCI) session in Ghent. These sessions were in addition to the usual shared CSIRTs network / EU-CyCLONe session and the first joint team-building CSIRTs network / EU-CyCLONe session, both of which took place in Budapest. The agency also fostered joint cooperation in terms of preparedness and shared situational awareness that resulted in successful integration during Cyber Europe, and further synchronisation of the CSIRTs network and EU-CyCLONe WG SOP leads during the year, including the input to the blueprint revision. Moreover, the agency organised a workshop on intra- and inter- network communication for the first time during cyber crisis for the CSIRTs network and EU-CyCLONe and HWPCI members. From an operational point of view, all this work resulted in the first joint coordination of the CSIRTs Network and EU-CyCLONe, related to the Romanian election situation.
4.2 Design and architect processes and tools to build an EU Vulnerability Database in close cooperation with the MS	ENISA successfully finalised the first phase of the EUVD by meeting the minimum requirements, completing the proof of concept and launching the preproduction and production environments. To ensure a secure and resilient system, a comprehensive set of security controls was implemented, including an external code review, a penetration test (pentest) report, and hosting in Azure with distributed denial of service protection. Communication efforts were also reinforced, with question and answer (Q & A) documents and press releases prepared to inform stakeholders. Outreach initiatives to the US Cybersecurity and Infrastructure Security Agency (CISA), CERT-EU and international conferences ensured the visibility and credibility of the EUVD within the cybersecurity community. To streamline operations, ENISA established clear processes and methodologies for handling MS requests, ensuring that vulnerability coordination is only provided upon request from the EU CSIRTs network. Standard operating procedures were drafted and validated to facilitate this process. The database integrated advanced predictive and automation tools, such as the Exploit Prediction Scoring System to assess exploitability and the common security advisory framework (CSAF) to enable rapid responses to reported vulnerabilities. Security measures were further reinforced with planned training sessions for both internal ENISA users and external stakeholders, with internal training set for completion by the end of Q1 2025. Strategically, ENISA strengthened its role by becoming a CNA and setting the foundation to become a Root CNA by 2026. Collaboration with MS was deepened through the CSIRTs network and benefited from open-source tools, such as the CIRCL Vulnerability Lookup, to build the database. ENISA drove the work of the WG on CVD, ensuring engagement through four coordination calls and a joint workshop within the CSIRTs network and the Cooperation Group.
4.3 Operate, maintain and promote operational cooperation infrastructure for the EU cyber security communities.	ENISA has made significant strides in consolidating IT assets to enhance service delivery for MS and external stakeholders. A comprehensive vision and mission were developed, along with strategic objectives to unify IT asset management under a structured approach. These efforts laid the foundation for improved operational efficiency, cost optimisation and stronger cybersecurity governance. A key achievement in automation was the successful deployment of automatic user management for the CSIRTs network, streamlining access and identity controls. The development of an automatic dashboard for the CSIRTs network started and aims to provide enhanced visibility improving coordination across the EU. Scalability was another major milestone, demonstrated by the successful migration of EU-CyCLONe tools to Azure. This transition not only ensured a more resilient and scalable infrastructure, but also enhanced security and performance. At the same time, ENISA strengthened its cybersecurity posture through the development of three dedicated security projects. First, a structured approach to security controls was established, fully aligned with ENISA's IT strategy and IT Management Committee (ITMC) recommendations. Second, security specifications were harmonised across all outsourced contracts and support services, ensuring consistent protection measures. Third, a series of targeted security enhancements were implemented across key platforms and services. These security enhancements included the deployment of EU-LOGIN multi-factor authentication for EU-CyCLONe, improving authentication robustness. In CSIRTs network services, multi-factor authentication was integrated into active directory federation services, reinforcing identity security. The DORA incident response framework was strengthened with enhanced security requirements ahead of its production launch. The EUVD was designed with a security-by-design approach, underwent a thorough pentest and completed an external code review.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	> 90 %	88 %
4.1	Enhanced information sharing and cooperation among CSIRTs network and EU-CyCLONe members	CSIRTs network and EU-CyCLONe members	Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)	N/A	99.95 % up time
4.2	ENISA provides numbering services for CVEs with a view to gradually establishing the EUVD	CSIRTs network and NIS CG	Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)		Not yet launched in 2024
4.3	Usage of the available tools	CSIRTs network and EU-CyCLONe members	N° of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA	Annual (report)	> 5 % increase	
			CSIRTs active users, % increase year-on-year			+ 27 %
			CSIRTs number of exchanges/interactions, % increase year-on-year			+ 35.46 %
			EU-CyCLONe active users, % increase year-on-year			+ 14.55 %
			EU-CyCLONe number of exchanges/interactions, % increase year-on-year			- 6 %

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	10.5	N° OF FTES ACTUALLY USED	8.65
PLANNED BUDGET (EUR) [14]	1 776 494.00	BUDGET CONSUMED (EUR) [15]	1 787 723.45
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	736 775.74

[14] Direct costs only.

[15] Direct costs only.

ACTIVITY 5 (a)

Contribute to cooperative response at Union and Member States level through effective situational awareness

Under Activity 5a, ENISA contributes to the cooperative response at the EU and MS levels primarily through effective situational awareness. The work was carried out primarily through three main activities:

- internal capabilities development to establish a threat information management system, also to strengthen collection, analysis and dissemination capabilities;
- collaboration with MS and EU entities to create joint assessments and a common view on threats, incidents and vulnerabilities impacting the EU;
- continuous development of the ENISA CPP, aiming at involving selected industry players in contributing to the EU common situational awareness.

In 2024, the agency further strengthened its situational awareness capabilities by working on establishing a Threat Information Management system, improving its processes and procedures, increasing the cooperation with external operational entities, primarily MS through the CSIRTs network, and EU entities, such as CERT-EU and Europol EC3. It also consolidated and leveraged the ENISA CPP to embed the private sector contribution, primarily within the EU-JCAR (CSA Article 7.6).

Under this activity, the following was achieved in 2024.

1. A new threat management system was introduced in 2024 to meet the objective of disseminating accurate and timely threat information to stakeholders. This allowed the agency to improve the quality of its analysis of the agency's deliverables, increase the speed of disseminating threat information, and was instrumental in improving collaboration with MS and EUIBAs.
2. Establishment of the EU-JCAR, a quarterly report produced jointly with CERT-EU and Europol EC3, along with contributions from MS and the industry via the CPP. This report fulfils the requirements under Article 7.6 of the CSA and is the technical/operational tool at the EU level for EU common situational awareness. In 2024, ENISA exited the pilot phase and formalised the report and its preparation life cycle. The number of contributing MS also increased, while the CSIRTs network and EU-CyCLONe were also involved in the process.
3. Establishment of the ENISA CPP. This is a voluntary, non-commercial programme for private sector cooperation, augmenting the agency's visibility and understanding of threats, vulnerability incidents and cyber security events. It targets companies from around the

world across the whole supply chain, and has visibility on the global threat landscape. Its main purpose is to contribute to increasing the EU common situational awareness.

The agency executed on all key performance indicators (KPIs) and met the objectives set at the beginning of the year despite reduced financial resources. The agency invested in this activity with additional resources allocated throughout the year, including by unlocking resources assigned to other activities within the agency, primarily Activity 5b.

The agency therefore achieved a high level of process standardisation and quality, which should allow further consolidation of the situational awareness tasks.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 5 moving forward.

- To streamline and consolidate production pipelines to integrate new tasks and reporting sources within standard production. This will enable better situational awareness and will save resources. This process is underpinned by a consolidation of tools. The development of the SRP, provided for by the CRA, is an opportunity for ENISA as it falls into this objective. A phased approach to the project is foreseen, with priority given to meeting the requirements of the CRA.
- To increase cooperation with MS, in order to better address their needs by fostering a more structured approach and by building more accurate and reliable situational awareness. This can be done by investing in tools which would facilitate cooperation and help coordinate information exchange. This would efficiently structure the engagement with relevant entities within MS, where ENISA could take an aggregator role, transforming the service and product from ENISA-led to EU-led.
- To further nurture cooperation with primary stakeholders and refine primary intelligence requirements, which will enable the agency to further tailor its services and produce value as expected.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO3: Effective operational cooperation within the Union in case of massive (large-scale, cross-border) cyber incidents	Risk level due to cyber threats is understood by the cybersecurity communities at Union level and decision-makers are able to prioritise actions to manage the risk

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
5a.A Threats and information are disseminated in a timely and accurate manner and/or available on demand	Article 7	2025	• Recipients are promptly and accurately informed about the latest threats, vulnerabilities and incidents • Usefulness of situational reports	• At least 80 % of recipients found the information being communicated promptly and accurately based on the level of confidence of the information. • At least 80 % of recipients found the reports useful
5a.B Improved common situational awareness through joint assessment, threat and risk analysis	Article 7	2025	• Stakeholders' ability to make informed decisions based on joint situational reports • Usefulness and timeliness of joint situational reports	• 100 % of quarterly JCAR reports have been issued on time • At least 80 % of recipients find the reports useful
5a.C Information exchange to augment EU common situational awareness through cooperation with private sector and non-EU entities	Article 7	2026	• The CPP is established • Information coming from private-sector partners and non-EU entities are part of the operational cycle of situational awareness production	• 90 % of selected entities are enrolled in the ENISA CPP • 90 % of the participating entities are actively contributing by exchanging information

OUTPUTS	OUTCOME
5a.1 Collect, organise and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports and threats, and support consolidation and exchange of information on the strategic, operational and technical levels [16]	The work under this output focused primarily on establishing a strong threat information management platform as well continuous improvement on the collection, monitoring and analysis processes. In addition, the agency formalised the methodology of Article 7.6 of the CSA report, also known as EU-JCAR, which exited the pilot phase and is now in production. This product is a joint assessment done with partnering operational stakeholders within EUIBAs, with contributions from a number of MS (11 at year end) and selected industry players via the ENISA CPP. In 2024, the agency continued to deliver on its entire situational awareness service catalogue, including the establishment of ENISA sectorial reports to support the NIS360 strategy.

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

OUTPUTS	OUTCOME
5a.2 Provide analysis and risk assessment jointly with other operational partners including EUIBAs, MS, industry partners, and non-EU partners	The agency's achievements in this area can be summarised as follows. • Improved **structure of daily collection and monitoring** through the first **ENISA cyber threat intelligence (CTI) doctrine.** As a result, the agency achieved **higher collection (> + 160 %)** while maintaining levels of accuracy and timeliness. ENISA expects to maintain this level in 2025 with throughput reaching a plateau. • Processes and tools. In 2024, all listed events were tracked and **enriched in OpenCTI, the daily round-ups are stored and delivered via the platform,** and the agency started operationalising the information stored (e.g. sectorial reports and ENISA threat landscape). • **Standardise process for Daily Briefs** and reports providing up-to-date information about relevant events. The daily brief makes use of the URSA dashboard for delivery. • Reached a **synthesis** on **SOPs for the EUIBAs,** involving the European External Action Service **(EEAS), EC3, CERTEU and ENISA,** as a joint procedure in case of large-scale or relevant incidents or events. These SOPs were being further refined in terms of tools and processes. • Continued delivering on **standard product portfolio maintaining level of quality and customer satisfaction.** Increased numbers of flash reports as a result of higher number of interesting events. Contributed to three ISAA workflows (IPCR activation on UA-RU, IL-HAM, EU election). • Successfully **exited the JCAR pilot and moved to production** with a **satisfaction score of 4.3 out of 5.** Established and ran a process to integrate MS **(currently 11 contributing MS)** and industry input via the **ENISA CPP.** • Executed on **synergies with other operational activities.** Increased integration on dataset for **ENISA threat landscapes** and operationalised **Sectorial Reports** part of NIS360 strategy (health, energy, transport, digital) with a satisfaction **score of > 4 out of 5.** • **Executed on SitCen strategy** by onboarding two HCs, which allowed the **offboarding** of a number of tasks (e.g. ISAA and review of CCTF bi-weekly report). • Nurtured cooperation with **CERT-EU** via structured cooperation. Co-produced **12 JRRs** to date and managed the **programme and joint initiatives.** Achieved the **first rotation of ENISA in EC3,** resulting in actual participation in cybercrime operation **(Operation on Anon Sudan)** and better mutual understanding of processes and tasks. • Increased participation in the CDT process via situational awareness. Provided **eight briefings at HWPCI** which contributed to increased relevancy of ENISA as a key player in situational awareness at the EU level. • Supported **ENISA international engagements** by **setting up processes and methodology** for operational exchanges with industry via the **CPP,** and with **CISA and Ukrainian authorities.** Executed four exchanges on the threat situation with Ukraine and one with CISA. The resource issue noticed in 2023 was partially offset through the addition of a number of new FTEs in 2024, along with the release of the resources previously assigned to Activity 5b during the year. The activity was also slightly impacted by the preparation activities related to the implementation of the CRA SRP. In addition, the participation within the activities of the Commission Situation Centre initially required an investment from the current allocation of FTEs, which was eventually offset once the hiring of resources was concluded (Q4 2024). This activity was also impacted by a reduced budget due to horizontal cuts in the agency, which was compensated for by terminating the Twitter/X subscription. The majority of the budget was used to procure expert CTI services and subscriptions, and for advancing the establishment of a threat information management platform. The agency therefore achieved a high level of process standardisation and quality, which should allow further consolidation of the situational awareness tasks. The consolidation of other tasks within Strategic Situational Awareness (threat landscapes) with Incident and Vulnerability means that in 2025, reporting (NIS2 and EUVD) under this activity will result in stronger synergies and further savings (expected in 2026), along with increased focus and quality in delivery.

OUTPUTS	OUTCOME
5a.2 Provide analysis and risk assessment jointly with other operational partners including EUIBAs, MS, industry partners, and non-EU partners	The agency cannot achieve the EU common situational awareness process on its own. Over the past years, the agency has built experience and processes, and has the talents and skills needed to support the process. The consolidation of NIS2 reporting and vulnerability-led sources (such as CRA SRP and EUVD) will provide additional input. However, engagement from the MS does require further structuring, in order to draw a realistic mapping of the EU threat and situational picture that will eventually be needed to support situational awareness in relation to large-scale incident cyber crisis.
5a.3 Maintain, develop and promote ENISA's CPP aiming at information exchange to support the agency's understanding of threats, vulnerabilities, incidents and cyber security events	In 2024, the agency established and piloted the ENISA CPP, a programme for private sector cooperation augmenting the agency's visibility and understanding of threats, vulnerabilities incidents and cyber security events. The programme supports the mission of the agency to achieve a high common level of cybersecurity across the EU. It targets companies from around the world, across the whole supply-chain, with visibility on the global threat landscape. Its main purpose is to contribute to increasing the EU common situational awareness. The agency's achievements in this area can be summarised as follows. • Onboarded 10 companies as per the initial plan. This includes selection, establishment of MOUs to govern the activities and active involvement in the activities. • Established internal methodologies and a standard operating procedure to execute the programme. Exited the pilot. • Supported situational awareness activities, primarily through contribution to the EU Joint Assessment Report, along with other ad hoc workshops and interactions, including briefings for the CSIRTs network on specific threats, incidents and vulnerabilities. • Established a procedure to exchange information with CPP members through RFI [17]. Established, jointly with CPP members, metrics and KPIs to monitor the effectiveness of the programme as well as participation and value added. This output operated with reduced resources for half of the year, specifically until resources were unlocked through the hiring in Activity 5b. Even so, the agency managed to conclude the pilot and reached the KPI set at the beginning of the year. The agency is now equipped with an established programme to cooperate with selected private-sector industry players in the context of CTI and situational awareness. This programme can be used in the future by ENISA to continue supporting its current and/or future tasks, such as the incident review mechanism provided for in the CSA.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	> 90 %	88 %
5a.1	• Establishment of a threat information management platform. • Production of briefings, reports and summaries of incidents, threats and vulnerabilities	CSIRT network, EU-CyCLONe, EUIBAs, national authorities within MS subscribed to the products	Timeliness and accuracy of reports	Annual (survey)	Above 4	4.14 out of 5 for accuracy and 4.21 out of 5 for timeliness

[17] Request for information.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
5a.1	• Increased understanding and timely access to information regarding the latest threats, incidents and vulnerabilities					
5a.2	• EU joint assessment and reports, sectorial analysis, threat and risk analysis [18] • Recipients receive accurate and timely assessment of threat actors and associated risk to the EU internal market	CSIRT network, EU-CyCLONe, EUIBAs, HWPCI, MB	Nº of contributing MS and relevant EUIBAs	Annual (report)	N/A	EUIBAs: 4 out of 4 (Commission, CERT-EU, EC3 & EEAS) MS: 11 [19] out of 27
5a.3	• Establishment and operation-alisation of the CPP • ENISA situa-tional aware-ness leverages private-sector partnership to augment the context and understanding of threats, vulnerabilities and incidents	CSIRT network, EU-CyCLONe, EUIBAs, HWPCI, MB	Nº of new and total partners in the ENISA partnership programme	Annual (report)	10/4	4 new and 10 in total
			Percentage of RFI answered by members of the partnership programme	Annual (report)	80 %	84 %

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	9.25	Nº OF FTES ACTUALLY USED	7.85
PLANNED BUDGET (EUR) [20]	867 459.00	BUDGET CONSUMED (EUR) [21]	879 730.71
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	224 896.59

[18] Including JCAR, JRR, Union Report, Joint Publication, CERT-EU Structured Cooperation, EC3 Cooperation and Connect Situation Centre.

[19] Contribution to JCAR.

[20] Direct costs only.

[21] Direct costs only.

ACTIVITY 5 (b)

Contribute to cooperative response at the EU and Member State levels through *ex ante and ex post* services provision

Under Activity 5b, ENISA contributes to further developing preparedness and response capabilities at the EU and MS levels for large-scale cross-border incidents or crises related to cybersecurity through the implementation and delivery of ex ante and ex post services. This is done via the cybersecurity support action, by providing pentests, threat hunting, risk monitoring and assessment and customised exercises, and by supporting the MS with incident response. The services are delivered upon request from the MS participating in the programme and, when needed, ENISA might use external commercial service providers to deliver part of the services.

In 2024, this activity was financed through a contribution agreement concluded between the agency and the Commission in December 2023, and implemented through the action 'Incident response support and preparedness for key sectors', as described in the main digital Europe programme (DEP) 2023–2024 work programme. The budget is used to procure services from external service providers but also to cover the salaries and missions of 10 Contract Agents which were hired to implement this programme. Additional budget was used to cover other expenses, such as the payment of central validation services via a service-level agreement (SLA) with the Research Executive Agency (REA).

ENISA operated as planned for this activity, despite the new requirements which were introduced through the funding via the DEP. In order to comply with these new requirements, the agency had to launch new tender procedures and conclude an SLA with the REA to perform the needed assessments. The agency was therefore unable to deliver some of the services requested in 2024 and had to postpone them to 2025. However, the agency fully met the forecasted figures for 2024 in terms of execution of the programme.

Under this activity, the following was achieved in 2024.

- Contribution to increase preparedness and ability to respond to cyber threats across the EU by consolidating a total of 482 request of services, of which 157 were fulfilled during the year. Specifically, the following services were delivered: 65 pentests / threat hunting; 9 new incident response retainers; 2 exercises; 32 trainings engagements; 6 other ad hoc services.

- Launch of new tender procedure to support the agency in service delivery and to comply with Article 12(5) of the DEP. This also required an SLA with REA to support the agency with the ownership and control assessment (OCA). With this tender, ENISA seeks to procure a larger set of services to facilitate the implementation of the cybersecurity support action and the Cyber Reserve, and possibly cater for future needs of the agency.

- Preparation for the transition to the implementation of the Cyber Reserve as per the CSA by establishing and testing methodology for an incident response retainer conversion. This will enable a fast transition to the Cyber Reserve once the Cyber Solidarity Act enters into force.

The major challenges in 2024 were primarily due to compliance with the DEP regulation and in particular the OCA. This introduced notable delays in the delivery of services to some MS – but has now been overcome, due to the conclusion of a new tender procedure.

On the basis of the lessons learned from 2024, in 2025 the priorities for the work in this area are summarised below:

- preparation of an assessment framework for the services offered;
- organisation of an exercise with the participation of at least four MS testing the activation of an incident response retainer, as part of the next Cyber Europe.

Activity 5b has been updated to Activity 6 in the 2025–2027 single programming document (SPD).

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO3: Effective operational cooperation within the EU in case of massive (large-scale, cross-border) cyber incidents	Level of preparedness and response to large-scale cross-border incidents

(22) Target response to qualitative survey regarding ENISA's ability to support MS, with a scale of 1 to 5, with 5 being the highest rating.

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET
5b.A Enhanced preparedness and effective incident response	Article 7	2025	Ability of ENISA to support MS to further develop preparedness and response capabilities through implementation and delivery of ex ante and ex post services delivery	> 4 [22]

OUTPUTS	OUTCOME

5b.1 Pentest and threat hunting services towards selected entities within MS [23]	These outputs implement the cybersecurity support action programme, established by ENISA in 2023, which provides pentests, threat hunting, risk monitoring and assessment and customised exercises, and supports the MS with incident response.
	The following summarises the major deliverables of 2024.
	• Full participation of all 27 MS to the programme.
	• A total of 482 request of services consolidated, of which 157 were fully dealt with and closed during the year. The agency delivered the following services:
	  • 65 pentests / threat hunting;
	  • 9 new incident response retainers;
	  • 2 exercises;
	  • 32 training engagements;
	  • 6 other ad hoc services.
	• Methodology for incident response retainer conversion established and tested. Converted unused retainers from 2023, resulting in high use of the budget. The conversion was used to provide 20 pentests, 4 exercises, 2 threat landscapes, 6 customised training engagements and 11 ad hoc services.
	• Ten new people onboarded, thus gradually relieving service delivery from internal resources. This made the programme self-sustainable, with minimum impact on the delivery of the ENISA work programme.
	• SLA established with REA for the provision of central validation services for the purpose of the OCA to meet the requirements of Article 12(5) of the DEP.
	• New tender procedure concluded for 28 lots, to ensure contractors fulfil the DEP requirements.

5b.2 Customised exercises and training for selected entities within MS [24]	
5b.3 Risk monitoring and assessment for selected entities within MS [25]	
5b.4 Support incident response and incident management of selected entities within MS [26]	

[23] Beneficiaries of the Activity 5b services are specified in the [Contribution Agreement].

[24] Beneficiaries of the Activity 5b services are specified in the [Contribution Agreement].

[25] Beneficiaries of the Activity 5b services are specified in the [Contribution Agreement].

[26] Beneficiaries of the Activity 5b services are specified in the [Contribution Agreement].

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
5b.1	Pentest and threat hunting services are delivered promptly and accurately to MS	MS, Connect, beneficiaries	% of MS requesting the service Satisfaction score [27]	Annual	50 % > 4	81.5 % N/A see relevant footnote
5b.2	Customised exercises and training services are delivered promptly and accurately to MS	MS, Connect, beneficiaries	% of MS requesting the service Satisfaction score [28]		50 % > 4	44 % N/A see relevant footnote
5b.3	ENISA is able to provide regular risk monitoring towards specific targets or at the national level, including by leveraging commercial off-the-shelf platforms, and provide specific risk assessments and threat landscapes as requested by MS	MS, Connect, beneficiaries	% of MS requesting the service Satisfaction score [29]		50 % > 4	30 % N/A see relevant footnote
5b.4	ENISA provides 24/7 support for incident response to MS	MS, Connect, beneficiaries	% of MS requesting the service Support was provided promptly Satisfaction score [30]		50 % > 4	55.5 % N/A see relevant footnote

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	3.5 + 9 (see Annex VI)	Nº OF FTES ACTUALLY USED	5.12 [31]

* Please refer to Annex VI for financial figures.

[27] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.
[28] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.
[29] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.
[30] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.
[31] FTEs in SPD 2024–2026 is based on a target head count, of which 3.5 ENISA establishment posts and the remaining CAs were financed via a contribution agreement. The actual number of FTEs is higher due to the hiring procedures of new colleagues in 2024, whose work was partially covered through contribution from colleagues across the work programme activities.

ACTIVITY 6

Development and maintenance of the EU cybersecurity certification framework

Under activity 6, the agency seeks to establish and support the EU cybersecurity certification framework by preparing and reviewing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the EU rolling work programme. Measures also include maintaining and evaluating adopted cybersecurity certification schemes and participating in peer reviews. In addition, ENISA assists the Commission with regard to the European Cybersecurity Certification Group (ECCG), co-chairing and providing the secretariat for the Stakeholder Cybersecurity Certification Group (SCCG). ENISA also provides and maintains a dedicated European cybersecurity certification website, as set out in Article 50 of the CSA.

ENISA turned a corner with the key area of cybersecurity certification stipulated in Article 8 of the CSA. In 2024, the adoption of the implementing act on EUCC and the subsequent amendment gave new impetus to cybersecurity certification, which was characterised by unpredictable timeframes to adopt a scheme. Along the same lines, ENISA supported the Commission when digital sovereignty requirements were no longer necessary for the EUCS scheme, and proposed a new relevant version of the EUCS scheme. Furthermore, ENISA proposed an approach to certify eUICC under the EUCC scheme for EU5G (European Union certification scheme for 5G networks) equipment.

Looking ahead, as ENISA all but finalised its contribution to schemes in response to existing cybersecurity certification requests, the agency stands by to assist the Commission and the MS, to adopt these schemes as quickly as possible. The role of ENISA in the EUDI Wallet cannot be overstated, as it seeks to work with the MS and at the EU level to propose appropriate requirements and an EU scheme.

ENISA also looks forward to contributing to the area of MSS and on the certification of AI, with certification feasibility studies and draft candidate schemes if the Commission issues suitable requests.

In 2024, ENISA prominently extended its online services on certification, along the lines of a certification website and a readily available stakeholders' platform which complements the tangible contributions that ENISA is able to make to support the Commission, the MS and private industry alike.

Under this activity, the following was achieved in 2024:

- the adoption of the first implementing act and its subsequent amendment on cybersecurity certification by the MS, on a Commission proposal, was an achievement attributed to the support of ENISA;
- the launch of the ad hoc working group (AHWG) on the EUDI Wallet can be attributed

to preparatory work of ENISA and its swift response to establish the AHWG, thus paving the way to support the certification schemes across the MS, along with the EU certification scheme on the EUDI Wallets;

- the adoption of the amendment to the CSA, concerning MSS, was supported by a feasibility study on cybersecurity certification for MS, which was carried out swiftly with a view to engage the MS and selected service providers across the EU.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 6 moving forward.

- Cybersecurity certification continues to be challenged by unpredictable timeframes concerning the adoption of a scheme. In other words, while ENISA proved its ability to deliver a draft candidate scheme in a predictable, reasonably short timeframe, the adoption of an act takes much longer. It follows that mitigation measures would be necessary at the MS and industry levels for long engagements of resources.

- The Union rolling work programme and the annual Union work programme on European standardisation have yet to be suitably aligned to allow for standards that are relevant to certification to be prepared before a certification scheme is promulgated.

- Despite the sound efforts of the Commission and the MS and the support of ENISA, the draft candidate scheme on cloud services (EUCS) remains an open question; it is unlikely to be adopted anytime soon. A similar observation can be made for EU5G. ENISA stands by to adapt the content of both these schemes to the exact expectations of the Commission and the MS.

Activity 6 has been updated to Activity 7 in the 2025–2027 SPD.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO5 High level of trust in secure digital solutions	Citizens trust in ICT certified and non-certified solutions in the EU market

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET / RESULTS
6.A Improve the certification requirements concerning security posture management of certified products, services, processes and gradually of MSS	Article 8 and Title III	2025	Monitor ENISA take-up of technical standards and technical specifications in support of EU legislation (document monitoring)	Applicable standards cybersecurity requirements have been considered by ENISA to promulgate better cybersecurity certification schemes
6.B Efficient and effective implementation of the European cybersecurity certification framework	Article 8 and Title III	2025	N° of stakeholders (public and private) in the internal market implementing the cybersecurity certification framework for their digital solutions	A scheme is promptly implemented across all relevant market sectors
6.C Increase use and uptake of European cybersecurity certification	Article 8 and Title III	2024		High number of private and public entities and/ or market sectors relevant to a given scheme taking up certification after the entry into force of the implementing act
			N° of schemes and additional requests addressed to ENISA by the Commission	RESULTS 2024: 1 (EUDI Wallets)
			N° of schemes and additional requests processed by ENISA	RESULTS 2024: 1 (EUDI Wallets)
			Uptake of certified digital solutions (products, services, processes and gradually MSS) using certification schemes under the CSA framework, as well as other directly applicable instruments, i.e. CRA, EUDI Wallets etc.	RESULTS 2024: undetermined because the EUCC implementing act came into force in 2025
6.D Increase trust in ICT products, services and processes	Article 8 and Title III	2025	N° of certificates issued and published under an EU certification scheme; high utilisation rate in the market.	High degree of visibility and use of EU cybersecurity certificates

[32] CEN/TS 18026:2024, Three-level approach for a set of cybersecurity requirements for cloud services and CEN/CLC/TS 18072:2024, Requirements for conformity assessment bodies certifying cloud services.

OUTPUTS	OUTCOME
6.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes	**MSS** In 2024, ENISA engaged in the drafting of a feasibility study on the certification of MSS, providing both a contextual analysis and a proposed certification strategy. This study aimed to support the Commission to establish a scheme request to ENISA and the future AHWG to support ENISA and other stakeholders in initiating a robust, adaptative certification scheme for MSS; this study also presented recommendations regarding the scheme's purpose, scope, essential standards, assurance levels, reuse of existing schemes and approaches to evolving threats. **EUCS** While ENISA started the year supporting the Commission and the MS with the draft scheme that included digital sovereignty requirements, a change of course in the ECCG was noted in Q1. It follows that in May 2024 ENISA provided the ECCG with an update of the candidate scheme, paying utmost attention to ECCG guidance on the sensitive topic of digital sovereignty. While the ECCG is still expected to provide its opinion, ENISA further collaborated with the European Committee for Standardisation (CEN)–CENELEC towards the adoption of two technical specifications supporting the draft EUCS schemes, and developed the initial set of supporting guidelines [32]. At this stage, ENISA is standing by to deliver portions thereof or the entire scheme to the ECCG. **EUDI Wallet** ENISA supported the Commission and MS for the development and adoption of the implementing regulation. Specifically, ENISA assisted in defining rules for the national certification of the EUDI Wallets. ENISA also participated in the preparation of the Commission request for the development of an EU scheme, and selected the experts of the AHWG, on the basis of an open call for experts to the AHWG to support ENISA. The AHWG had its first meeting in January 2025, and is expected to develop an initial scheme within two years. In addition, ENISA has been working with selected MS to develop further national certification schemes on digital wallets. **EU5G** ENISA finalised one chapter of the scheme's request, related to the specification and certification of eUICCs, following a public consultation. Since eUICCs would be EUCC-certified, these elements were submitted to the EUCC scheme for consideration as possible guidelines. ENISA continued developing the EU NESAS candidate scheme by means of the following activities: the review of GSMA documentation, with comments passed back to GSMA for possible adaptation of their framework; and pilots on the possible improvement of the vulnerability assessment of NESAS products, combining Common Criteria and CVSS approaches. In Q1, ENISA engaged with the O-RAN Alliance and undertook the task to extend the EU5G scheme to include relevant cybersecurity requirements. ENISA continued engaging with the GSMa and 3GPP, particularly in view of its new role as Counsellor to the European Telecommunications Standards Institute (ETSI) under the Commission delegation, a role that was affirmed in 2024. At this stage, ENISA is standing by to deliver portions thereof or the entire scheme to the ECCG. **CSA evaluation** ENISA supported the MB and the Commission in the CSA evaluation, providing an assessment of well-functioning elements of the CSA and gaps related to the certification chapter. ENISA also identified possible improvements that could support a potential review of the CSA. **EUCC-CRA mapping** ENISA updated an internal 2023 report on the possible fulfilment of CRA essential requirements via EUCC certification, taking into consideration adopted versions of this regulation, as well as ECCG, SCCG and EC feedback. ENISA intends to publish the updated report in early 2025, to allow engaging pilots on its application that could bring about value for the preparation of future regulation establishing presumption of conformity to the CRA by means of cybersecurity certification under the Cybersecurity Act.

OUTPUTS	OUTCOME
6.1 Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes	**AI feasibility study** In 2024, ENISA concluded for all practical purposes the assessment of the feasibility of certifying AI through EU cybersecurity certification schemes, on the basis of Regulation (EU) 2019/881. This study seeks to support the operationalisation of the cybersecurity requirements set out in Regulation (EU) 2024/1689 (AI Act), as well as in other legal instruments, such as Regulation (EU) 2024/2847 (CRA). It proposes actionable conclusions, drawn from the analysis of six use cases.
6.2 Implementing and maintaining of the established schemes including evaluation of adopted schemes, participation in peer reviews etc. monitoring the dependencies and vulnerabilities of ICT products and services	**EUCC** On 31 January 2024, the EUCC scheme was adopted as European Commission Implementing Regulation (EU) 2024/482 and entered into force in February 2024, as far as the provisions related to the notification of Conformity Assessment Bodies is concerned. Based on ENISA recommendations, the organisation supporting the maintenance of the EUCC scheme was set up, leading to the first amendment of the scheme by means of Commission Implementing Regulation (EC) 2024/3144. Considering the significant efforts needed, ENISA received an additional Commission request to support maintenance, which was tested in 2024 with the development of new state-of-the art documents referred to in the amendment, and it will formally and comprehensively be put in place in 2025. ENISA also finalised, and received a positive opinion from the ECCG on, guidelines supporting the EUCC scheme related to vulnerability management and disclosure, and providing guidance for the holder of the EUCC certificate and the IT Security Evaluation Facilities on how to apply the rules of the Implementing Regulation. These ENISA guidelines are also addressed to certification bodies, national cybersecurity certification authorities and CSIRTs designated across the MS to coordinate for the purposes of the CVD process.
6.3 Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks	**Support to statutory bodies** ENISA supported the Commission in five ECCG meetings, presenting updates of ENISA's activities and actively contributing to the debates. ENISA also organised an NCCA training session, relying on selected NCCAs to share their experiences. This activity also contributes to the development of a peer-review strategy, for which a new ECCG sub-group was established with the support of ENISA. ENISA co-chaired with the Commission two meetings of the SCCG, to present, interact with stakeholders and gather feedback on preliminary ENISA work, particularly relating to aspects of EUCC, CRA, the cybersecurity market, etc. **ECCG sub-group on cryptography** In 2024, ENISA chaired the ECCG sub-group on cryptography. Subsequently, ENISA developed the first version of guidelines based on contributions previously produced by the SOG-IS cryptography WG. These guidelines, which supported the EUCC scheme, were primarily addressed to developers and evaluators, to provide recommendations for the preferred cryptographic mechanisms to be used in ICT products submitted to certification. The next steps were defined during the reporting year, with a view to drafting a new version to Post Quantum Cryptographic in 2025 and a supporting document to the related roadmap.
6.4 Developing and maintaining the necessary provisions and tools and services concerning the EU's cybersecurity certification framework (including certification website, support the Commission in relation to the core stakeholder service platform of the CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework, etc.)	**ENISA website dedicated to certification** ENISA populated the website with the adopted scheme and related supporting documents. ENISA also used the website to promote certification and its various reports related to certification. ENISA, with the support of MS, began developing new functionalities to support the publication of EU certificates and the maintenance of their status. Importantly, the technical capacity of the certification website was enhanced thanks to services directly acquired by the Commission / DG Digital Services, to ensure enhanced resilience and availability of service. **European Cybersecurity Certification Platform (CEF Platform project)** ENISA supported the development of the CEF Platform, a demanding Commission project with a range of challenges. A key difficulty was the lack of engagement with the cybersecurity community, attributed to the longer-than-planned preparation time. Additionally, the platform's functionalities – especially for discussions – were quite limited, further restricting user adoption and appeal. Furthermore, ENISA still expects the platform to be transferred to ENISA. The agency is therefore considering migration to a more durable Commission-provided platform.

OUTPUTS	OUTCOME
6.4 Developing and maintaining the necessary provisions and tools and services concerning the EU's cybersecurity certification framework (including certification website, support the Commission in relation to the core stakeholder service platform of the CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework, etc.)	**Certification uptake** ENISA participated in a European accreditation workshop along with the Commission to present the EUCC scheme and the new rules on the accreditation of EUCC CABs, in order to raise the awareness of the EU NABs. ENISA published the Cybersecurity assessments – Evaluations & certifications – State of play 2018–2022 report, presenting the current state of play of cybersecurity assessments of ICT products and cloud services. To study the dynamic of the related market, the report focuses on the evolution of the number of assessed ICT solutions. In April 2024, ENISA organised its annual Cybersecurity Certification Conference, gathering 200 participants onsite in Brussels and around 1 000 online. Furthermore, ENISA staff gave presentations in a broad range of national EU, and international conferences and events to promote EU certification and to engage with stakeholders with an increased interest in certification.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	75 %	72 %
6.1	• Scheme meets stakeholder requirements, notably of the MS and the Commission • Take-up of schemes by stakeholders	AHWG on certification ECCG Commission	Nº of opinions of stakeholders managed	Annual (report)	100 opinion items per scheme	27 MS and the Commission delivered through ECCG [33]
	• Timely delivery of all schemes requested in cooperation with the Commission • Statutory bodies and AHWG actively involved		Nº of people/organisations engaged in the preparation of certification schemes	Annual (report)	At least 20 AHWG members from third-party experts; at least 15 MS joining AHWG	EUCS scheme: 17 EU5G: 25 EUDI Wallet: 25 MS: 15

[33] Indicator to be reconsidered going forward.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
6.2	• Review of schemes to improve efficiency and effectiveness • Take-up of schemes by stakeholders	AHWG on certification ECCG Commission	ENISA response to consolidated monitoring and maintenance requirements of schemes adopted	Triennial (survey)	75 %	N/A
			Satisfaction of ENISA's role in NCCA peer reviews	Triennial (survey)	75 %	N/A
6.3		ECCG Commission SCCG	Feedback from statutory bodies including NCCAs on ENISA's role	Biennial (survey)	75 %	72 %
6.4	• Supporting in transparency and trust of ICT products, services and processes • Stakeholders engagement promotion of certification	ECCG Commission SCCG	Users satisfaction concerning the certification website services	Annual (survey)	75 %	N/A [34]
			Usage of certification website	Annual (report)	75 %	N/A [35]

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	9.5	Nº OF FTES ACTUALLY USED	8.18
PLANNED BUDGET (EUR) [36]	571 896.00	BUDGET CONSUMED (EUR) [37]	549 128.47
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	211 043.53

[34] Annual survey postponed in 2024

[35] Figures not available

[36] Direct costs only.

[37] Direct costs only.

ACTIVITY 7

Supporting the European cybersecurity market and industry

Under Activity 7, ENISA supports the development of the cybersecurity market for products and services in the EU and of the cybersecurity industry and services, in particular small and medium-sized enterprises (SMEs) and start-ups. The objective here is to reduce dependence on external markets, increase the capacity of the EU and reinforce supply chains for the benefit of the internal market.

In 2024, ENISA focused its attention on the composite policy area of Article 8 of the CSA, namely market and standardisation.

With the perspective of the adoption of CRA, ENISA processed specific requests of the Commission regarding products catalogues in relation to the cybersecurity market. Together with cybersecurity market analyses, such processes broaden the scope of the support of the agency to the Commission and the MS.

ENISA was admitted as a Counsellor to ETSI under the Commission delegation. This admission gives the agency a proactive role on standardisation. ENISA seeks to influence the standardisation agenda and to reach out further to relevant industry players, notably standard-developing organisations at large. Along the same lines, by adopting two European standards proposed by ENISA on EUCS, CEN–CENELEC affirmed the assertive role of ENISA in contributing to standards and technology across the EU. This is a significant step, considering how long it will take for the EUCS to be adopted. In the meantime, European standards cover a portion of the gap, which is of particular relevance, even in the absence of an adopted cybersecurity certification scheme on cloud services.

In terms of market and of the CRA, ENISA seeks to support market surveillance authorities and to thus support the Commission with the implementation of the CRA. Concurrently rolling out the market analysis methodology to support market sweeps provides a new opportunity. In order to remain instrumental to the success of the CRA, ENISA will explore new avenues to provide tailored support to the MS, in full coordination and at the service of the Commission.

Under this activity, the following was achieved in 2024:

- ENISA responded appropriately and promptly to the Commission requests concerning products catalogues under the CRA, providing substance to the high-level stipulations of the CRA itself;
- ENISA was finally admitted as Counsellor under the Commission delegation to the ETSI governing board, thus gaining access to WGs and consortia relevant to its certification work, namely EU5G, and enhancing its ability to communicate standardisation requirements on cybersecurity;

- concurrently with newly-established CRA-related work, ENISA supported its market outputs with a report on the market for MSS under the CSA amendment, thus further underpinning certification and providing rich contextual information to better understand cybersecurity market dynamics.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 7 moving forward.

- In 2024, two European standards proposed by ENISA on EUCS, i.e. TS 8026:2024 and 18072:2024, were adopted by CEN–CENELEC on a proposal previously introduced by ENISA and duly accepted by CEN–CENELEC. A coordination mechanism and set timeframe to promulgate standards or parts thereof to the benefit of cybersecurity policy, including certification, remains a challenge for ENISA, as an additional proposal remains work in progress.
- As the mandate of ENISA in the CRA vis-à-vis market surveillance authorities needs to be composed of diverse elements, ENISA needs to further explore the actions expected by MS and by the Commission to facilitate their role in the CRA. An approach towards market sweeps will therefore also be expected to follow a collaborative pattern, to bring together the requirements of the Commission and of the MS. On the positive side, the market analysis framework provides a solid basis to develop an approach concerning market sweeps.
- Conformity assessment requirements of the CRA and of the CSA certification remain aligned. ENISA can provide guidance and input to the legislative instruments as appropriate to ensure that deviations remain checked.

Activity 7 has been updated to Activity 8 in the 2025–2027 SPD.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO5 High level of trust in secure digital solutions	Monitor metrics such as the number of certificates issued under an EU scheme; the number of companies interested in EU certification; growth observed in the number of CABs or EU certification functions thereof recorded in the MS.

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET / RESULTS
7.A Foster a robust European cybersecurity industry and market	CSA Article 8 and Title III CRA proposal	2024	• Stakeholders' satisfaction with of the ENISA survey • State of the EU cybersecurity industry and market for products and services (index) • Industry perception of the internal market (survey)	Improved ability of ENISA and the EU to analyse the EU cybersecurity market RESULT: this indicator was finally not established in the cybersecurity index and therefore could not be reported RESULT: N/A [38]
7.B Improve the conditions for the functioning of the internal market	CSA Article 8 and Title III CRA proposal	2025	Better informed choices by users of products in market niches analysed	Improve the understanding of stakeholders on the cybersecurity market conditions in the EU

OUTPUTS	OUTCOME
7.1 Market analysis on the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes	In 2024 ENISA conducted a **market analysis on MSS.** This analysis focused on the demand and supply of such services. It served to identify market drivers, challenges and trends, and provided a range of observations from a cybersecurity market standpoint. In Q1, pursuant to a Commission request, ENISA started **preparing for the transition to the CRA** [39]. Preparations aimed at supporting the Commission in terms of products catalogues and requirements thereto. Specifically, the agency supported the Commission in the preparatory phase of the implementation of the CRA by compiling **a catalogue of important and critical products with digital elements.** This was an additional work item requested by the Commission, and was not foreseen in the ENISA SPD 2024. Deliverables carried out under Output 7.1 were tailored in a way that the CRA gradually became a core part of the ENISA work programme, supporting the Commission request on the CRA by reprioritising its planned deliverables for 2024 and inserting new ones. During the reporting period, ENISA – for the first time together with the ECCC – organised the **Cybersecurity Resilience and Market Conference** on 31 October 2024 in Bucharest, hosted by the Romanian National Cyber Security Directorate (DNSC). More than 1 000 representatives from public authorities across the MS joined this hybrid event, including market surveillance authorities under the CRA, industry associations, consumer protections organisations, EUIBAs, National Competence Centres (NCCs), vendors, manufacturers and services providers affected by the CRA. By bringing the different stakeholders together, the conference offered the ideal forum to discuss topics and priorities, such as the regulatory framework from the perspective of digital internal market and the cyber resilience of the Single Market in practice, and to build a **cybersecurity resilience and market community.** ENISA also started reviewing aspects pertinent to market surveillance authorities.

[38] The survey was not performed. However, industry stakeholder perceptions were collected from dedicated Commission stakeholder consultation calls.

[39] The CRA entered into force in December 2024.

OUTPUTS	OUTCOME
7.1 Market analysis on the main trends in the cybersecurity market on both the demand and supply side, and evaluation of certified products, services and processes	By exploiting synergies with the MS and EUIBAs, engaging external experts and tailoring goals according to the capacity available, the agency delivered the work under this output as foreseen in its work programme, and went a step further by conducting work relating to a Commission request in preparation for the CRA and to the CSOA. During the reporting period, ENISA also supported the Commission regarding technical matters in the realm of the **EU–US dialogue in the area of cybersecurity issues of open-source software.** Together with the Joint Research Centre (JRC), the Department of Homeland Security and CISA, various risk elements of this type of software were discussed,
7.2 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 2024 ENISA continued its participation in relevant standardisation activities and industrial bodies' initiatives, contributing to the assessment and limited influence of the current activities in the development of standards. ENISA contributed to such developments by assuring liaisons with the technical committees of a number of standardisation bodies (mainly European), in particular ETSI: TC CYBER (cybersecurity); TC ESI (electronic signatures and trust infrastructures); CEN–CENELEC JTC13 (cybersecurity and privacy); JTC21 (AI); CEN TC224 (personal identification and related personal devices with secure elements, systems, operations and privacy in a multi-sectorial environment): various WGs; CENELEC TC47X (semiconductor devices and trusted chips): hosting a meeting in Athens; and ISO/IEC JTC1 SC27 (Information security, cybersecurity and privacy protection). The agency also continued close collaboration (exchange/comments on documents of mutual interest and participation in events) with industry organisations, for example 3GPP, GSMA, GlobalPlatform and Eurosmart. ENISA also participated in the Global Government Expert Forum on SBOM (set up by CISA) and supported the task force on standardisation of the multi stakeholders platform (setting up the annual rolling work plan for standardisation), advising on cybersecurity issues. In 2024, ENISA achieved the status of ETSI Counsellor under the Commission delegation, giving it wider access to ETSI activities. The agency's presence in the advisory or strategy board of various European projects remained as before. An area of particular interest was the organisation and participation in standardisation-related conferences and events. Examples include the successful organisation of the ENISA-ESOs Cybersecurity Standardisation Conference (the largest cybersecurity standardisation event in Europe, gathering around 3 000 registrations each year), the support to the Programme Committee of the Trust Services and eID (electronic identification) Forum and other conferences, either in the Programme Committees (ETSI Security Conference, Trusted Economy Forum) or in providing speakers. The agency continues its work on CRA standardisation (participation in CEN–CENELEC JTC13/WG9 and an informal Commission–JRC–ENISA group), and prepared a deliverable on the overview and analysis of standards (existing / under elaboration / planned) related to the area of digital identities, which discussed requirements of the Electronic Identification and Trust Services Regulation (eIDAS2), analysed existing standards (including those suitable for certification of the EUDI Wallets) and identified existing gaps.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	60 %	67 %
7.1	Improved understanding of the market/ industry	AHWG on cybersecurity market analysis ECCG (as necessary) SCCG Advisory Group NLO (as necessary)	Cybersecurity market analysis; cybersecurity product and services analysis; analysis on vulnerabilities and dependencies in ICT products and services as appropriate; analysis of other relevant market areas	Annual (report)	All reports produced as planned	One report delivered on MSS [40]
7.2	Alignment with standards	SCCG Advisory Group NLO (as necessary)	Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification.	Annual (report)	All reports produced as planned	One report produced as planned [41]

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	7	N° OF FTES ACTUALLY USED	4.99
PLANNED BUDGET (EUR) [42]	266 666.00	BUDGET CONSUMED (EUR) [43]	239 830.74
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	99 672.82

[40] Pending publication of the 'MSS market analysis' report.

[41] Pending publication of the 'Digital Identity Standards – Analysis of current situation in standardisation related to the EU Digital Identity Framework Regulation' report.

[42] Direct costs only.

[43] Direct costs only.

ACTIVITY 8

Knowledge on emerging cybersecurity challenges and opportunities

Under Activity 8, ENISA provides strategic long-term analysis, guidance and advice on the cybersecurity threat landscape, emerging technologies and cybersecurity challenges, while assessing the level of cybersecurity maturity across the EU to identify opportunities and gaps. Activity 8 also provides topic-specific recommendations and general assessments on the impact of cybersecurity requirements and challenges, and contributes to the fulfilment of the strategic objectives of efficient and effective cybersecurity information and knowledge management for Europe, and foresight regarding emerging and future cybersecurity challenges. The activity seeks to achieve the strategic objectives by building on aggregating and analysing information across the ecosystem (legal, regulatory, technical, societal, etc.), and by leveraging expertise to provide relevant analyses. It relies on a series of empowered and engaged ENISA communities, particularly the NLO network, Advisory Group, dedicated AHWG (cyber threat landscapes, foresight) and NIS CG.

The activity collects, consolidates, analyses and provides recommendations and reports on information and knowledge across the cybersecurity ecosystem and ENISA SPD activities (e.g. incident reporting, situational awareness, NIS investments, threat landscapes, skills and education, market analyses, national cybersecurity strategies). One of the key related outputs (8.1) is on the EU-CSI, which aims at assessing the level of cybersecurity maturity across the EU via a series of qualitative and quantitative indicators, metrics for which are collected by MS and via external sources. In doing so, the EU-CSI work consolidates information from across all ENISA activities, while generating qualitative and quantitative results that yield significant information on both ENISA's and the EU's progress in raising the level of cybersecurity. The EU-CSI belongs to the five service packages identified by the MB as a strategic priority for the agency.

Moreover, the analyses and recommendations under Activity 8 feed into the work and prioritisation of topics of other activities, with a notable example being the threat landscapes, the findings of which guide the selection of topics for training and exercises (Activity 3), and feeds into the NIS strategy (Activity 2) with the provision of sectorial threat landscapes. In this respect, by consolidating information across ENISA's ecosystem of activities, analysing them and feeding back to the activities of ENISA, effective cybersecurity knowledge management takes place.

Under this activity, the following was achieved in 2024:

- a high level of satisfaction and acceptance from all relevant stakeholders:
    - **all 27 MS participated actively in the cybersecurity index,**

- **first 2024 report on the state of cybersecurity in the Union delivered to the Parliament in December 2024;**

- the **ENISA Threat Landscape 2024 report** attracted significant media attention and was the only ENISA source highlighted in the influential Draghi and Niinistö reports:

  - **ENISA is recognised as the source of truth for the cybersecurity threat landscape;**

- prepared **NIS2 transition and consolidation for incident reporting** by spearheading the adoption of relevant incident notification criteria, thresholds and templates, while implementing and maintaining relevant tooling;

- published the **Foresight Cybersecurity Threats for 2030 – Update report** and institutionalised strategic foresight for the early identification of emerging cybersecurity challenges.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 8 moving forward.

Promote the uptake of the recommendations in the 2024 report on the state of cybersecurity in the Union:

- 2025 action: work closely with MS to identify how the recommendations can be taken up in national cybersecurity strategies;

- 2025 action: revise and restructure cybersecurity index as per MB guidance and lessons learned from 2024.

Incident reporting harmonisation and simplification is a necessity:

- 2025 action: Align elements of incident reporting across different legislative streams in agreement with relevant stakeholders.

Conducting strategic cybersecurity foresight for the entire cybersecurity community and industry requires significant resources:

- 2025 action: Introduce strategic foresight in a horizontal manner for the agency and establish the grounds for a long-term and sustained technology and innovation radar.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO6. Foresight on emerging and future cybersecurity challenges SO7. Efficient and effective cybersecurity information and knowledge management for Europe	EU-level cybersecurity risk assessment and cyber threat landscape (adopted in accordance with Article 18(1)(a)

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET / RESULTS
8.A Knowledge and uptake of future challenges and opportunities by MS and EU stakeholders.	Article 9 CSA	2025	• Cybersecurity index indicator 'emerging technology threats are considered by national risk assessments' • Level of the acceptance of the report of the state of cybersecurity in the Union	Positive adoption by the Parliament High take-up of the report by MS and EU stakeholders All MS have considered at least 1/3 of the mapped emerging technology threats in assessing risk at the national level
8.B Increase understanding of the state of cybersecurity	Article 9 of the CSA and eIDAS Article 10	2025	Use of cybersecurity index by MS	All MS give input to the cybersecurity index 2/3 of MS are using the index to inform their national cybersecurity strategies
8.C Deliver relevant and timely information	Article 9 of the CSA	2024	• Usage of knowledge management portals, i.e. index, CIRAS, etc. • Value and usability of knowledge management portals	2/3 of targeted stakeholders use the portals regularly RESULTS 2024: all 27 MS 2/3 of stakeholders are satisfied with the portals RESULTS 2024: all 27 MS use and find value in the portals

OUTPUTS	OUTCOME
8.1 Develop and maintain the EU-CSI	The **EU-CSI** provides ENISA and MS with insights about the EU cybersecurity posture in general and on matters of particular relevance, such as the protection of critical infrastructures. ENISA released to the MS the results of the first fully-fledged EU-CSI, after two years of piloting. The EU-CSI continued to be a product built in collaboration with all MS. It aggregates into a coherent overview the knowledge produced by ENISA and the EU institutions, as well as information from the MS themselves. The data has been used as an evidence base, among other things, for the **2024 report on the state of cybersecurity in the Union** [44] and, in particular, for the identification of the priority areas described.

[44] https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

OUTPUTS	OUTCOME
8.1 Develop and maintain the EU-CSI	The EU-CSI is available only to MS. The output not only achieved its objectives in 2024, but went beyond by coordinating all ENISA efforts on delivering the first-of-its-kind NIS2 Article 18 report on the state of cybersecurity in the EU. The output underscores the impact of combining ENISA expertise with other sources, in particular in MS, to obtain actionable information to be used by policymakers. In 2024, the efforts and impact of Output 8.1, also taking into account the strategic importance of the NIS2 Article 18 report, make it necessary to consider this output as having a more horizontal and coordinating role in future ENISA work programmes. It should also beconsideredin tandemwith other activities targeted at MS and EU cybersecurity maturity,such as the work onnationalcybersecuritystrategies, and policy monitoring and analysis in general.
8.2 Collect and analyse information to report on the cyber threat landscapes	In 2024, ENISA continued its extensive efforts in collecting, analysing, and reporting on the evolving cyber threat landscape. The ***ENISA Threat Landscape 2024*** [45] report was published in September 2024, providing a comprehensive analysis of emerging threats, attack techniques and cybersecurity trends across various sectors. To further enrich this analysis, ENISA included dedicated sector-specific threat landscapes, including a specialised report on the finance sector (published in February 2025). This sectorial approach enhances the broader ENISA threat landscape, offering tailored insights that support and empower NISD sectorial communities while strengthening Europe's cybersecurity posture. Additionally, ENISA continued its collaboration with EEAS by further mapping the threat landscape of foreign information manipulation and interference. This work was included as a dedicated chapter in the *ENISA Threat Landscape 2024 report,* highlighting the growing concerns around misinformation campaigns and hybrid threats. Moreover, ENISA conducted a deep-dive analysis on vulnerabilities and their impact on the threat landscape in 2024, identifying systemic security weaknesses that can be exploited by adversaries. These findings were also integrated into ENISA Threat Landscape 2024, ensuring a more holistic view of cybersecurity challenges. Recognising the importance of CTI and the role of information-sharing in effective threat landscape mapping, ENISA actively engaged with the CTI community. A dedicated CTI conference was held in October 2024, gathering around 120 participants from the cybersecurity ecosystem. The event fostered collaboration, knowledge exchange and best practices in CTI, reinforcing the EU's capacity to anticipate and respond to cyber threats. The achievements of the *ENISA Threat Landscape 2024* report and the CTI engagements directly support ENISA's statutory task to perform long-term strategic analyses of cyber threats and incidents (Article 9(2) of the CSA). These efforts align with ENISA's strategic objective SO7, which focuses on efficient and effective cybersecurity information and knowledge management for Europe. The internal coordination activities, synergies with situational awareness efforts (Activity 5) and enhanced incident reporting processes (Output 8.3) demonstrate ENISA's commitment to delivering timely, accessible and service-oriented threat intelligence. This is a direction that should be further pursued in 2025, namely to address all situational awareness efforts in a cohesive manner. Overall, the output achieved all of its objectives in 2024. The impact of ENISA's work is further underscored by its recognition and integration into high-profile reports and policy frameworks. Notably, ENISA's threat landscape was referenced by major publications, including the Draghi report on competitiveness and the Niinistö report on strengthening Europe's civil and military preparedness and readiness, highlighting its credibility and strategic importance in shaping European cybersecurity policy. Moreover, key insights from ENISA's analysis were integrated into the *2024 report on the state of cybersecurity in the Union,* further embedding ENISA's findings into EU-wide cybersecurity directives and strategies.
8.3 Analyse and report on incidents as required by Article 5(6) of CSA as well as other sectorial legislations (e.g. DORA, eIDAS Article 10, etc.)	The output focused on delivering on strategic objectives of cybersecurity as an integral part of EU policies and efficient and effective cybersecurity information and knowledge management for the EU, by supporting MS incident reporting as required by Article 5(6) of the CSA and other sectorial legislations (e.g. DORA, eIDAS Article 10, etc.), and providing relevant summary reports.

[45] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

OUTPUTS	OUTCOME
8.3 Analyse and report on incidents as required by Article 5(6) of CSA as well as other sectorial legislations (e.g. DORA, eIDAS Article 10, etc.)	In 2024, three annual reports were produced – Telecom security incidents; Trust services security incidents [46] and NIS Directive incidents with a unified structure – in preparation for a single consolidated cybersecurity incident report, starting from 2025. Cooperation with NIS CG WS on incident reporting and the Ecasec and ECATS expert groups was done to engage MS for data structure and process. In addition, the agency cooperated with the ESAs (EBA, EIOPA and ESMA) for harmonisation of incident-reporting content and templates within the DORA framework. The CIRAS platform was available and used by MS for incident reporting, and preparatory work for NIS2 was started on the platform. The output achieved its objectives in 2024.
8.4 Foresight on emerging and future cybersecurity challenges and recommendations	In 2024, ENISA worked, in line with Article 9(1) of the CSA, to deliver foresight on emerging and future cybersecurity challenges and provide recommendations for identified challenges. With regard to foresight, with the participation of the ENISA Advisory Group and the ENISA AHWG on foresight, the agency conducted a foresight exercise on future scenarios concerning the implementation and uptake of the CRA. Given that the CRA entered into force in December 2024 and that a dedicated EC CRA expert group will be formed in 2025, the results of the exercise were not published and will be revisited as of 2025 with the participation of the wider CRA statutory community. In addition, the agency revisited and reassessed potential threats regarding the expected societal, legal, economic and regulatory impacts of technological innovations on cybersecurity, and resulted in an update of the top 10 cybersecurity threats for 2030. The relevant report [47] was published in March 2024. Moreover, in September 2024, the flagship conference Threathunt 2030 was organised, bringing together the cybersecurity communities to discuss future challenges and to collectively pave the way forward. This work fully delivers on ENISA's strategic objective SO6 on foresight regarding emerging and future cybersecurity challenges. Building on the results of ENISA's foresight efforts conducted in 2023, in 2024 recommendations and targeted analyses on two identified challenges were conducted, namely on generative AI and on mapping the space threat landscape. Two dedicated reports were produced and validated by relevant communities and ENISA advisory group and NLO network, with their publication pending for 2025. The significance and added value of this output in enhancing preparedness for emerging challenges and conducting foresight allows the definition of early mitigation strategies to improve the EU's resilience. Given the vast field of emerging challenges, it is essential for ENISA to have a mechanism in place to prioritise areas where dedicated studies will be conducted. Accordingly, in order to identify the topics for targeted recommendations and analyses, the agency has put forward a methodology to incorporate and take up the results of the regular foresight exercises, also involving the ENISA Advisory Group and NLO network. This methodology was first applied during 2023 to feed into the 2024 SPD, and aims at enhancing the scope and focus of the output to better contribute and bring added value to obtaining strategic objective SO6. In addition, it is assessed in terms of performance by means of a dedicated KPI, namely 8.4, to measure the number of topics identified by foresight and subsequently analysed in the scope of Output 8.4 efforts. Two such topics were covered in 2024, in particular AI cybersecurity and space cybersecurity. Whereas the value of the output in contributing to ENISA's mandate and strategic objectives is undeniable, the results of this work are of a horizontal nature and should not be limited to just feeding into targeted recommendations. Strategic foresight is also a powerful and useful tool for other directions, such as policy development and, accordingly, a more cross-cutting approach for the delivery of the work under Output 8.4 should be considered in the future. A sustained technology and innovation radar, building on strategic foresight, would allow to repeat comparable and less resource-consuming achievements of relevant KPIs.

[46] https://www.enisa.europa.eu/publications/annual-report-trust-services-security-incidents-2023.

[47] https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	> 5 % compared with 2023	98 %
8.1	• Measuring maturity • Stakeholders can better prepare for future challenges based on indication of maturity	NISD CG, NLO, CSIRTs network	Uptake of the cybersecurity index	Biennial (survey)	20 MS representatives 60 % satisfaction rate Agreement by all validating bodies	27 MS were represented in the 2024 EU-CSI 88% All validating bodies (NIS CG, COM) agreement on NIS2 Article 18 report
8.2	Mapping threats generate recommendations for stakeholders to take up	NLO, AG and cybersecurity threat landscape AHWG CSIRTs network	N° of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	± 5 % compared with 2023	1 012 challenges, recommendations and security controls identified (ENISA Threat Landscape 2024)
			Uptake of reports generated in Activity 8	Annual (report)	± 5 % compared with 2023	88%
8.3	Analysing incidents Generate recommendations for stakeholders to take up	WS3 of the NISD CG, Ecasec and eIDAS Article 19 groups	EU incident reporting maturity	Annual (report)	EU Average > 50 %	'Incident reporting implementation' indicator: 60.43 % 'Establishment of a national reporting scheme for major cyber incidents' indicator: 69.27 %
			N° of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	± 5 % compared with 2023	NIS (17) eIDAS (7) European Electronic Communications Code (9 – to be published in 2025)
			Uptake of reports generated in Activity 8	Annual (report)	± 5 % compared with 2023	88 %

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
8.4	Identifying future challenges and opportunities Generate recommendations for stakeholders to take up	Foresight AHWG, NLO and AG	Nº of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	± 5 % compared with 2023	62 for the 'Generative AI' report (to be published in 2025) 10 for the updated 'Foresight 2030 Threats' report 471 for space threat landscape (to be published in 2025)
			The influence of foresight on the development of ENISA's work programme	Biennial (ENISA SPD)	> 2 emerging areas identified	10 areas identified
			Uptake of reports generated in Activity 8	Annual (report)	± 5 % compared with 2023	88 %

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	7.5	Nº OF FTES ACTUALLY USED	7.48
PLANNED BUDGET (EUR) [48]	711 646.00	BUDGET CONSUMED (EUR) [49]	740 754.56
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	74 836.01

[48] Direct costs only.

[49] Direct costs only.

ACTIVITY 9

Outreach and education

Under Activity 9, ENISA aimed to raise the overall awareness of cybersecurity risks and practices in cooperation with MS and EU entities and to foster engaged communities within and outside of the EU. This was achieved through awareness campaigns, educational initiatives and workforce development programmes, including upskilling and reskilling efforts. Moreover, Activity 9 seeks to contribute to the EU's efforts to cooperate with non-EU countries and international organisations on cybersecurity via the implementation of the international strategy.

Under this activity, the following was achieved in 2024.

- ECSF became the reference framework at the national, European and international levels: the ECSF has been endorsed or adopted as is by 14 MS and more than 500 European companies use it for recruitment purposes; it is mapped against the ESCO framework, giving a definition to the cybersecurity professional; and it is mapped against international frameworks (including NICE) under the activities of the International Coalition for Cybersecurity Skills. Thus, the success of the ECSF supported the objective of increasing the supply of skilled professionals to meet market demand.
- AR-in-a-Box was successfully piloted as a service for the first time. The service package was offered as a pilot in two countries (Cyprus and Romania). Six entities from different NIS2 sectors – namely digital infrastructure, transport, health, energy and public administration – participated in the development of a customised cyber awareness programme, with ENISA's support. The total reach was estimated at approximately 5 000 professionals and the majority of the entities running the programmes were able to increase their budgets. Thus, the AR-in-a-Box objective successfully helped to increase awareness of cybersecurity risks and improved cyber-secure behaviour across the EU.
- Through its international strategy, the agency has continued to support the EU external actions and to increase outreach. The agency has operationalised the working arrangements with Ukraine (SSSCIP/HCSCC) and the United States (CISA) through the establishment of a work plan, including actions to be carried forward. ENISA also continues to support the EU in its external dialogues, notably with Japan, Ukraine, the United Kingdom and the United States, and has established a services catalogue to contribute to the growth action towards neighbouring regions such as the Western Balkans. Thus, the success of these actions has supported the objective of fostering EU cybersecurity values and priorities.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 9 moving forward.

- The Cybersecurity Skills Academy communication required resource recalibration because of the number of tasks and their political importance, which was not initially planned. High-priority tasks, such as the creation of the cybersecurity workforce indicators, support to MS to collect and share data and the piloting of the attestation schemes for skills, in particular with regards to the CSA-related profiles, are still ongoing in 2025 and require resources.
- Scaling of AR-in-a-Box: apart from the addition of raising awareness under the support action catalogue, the concept of 'train-the-trainer' and the ambassadors' programme could be further enhanced to achieve greater scalability.
- ECSF to be integrated in all the capacity-building activities delivered by the agency or by other offerings. This will enable actual monitoring of the skills gaps and needs in the European public and private sectors.
- Increased interest from the international community to interact with ENISA points to the necessity of further enhancing and prioritising efforts in accordance with the agency's international strategy.
- The increased level of threats and geopolitical tension calls for a higher engagement of the EU within the international arena. ENISA's international strategy has contributed, albeit with limited resources, to these actions. It is clear and, as mentioned in the Council conclusions on ENISA and Western Balkan declaration, there is a need for further support via established working arrangement and cooperation, including for neighbouring regions. Although further steps have been introduced (e.g. the consolidation of a service catalogue), with the current resources allocated, the agency would not be able to make a significant impact in supporting the EU. An alternative mechanism for resources could be foreseen to increase the efficacy and impact of ENISA's international strategy. Additionally, an update to the international strategy should be foreseen to take into account the new global challenges.

Activity 9 actions have been merged with those of Activity 3 (awareness raising) and Activity 4 (international) in the 2025–2027 SPD.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO1. Empowered and engaged communities across the ecosystem	The % gap between demand and supply of cybersecurity skilled professionals
SO4. Cutting edge competences and capabilities in cybersecurity across the EU	General level of cyber-security awareness and cyber hygiene among citizens and entities

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET / RESULTS
9.A Increase awareness of cybersecurity risks and improve cyber-secure behaviour	Article 10	2025	• Cybersecurity indicator 'Enterprises: staff awareness' • Cybersecurity indicator 'SME culture of cybersecurity' • Nº of cybersecurity incidents with human error as a root cause • Cybersecurity index indicator 'National culture of cybersecurity'	1–2 % increase of cybersecurity indicator 'SME culture of cybersecurity' year-on-year Number of cybersecurity incidents in critical sectors with human error as root cause decreases year-on-year in relative percentages 1–2 % increase of cybersecurity index 'National culture of cybersecurity'
9.B Increase the supply of skilled professionals to meet market demand	Articles 10 and 6 EU priority on skills shortage Commission communication on the Cybersecurity Skills Academy	2025	• Increase in cybersecurity indicator 'Cybersecurity graduates in higher education' • Number of professionals trained at the Cybersecurity Skills Academy	'Cybersecurity graduates in higher education' At least 200 000 professionals trained by 2025
9.C Foster EU cybersecurity values and priorities	Article 42 of the CSA	2024	• Ability to support the EU's external objectives • Coherence of ENISA's international engagement with the agency's strategy	TARGET: ENISA is seen as key contributor to foster EU cybersecurity values and priorities were engaged RESULTS: alignment was made in consultation with EEAS and COM TARGET: ENISA activities are judged as aligned with its international strategy RESULTS: engagement during 2024 was formally approved/declined according to the ENISA international strategy and the international engagement output was approved for closure at the MT meeting in Q1 2025

OUTPUTS	OUTCOME
9.1 Develop activities to enhance behavioural change by essential entities [50]	AR-in-a-Box: increasing reach-out and promoting the service model: • publication of a C-level guide on building awareness for C-level executives, • SME version of AR-in-a-Box (lighter version for awareness programmes with few resources), https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box, • deployment of the AR-in-a-Box course in the EU Academy platform maintained by JRC (and train the trainer courses), https://academy.europa.eu/courses/ar-in-a-box-game, • running the ambassadors' programme to further promote AR-in-a-Box (non-ENISA experts were presenting the topic increasing reach out), • AR-in-a-Box+ service piloted in Cyprus and Romania, developing and monitoring the execution of awareness programmes for six operators of critical infrastructures; Online campaign and material for NIS2: • awareness material (infographics, social media cards, videos, booklet) for the NIS2 https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2, • dissemination and use by NIS CG MS.
9.2 Promote cybersecurity topics and good practices [51]	• Promoted tools and ENISA material through several channels • Co-organised events for SMEs with NCCs (Estonia, Cyprus, Latvia, Lithuania, Portugal, Slovenia) • European Cybersecurity Month (ECSM) fade out – ECSM awards, community handover • 1st Cybersecurity Awareness Conference
9.3 Implement ENISA international strategy and outreach	ENISA has been recording all incoming and outgoing international cooperation requests and activities since 2022. The International Cooperation Engagement Registry provides statistics showcasing the agency's actions to facilitate international engagements in assisting and developing outreach approaches in 2024, but also how these have developed since the registry was launched in 2022. This is how ENISA identified new cooperation opportunities. The processes also allow ENISA to improve the visibility of its work and efforts of the respective units and teams involved in international cooperation. The high level of general interest in ENISA's international engagement has led to significant progress in key areas. Regular updates and discussions took place at both the Executive Board and MB levels and ENISA also worked very closely with both the Commission and EEAS. Regular updates and discussions also took place at the level of the HWPCI. In 2024, ENISA accomplished the items shown below. • Completed well over half of the actions agreed upon in both WGs – and in some cases went beyond this – for both Ukraine and the United States. Working arrangements with Ukraine (SSSCIP/HCSCC) and the United States (CISA) have been in place since Q4 2023 and work plans which operationalise the arrangements have been established since the first half of 2024. These cover the cooperation areas of building capacity/awareness, exchanging best practices and sharing information.

[50] Defined by NIS2.

[51] Including based on stakeholder strategy.

OUTPUTS	OUTCOME
9.3 Implement ENISA international strategy and outreach	• Coordinated the agency activities within the context of the EU–US dialogue work streams, in cooperation with involved units and teams. • Supported EEAS and the Commission in the context of the EU external dialogues, such as with Japan, Ukraine, the United Kingdom and the United States. • Nurtured the relationship with key EU stakeholders such as EEAS, Connect and DG Enlargement and Eastern Neighbourhood. This has enabled the agency to appropriately implement its international strategy and to be considered a strategic partner for external actions on behalf of the EU. • Set the foundation to further support the EU action within the Western Balkans by consolidating a service-offering catalogue. • Specifically, ENISA's international cooperation handled 146 requests: 13 for outreach engagements, 18 for assisting engagements and 115 for limited engagements. This is a slight increase on 2023. • Declined a total of 41 requests, i.e. 27.9 % of the total (compared with 26 or 18.4 % in 2023 and only 8 or 7.8 % in 2022). This was justified because they were found to be outside of the priorities set in the strategy, showing commitment from the agency to adhere to its international strategy. • Earmarked 41 of its 93 approved limited and assisting engagements as support of an outreach activity. This is an increase on 2023, showing how the agency gives priority to high-value engagements.
9.4 Support the implementation and uptake of EU cybersecurity skills framework	Minimise the cybersecurity skills gap through a common language: • ECSF review process through public consultation and analysis of the findings; • facilitate essential/important entities to create a strategic workforce plan, in order to be aligned with NIS2; • mapping with the EU framework (i.e. DG Employment, Social Affairs and Inclusion's ESCO) and with international initiatives (under the International Coalition for Cybersecurity Skills and the World Economic Forum initiative). • Implementation of the Cybersecurity Skills Academy communication tasks: • leading the process for the attestation of skills; • validating skills indicators with MS (NIS CG); • providing feedback on the technical specifications for the repositories of certifications and the repositories of trainings under the digital jobs and skills platform. • Support close coordination between main stakeholders in order to bridge the skills gaps: • CyberHEAD maintenance and enhancement of programmes with information related to the ECSF profiles; • promotion and dissemination of ECSF through the annual conference and ambassadors – 3rd Cybersecurity Skills Conference; • NCC WG5 on skills alignment of activities.
9.5 Implement the Cybersecurity in Education roadmap	Publication of the education platform – 25 MS provided information and feedback that resulted in 101 learning materials, including 5 EU-wide initiatives from the Commission, the European Cyber Security Organisation and the European Schoolnet that were introduced in the platform: https://tools.enisa.europa.eu/topics/education/cyberedu#/. Numerous events to promote education and validate the platform information

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	> 1 % increase (from previous year – decrease in duplication)	87 %
9.1	• Targeted awareness campaigns to improve behaviour • Take-up of best practices by stakeholders	Awareness raising AHWG, NISD WS	Nº of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics			
			Total social media impressions	Annual (report)	> 5 % increase	464 900
			Total social media engagement			506 000
			Total video views			n/a
			Total website visits			9 967
			Total participation at events			16 events (total of ~ 800–1 000 participants)
			Nº of download of materials and overall use of AR tools (i.e. AR-in-a-Box and SME tool)	Annual (ENISA website)	> 4 000 per semester	SME Maturity Tool: 1 610 visitors, 10 745 pageviews AR-in-a-Box: 2 725 visitors, 68 694 pageviews, 4 352 downloads
9.2	Recognise threats and risks and how to act cyber secure	AR AHWG, ECSM coordinators group	Nº of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics	Annual (report)	> 5 % increase	C-Days Portugal (~ 70 people) Cyber 4.0 Conference (~ 500 people) NCC Cyprus (~ 70 people) 1st Awareness Conference (~ 250 people) Cyber Bazaar – NCCs LT, EE, LV (~ 250 people)
9.3	EU values recognised by international stakeholders International cooperation support ENISA objectives	MT, EEAS, COM and MB (as required)	Staff satisfaction with international coordination	Annual (survey)	> 80 %	N/A [52]
			Nº of international engagements	Annual (report)		156 engagement requests, 112 engagements approved, 44 declined

[52] The internal survey was postponed. However, the work undertaken within the output was endorsed by the management team during the closure of the project for the year.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
9.4	Promoting cybersecurity skills courses Greater N° of participants in cybersecurity courses	AHWG on Cybersecurity Skills, ECCC WG on Skills	Total N° of students enrolled in the first year of the academic programmes	Annual (cyberhead platform)	1–2 % increase	9765
			Student gender distribution (% female: % male)			79% male / 21% female
			Total N° of cybersecurity programmes			162
			N° of master's degree programmes			37
			N° of bachelor's degree programmes			125
			N° of entities included in ECSF registry (i.e. number of MS adopting ECSF, number of ECSF implementations/ pledges)	Annual (register of activities)	30 % of MS to adopt ECSF, At least 15 organisations to have endorsed ECSF	14 MS adopted or endorsed ECSF at the national level
9.5	• Influence education to include cybersecurity • Greater awareness and interest in cybersecurity as a career path	AR AHWG				

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	9.1	N° OF FTES ACTUALLY USED	8.18
PLANNED BUDGET (EUR) [53]	409 315.00	BUDGET CONSUMED (EUR) [54]	387 712.23
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	52 532.49

[53] Direct costs only.

[54] Direct costs only.

ACTIVITY 10

Advise on R & I need and priorities

Under Activity 10, ENISA provides advice on research and innovation (R & I) needs and priorities to MS and EUIBAs. To achieve this goal, ENISA follows a two-pronged approach. First, the agency takes stock of past and ongoing research, activities in development and technology assessment, and second, ENISA scans the horizon for emerging and future technological, societal and economic trends that may have an impact on cybersecurity. The findings of both strands of work contributes to the EU's strategic R & I agenda, by means of the alignment and collaboration with the ECCC and Network of National Coordination Centres (NCCs), as well as with the wider R & I community (given the limited resources in 2024, the academic R & I community was not targeted in depth and priority was given to ECCC/NCCs).

The actions taken here are in line with the strategic objective on foresight regarding emerging and future cybersecurity challenges. Indeed, the activity relies on the regular consultations with ECCC, NCCs, NLOs and relevant user groups, projects (including EU funded projects), researchers, universities, institutes, industries, start-ups and digital innovation hubs. The objective of such consultations is to consolidate information and identify gaps, challenges and opportunities in R & I from the different quadrants of the community. In this way, the agency delivers on its mandate as per Article 11 of the CSA.

The focus and objectives of the activity are to:

1. identify R & I trends and gaps by introducing assessment frameworks at the MS and EU levels;

2. introduce and promote the uptake of the NCC impact assessment toolbox;

3. capitalise on ENISA activities as part of its ECCC statutory tasks by building ENISA's status as a trusted ECCC partner, bringing knowledge from different communities (e.g. academia v industry), and via foresight on 2035 disruptive technologies as input to R & I proposals.

Under this activity, the following was achieved in 2024:

- **a high level** of satisfaction from ECCC, NCCs and the
- interest from **NCCs on the R & I assessment framework,**
- introduction of the **NCC Impact Assessment Toolbox;**
- **ENISA's input to the DEP 2025–2027 WP** considered by ECCC (including the Governing Board), and the relationship between ENISA and ECCC is becoming more structured:

- **ENISA recognised as a trusted ECCC partner.**

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 10 moving forward.

R & I foresight requires a lot of time (typically at least one year) and community engagement:

- 2025 action: focus on evidence-based input to R & I priorities by means of the R & I assessment framework developed in 2024;
- 2025 action: need to maintain a sustained technology and innovation radar, and thus limit individualised, one-off foresight exercises.

ENISA's advice is highly valued and appreciated by ECCC (including the Governing Board) and NCCs:

- 2025 action: strengthen relationships with ECCC/NCCs and prioritise them as stakeholders.

Identifying and analysing R & I from the wide cybersecurity community and industry requires significant resources:

- 2025 action: focus on key stakeholders and opt for synergies with NCCs – R & I cannot be seen separately from the wider cybersecurity market ecosystem;
- 2025 action: capitalise on ongoing ENISA actions, such as the Article 18 report.

Activity 10 actions were merged with Activity 8 in the 2025–2027 SPD.

LINK TO STRATEGIC OBJECTIVES (ENISA STRATEGY)	INDICATOR FOR STRATEGIC OBJECTIVES
SO6. Foresight on emerging and future cybersecurity challenges	Overall EU investment in R & I activities addressing emerging cybersecurity challenges

GENERAL ACTIVITY OBJECTIVES	CSA ARTICLE AND OTHER EU POLICY PRIORITIES	TIMEFRAME OF OBJECTIVE	INDICATOR	TARGET / RESULTS
10.A EU R & I funding programmes address emerging cybersecurity challenges identified by ENISA	Article 11, EU Research Agenda	2024	Assessment of ENISA contribution to EU R & I funding and work programmes	TARGET: 50 % [55] RESULT: 59 %
10.B EU R & I funding programmes focus on the development of solutions made in the EU	Article 11, EU Research Agenda	2025	Assessment of EU-funded projects transitioning from research to deployment of new cybersecurity solutions	TARGET: 10
10.C EU cybersecurity R & I community generates knowledge on emerging cybersecurity challenges identified by ENISA	Article 11	2024	Number of research articles and papers generated by the community reviewing emerging cybersecurity challenges identified by ENISA	TARGET: 10 RESULTS: undetermined

OUTPUTS	OUTCOME
10.1 Collect and analyse information on new and emerging information and communications technologies in order to identify gaps, trends, opportunities and threats (R & I observatory).	In 2024, ENISA concluded a foresight exercise initially started in 2023, focusing on disruptive technologies and covering a timeframe of 10 years. A total of 20 general trends were identified. Given the lengthy process in conducting foresight exercises, but also the need to provide evidence-based guidance on new and emerging technologies to identify gaps, trends and opportunities, ENISA initiated a more systematic and structured fremwork for the collection and analysis of information. Accordingly, an assessment framework for R & I at the EU and MS levels was developed, introducing 11 strategic objectives across four quadrants (market fit, R & I performance, operational excellence, talent development). Defined to guide the design of the framework, these four quadrants aim to assess, on one hand, the gaps and opportunities for R & I in the EU, and on the other hand, the impact of different initiatives on R & I as the collection and analysis of the framework indicators' data was analysed during the years. In this respect, 12 qualitative and quantitative indicators to measure R & I performance and impact were identified. The aim of the framework to be piloted in 2025 is to support ENISA's mandate. This means that it will provide evidence-based information on funding gaps and opportunities in R & I to support ECCC WP and relevant activities, to help prioritise relevant ENISA actions, and to serve as input for the strengthening of the ENISA index and feed into the prospective NIS2 Article 18 reports.

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

OUTPUTS	OUTCOME
10.2 Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment.	In 2024, ENISA continued to collaborate closely with the ECCC and the network of NCCs, both on the basis of statutory tasks but also on the MOU signed with the ECCC in 2023. Further to acting as co-chair of ECCC governing board WGs (particularly on strategic agenda, community building and cybersecurity skills), ENISA also focused on providing advice on R & I priorities for funding. A total of 10 of the 17 proposals in the draft DEP WP 2025–2027 stem from ENISA input. The advice on R & I priorities for funding is based on findings from existing ENISA activities and outputs, such as the cybersecurity index, foresight and the NIS2 Article 18 report. ENISA also took the initiative to develop an impact assessment toolbox. The toolbox aimed to empower NCCs to develop their own impact assessment methodology, identify their goals and start measuring the outcomes of their efforts. Lastly, ENISA followed up on the SLA that was set up with the ECCC concerning the offer of support on accounting and Data Protection Officer services.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
All			Stakeholder satisfaction	Biennial (survey)	> 90 %	91 %
10.1	Identifying current and emerging R & I needs and funding priorities	Academia, industry and national R & I entities (including NCCs) and EUIBAs	Evaluation of the trends, wild cards and weak signals on emerging cybersecurity challenges leading to R & I needs and priorities	Annual (annual work programme)	3	20 trends identified in the ENISA foresight study
10.2	Advising EU funding programmes including the ECCC	Commission, including Connect and JRC, ECCC and NCCs	N° of contributions to EU funding programmes	Annual (reports)	5	10/17 ENISA proposals in the DEP 2025–2027 WP

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	3.75	N° OF FTES ACTUALLY USED	2.24
PLANNED BUDGET (EUR) [56]	126 000.00	BUDGET CONSUMED (EUR) [57]	113 400.01
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	1 043.30

[56] Direct costs only.

[57] Direct costs only.

ACTIVITY 11

Performance and sustainability

Under Activity 11, ENISA seeks to improve organisational performance, risk management and compliance with ENISA's legal and regulatory framework.

The work undertaken within the activity is 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, the activity includes a contribution to efficiency gains, for example via shared services in the EU Agencies Network (EUAN) and in key areas of the agency's expertise. As part of this activity, ENISA seeks to achieve key objectives of the agency's corporate strategy (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 ensures that the agency adheres to sound financial management. In the area of IT systems and services, the IT Management Committee oversees and monitors the comprehensive application of the agency's IT strategy and relevant policies.

Under this activity, the following was achieved in 2024.

- Preparing ENISA to meet the obligations of Regulation (EU, Euratom) 2023/2841 on a high common level of cybersecurity in the EUIBAs, including by conducting risk assessments and a horizontal cybersecurity audit that will form the basis for the agency's long-term cybersecurity strategy and planning.
- Contributing to the EUAN effort for the provision of shared services via a number of initiatives, including collaboration with CERT-EU on a shared service offering on risk assessment, and ENISA's participation in the EU agency troika shared-services pilot with the provision of cybersecurity support.
- Designing the transition to the agency's new IT governance model (corporate and operational IT) and paving the way towards environmental compliance.

These highlights reflect ENISA's culture, which is focused on performance management through practicable steps, with the goal of protecting the agency's assets and reputation while reducing risks.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 11 moving forward.

- Further enhance data collection and analysis of stakeholders' opinions, to simplify internal processes and address emerging priorities, such as the development of an AI framework to meet the agency's future operational and corporate needs.

- In 2024, the activity had a new set of KPIs introduced in the 2024 SPD. The results show that this recalibration of work, combined with an increase in the number of FTEs allocated, also including external support, rebalanced the workload within the unit and drove the activity towards the priorities of ENISA's corporate strategy.

- Objectives and KPIs were generally met in 2024 and additional activities (not planned initially) were carried out with the budgetary support of internal transfers. The end of the year budget process allowed surplus funds to be channelled to website maintenance and support, and the strengthening of administrative support for the units. To achieve this, there was a need to carry forward certain budget amounts to 2025.

ANNUAL

GENERAL ACTIVITY OBJECTIVES	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	TARGET	RESULTS 2024
11.A Maintain corporate performance and coordinate strategic planning	Ensure efficient corporate services	Proportion of SPD KPIs meeting targets	Annual	> 80 of indicators	73% [58]
	Continuous innovation and service excellence	Results of Internal control framework assessment	Annual	Effective (Level 1/2)	Effective (Level 2)
	Developing service propositions with additional external resourcing	High satis-faction with essential corporate services in the area of compliance and coordi-nation	Annual	> 60 %	75 %
11.B Increase corporate sustainability	Ensure a climate-neutral ENISA by 2030	EU Eco-man-agement and Audit Scheme (EMAS) es-tablished	Annual	Adopted by end 2024	EMAS audit conducted on 27/2/25
	Develop efficient framework for ENISA continuous governance to safeguard high level of IT security	Agency IT strategy aligned with corporate strategy Proportion of total IT budget allocated to information security pro-portional to the level of risks across various IT systems within the agency	Annual	Revised IT strategy by 2024 20 % by 2024	Revised IT strategy proposal submitted end 2024; strategy to be adopted by Q2 2025 18 % of total IT costs

[58] Of the 149 indicators 37 met and 72 outperformed the target set, whilst 23 underperformed, 10 where postponed and 5 found not applicable

OUTPUTS	OUTCOME
11.1 Coordinate the implementation of the agency's performance management framework, including agency-wide budget management and IT management processes, environmental management and regulatory compliance	Coordination of the SPD and AAR process, including internal assessment and calibration of processes to increase efficiency and effectiveness. Internal controls assessment, management of ECA and Internal Audit Service (IAS) audit recommendations, risk assessment and consolidated reporting to the agency's management. Legal coordination and support across the agency, including management of Court cases and requests from supervisory authorities; data protection advice and support. IT management across the agency and implementation of the new IT governance scheme, including a proposal for a revised IT strategy (ITMC). Budget management across the agency, including a methodology for the categorisation and prioritisation of costs (BMC). Environmental management across the agency in cooperation with Corporate Support Services (CSS) (Activity 13), including preparation for the agency's first EMAS audit (conducted in February 2025).
11.2 Maintain and enhance ENISA's cybersecurity posture	Day-to-day support on cybersecurity across the agency, including log monitoring, pentest organisation, incident management, technical advice and coordination with IT units. Preparation of the agency to meet the obligations of Regulation (EU, Euratom) 2023/2841 on a high common level of cybersecurity in EUIBAs (risk assessment, red teaming exercise, phishing exercise, horizontal cybersecurity audit). Internal cybersecurity awareness-raising sessions (with the use of a specific training platform).
11.3 Provide support services in the EUAN and in key areas of the agency's expertise	DPO and accounting services provided to ECCC (under specific SLA). Legal support services on host country matters provided to the European Centre for the Development of Vocational Training (Cedefop) under a specific SLA. Cooperation with CERT-EU and definition of a shared-service offering on risk assessment (pilot kicked off in December 2024). Support in the EU agency troika shared-services pilot with the provision of cybersecurity support (as of November 2024).
11.4 Ensure the implementation of single administration processes across the agency	Continuous administrative support offered to all units and teams in Athens and Brussels.

OUTPUTS	HOW OUTPUT EXPECTED TO CONTRIBUTE TO ACTIVITY OBJECTIVE FOR THE YEAR	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
11.1	• Unified day-to-day practices across the agency upon implementing SPD • Annual risk assessment and internal controls assessment performed and reported • Legal and regulatory compliance are monitored; issues and areas of improvement identified • Streamlined IT system management across the agency and in accordance with ENISA's IT strategy; reports from ITMC • Streamlined budget management across the agency; reports from BMC • A plan to reduce carbon dioxide emissions at ENISA's HQ	MT & relevant committees External and internal audits Statutory bodies	Efficiency and effectiveness of project management procedures and tools (survey)	Annual	> 80 %	77 % Survey results were used to recalibrate the internal processes and planning for increased efficiency
			Nº of high risks identified in annual risk assessment		≤ 3	3
			Percentage of identified internal controls deficiencies addressed within timelines		100 % for critical, 80 % for major, 60 % for moderate	No critical recommendation issued in 2023 ICF assessment. Out of 3 moderate and 2 major – the recommendations remain valid as the deficiencies have not been fully mitigated.
			Nº of complaints filed against ENISA / number of identified legal or regulatory breaches		≤ 3	4 complaints; 2 identified breaches
			% of revised and up to date corporate rules (MBD, EDD, policies, processes)		60 % corporate rules which have not been reviewed less than three years ago; 80 % corporate rules which have not been reviewed less than four years ago	23 MBDs on corporate rules from before 2019
			MOU with Greek authorities for carbon dioxide reduction in ENISA HQ in place		MOU process initiated by the end of 2024	Process has not started
			Efficiency and effectiveness of ITMC/BMC processes (survey)		> 60 %	ITMC: 75 % BMC: 63 %

OUTPUTS	HOW OUTPUT EXPECTED TO CONTRIBUTE TO ACTIVITY OBJECTIVE FOR THE YEAR	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
11.2	• Compliance with new regulation on a high common level of cybersecurity within EUIBAs • Timely identification and response to cybersecurity risks • Continuous monitoring of IT systems cybersecurity and timely identification of issues and areas of improvement (first level and second level controls)	MT and relevant committees External and internal audits Statutory bodies	Percentage of identified high risk mitigation measures addressed within timelines	Annual	90 %	All high risks addressed within timelines and/or accordingly reported and planned
			Cybersecurity training session for staff and managers	Annual	90 % At least two trainings per year	Two training sessions by ISO; training programme and phishing exercise (via dedicated training platform)
11.3	• Cybersecurity advisory in implementation of the new Regulation on a high common level of cybersecurity in EUIBAs and in cooperation with CERT-EU • Shared services in the area of data protection, legal services and accounting	MT, BMC EUAN (agencies receiving ENISA's support)	Satisfaction within the EU agency network with ENISA support services	Annual	> 80 %	High satisfaction expressed by the agencies that received ENISA's services
11.4	Streamlined document management practices	MT, Staff Committee	Percentage of staff considering that the information they need to do their job is easily available/accessible within ENISA	Annual	55 %	66 % of staff survey respondent agree that ENISA's internal communication is timely and clear (result of last year was 39 %)
			Response timeliness to external parties (internal reporting)		48h	High response rates in accordance with ENISA's code of conduct

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	11	Nº OF FTES ACTUALLY USED	11.26
PLANNED BUDGET (EUR) [59]	470 888	BUDGET CONSUMED (EUR) [60]	614 559
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	240 637

[59] Direct costs only.

[60] Direct costs only.

ACTIVITY 12

Reputation and trust

Under Activity 12, ENISA seeks to achieve the requirements set out in Article 4(1) of the CSA to 'be a centre of expertise on cybersecurity' and further build its reputation as a trusted entity through consistent messaging, adherence to corporate rules for communications activities. In the 2024–2026 SPD, a new activity on reputation and trust was created with new KPIs. Outreach and coherent messaging about ENISA's overall mandate, tasks and work are supported by this activity, which includes the dissemination of information to ENISA's external stakeholders.

Under this activity, the following was achieved in 2024.

- ENISA's strategy was updated and refined in order to respond to known challenges and to anticipate forthcoming ones with input from all statutory bodies.
- Successful website redesign and launch: ENISA's communication sector launched a modernised website in December 2024, improving user experience, accessibility and information architecture. This enhanced the agency's digital presence and streamlined access to key resources and providing information to a wider audience.
- Significant growth in media coverage: press mentions increased by 36.95 % in 2024 (1 149 mentions compared with 839 in 2023), strengthening ENISA's visibility and outreach across media channels.
- Strategic communications execution: the implementation of 20 tailored communication plans and support for ENISA's events and campaigns ensured effective stakeholder engagement, reinforcing ENISA's communication impact.
- Stakeholder engagement: ENISA organised 13 meetings of its statutory bodies. In 2024, the respective secretariats onboarded 25 representatives, representing a high turn-over within the statutory bodies. An event highlight included hosting the directors of the national cybersecurity authorities of MS, the European Free Trade Association countries, Ukraine (SSSCIP), the United Kingdom (NCSC-UK) and the United States (CISA), in order to discuss cybersecurity threats and trends assessments on a national level, and practical implementation challenges of the NIS2 Directive.

- A new biennial ENISA satisfaction survey received 186 responses, a 15% increase from the previous survey. The results overall were positive with a 1% increase in trust in the Agency being able to fulfil its mandate.

Based on the lessons learned in 2024, the following changes could strengthen and consolidate the focus of Activity 12 moving forward.

- Improvements to and streamlining of the internal communications processes. Through the involvement of the communication team as players in the Cyber Europe exercise, it was observed that there is room for further improvement to efficient communications, such as lines to take and public communications.
- Activity 12 met its objectives, although not all targets were reached. The activity results showed a 1 % increase in the level of trust in ENISA to achieve its mandate compared with the 2023 survey.
- Increased demand for presence at physical events had a direct impact on the activity's budget. Limited available resources led to the de-prioritisation of several activities and changes in statutory body meetings. The centralisation of event budget management by ENISA will improve this in 2025.

ANNUAL

GENERAL ACTIVITY OBJECTIVES	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	TARGET	RESULTS 2024
12.A Protect and grow the agency's brand and reputation	Ensure efficient corporate services	Level of trust in ENISA (as per the biennial stakeholder survey)	Biennial	95 %	96%
12.B Support the activities implementing the core mandate by improving knowledge sharing	Ensure efficient corporate services	High satisfaction with essential communication and assistant services	Annual (MT survey	60 %	63%
		High satisfaction with demand-driven communication and assistant services	Annual (MT survey)	60 %	50%
	Develop service propositions with additional external resourcing	Limited disruption of continuity of internal and external communications	Annual (business continuity plan)	Target set in business continuity plan and agreed response time objectives	6–12 hours (before reaching maximum tolerable downtime) for ENISA's website

OUTPUTS	OUTCOME
12.1 Implement the multiannual communications and stakeholders' strategies	ENISA celebrated its 20th anniversary in 2024 and used the opportunity to raise awareness of its mission and work among its external stakeholders, to increase the reputation of a long-standing reputable agency, and to celebrate staff contributions. An anniversary logo and dedicated materials were created, while an MB and Advisory Group event celebrated the occasion in the presence of the Greek Minister for Digital Governance and the press. To implement the communications strategy, 20 individual communication plans were developed in collaboration with operational units and teams. The communications sector supported the publication of 22 reports, 21 press releases and 12 news items during the year. Additionally, ENISA organised a total of 108 events, including meetings, workshops, and 13 meetings of statutory bodies (MB, EB, AG, NLO Network). In the course of 2024, in line with its event policy, ENISA conducted satisfaction surveys for 15 of its largest events, for which 1 058 responses were received.

OUTPUTS	OUTCOME
12.1 Implement the multiannual communications and stakeholders' strategies	Of the 1 058 respondents, a percentage of 88 % were overall 'very satisfied' and 'satisfied' with the organisation of the events. The responses were further processed to define metrics and KPIs for 'lessons learned'. The event participants came mainly from national public administrations (39 %) and industry (37 %). The remaining stakeholders represent EU public organisations, international organisations, civil society or consumer organisations and academia or research. A significant increase in press and media mentions was recorded, with 1 149 press mentions in 2024, compared with 839 in 2023 – reflecting a 36.95 % rise within a year. ENISA's website received 2.3 million visits in 2024, a slight decrease from 2023. To enhance its online presence, a new modern website was designed and launched in December 2024. This redesign aimed to modernise the agency's web image while improving user experience through enhanced information architecture and the implementation of accessibility features. The sustained website traffic resulted from the proactive approach adopted in 2023, which involved restructuring thematic topics and strategically promoting ENISA's content across various platforms, social media channels and events. However, social media impressions declined to approximately 3.3 million in 2024, compared with 4.4 million in 2023, primarily due to the reduced use and promotion of X (formerly Twitter).
12.2 Implement internal communications strategy	The internal communications strategy, as part of the overall communications strategy, contributed to increased knowledge-sharing and internal synergies. During 2024, the annual Staff Strategy Days were organised to engage all staff in exploring strategic avenues for growth and foster an agency-wide spirit. The events are vital, as staff are spread across three offices and hybrid working means less occasions for them to meet as a group. A satisfaction survey found that 'Interactions with colleagues and familiarisation with their work' was rated as 4.1/5, while 'Engagement with discussions on strategic growth' was rated as 3.3/5 by staff members. 28 Q & A sessions and six ENISA academies were organised for internal knowledge-sharing. A dedicated staff satisfaction survey took place on the content and the frequency of the Q & As as one of the main internal communication tools. 72 % of the staff were satisfied and 26 % neutral with the content of the Q & As, while 58 % felt satisfied with the frequency and 26 % were neutral about it. Dedicated inductions to all newcomers were conducted. In addition, the agency released weekly management team updates in the form of short debrief videos (51 videos) and a total of 247 internal announcements (compared with 171 in 2023), in an effort to ensure coherent and consistent information circulation within the agency.
12.3 Manage and provide the secretariat for the statutory bodies	ENISA organised 3 meetings for the ENISA MB (1 online, 1 hybrid, 1 physical), 2 digital votes of the MB for Executive Board vacancies, 4 meetings of the Executive Board (3 online, 1 physical), 2 meetings of the Advisory Group (2 hybrid) and 4 meetings of the NLO network (3 online, 1 hybrid). Additional drafting meetings (online) were held with volunteering Advisory Group members for the formulation of 3 Advisory Group opinion papers. In 2024, the respective secretariats onboarded 15 new MB members and alternates (8 members, 7 alternates) and 10 new NLO members (9 members and 1 alternate). In total, the MB made 17 decisions during the year, including decisions on the extension of the Executive Director's term of office, the establishment of ENISA's internal structures and the general direction of ENISA's operations (revision of the ENISA strategy).

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
12.1	• Increase transparency and outreach • Engaged communities • Increased impact of ENISA activities • Relevant and easily accesible information is provided to stakeholders	Management team and agency stakeholders	Nº and types of activities at each engagement level (stakeholder strategy implementation)	Annual (internal report)	N/A	Total engagements: 391 40% Partner 11% INVOLVE/ ENGAGE 18% Consult 31% Inform
			Number of social media engagement	Annual (media monitoring)	> 80 000	66 300
			Stakeholder satisfaction with ENISA outreach	Biennial (survey)	> 80 %	96%
			Number of total ENISA website visits	Annual (website analytics)	> 2.5 million	2.3 million
12.2	Engaged staff	Management team and Staff Committee	Staff satisfaction with the quality and timing of ENISA internal communications [61]	Annual (survey)	> 50 %	65 %
12.3	• Support the operation and organisation of ENISA statutory bodies • Support effectiveness of implementation of work programme (validation of operational outputs) • Providing administrative support for the day to day working of the MB decisions and recommendations from NLO and AG	Statutory bodies, management team and committees	Number of feedback received per NLO consultation	Annual (Internal report)	> 2	27 for NLO subgroups (3.6 as average for validations in NLO Network
			Nº of feedback received per AG consultation	Annual (internal report)	> 2	11.3 average
			Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA	Annual (survey)	> 80 %	97%
			Satisfaction of statutory bodies with ENISA portals	Annual (survey)	> 80 %	83%

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	5.5	Nº OF FTES ACTUALLY USED	4.39
PLANNED BUDGET (EUR) [62]	485 000	BUDGET CONSUMED (EUR) [63]	729 662
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	284 753

[61] The question in the 2024 staff satisfaction survey was phrased slightly differently.

[62] [63] Direct costs only.

ACTIVITY 13

Effective and efficient corporate services

This activity supported ENISA aspirations as stipulated in Article 3(4) of Regulation EU No 2019/881 (Cybersecurity Act), which obliges the agency to: 'develop its own resources, including … human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation'. Overall, this activity is of a dynamic nature and driven by demand and compliance, all while aiming to enhance innovation and increase organisational efficiency. In parallel, it provides cross-cutting support to all ENISA activities, while aiming for administrative excellence with a service-driven mindset. Continuous improvement cycles are an element of the service provison.

In 2024, the unit managed to achieve day-to-day business continuity of critical services in the areas of HR, finance and procurement, despite resources being overextended due to an increasing demand for service provision from operations, thus requiring use of overtime and surplus hours to fulfil activities. Resources remained stretched, especially in the area of budget and finance. Operational activities required extra support in further analysing data, providing budget foresight and reporting and qualitative analysis.

In this context, CSS continued to review and upgrade its service, policy provision and digitalisation processes, where feasible.

In 2024, the first year of the corporate and HR strategy was completed, during which key HR user-centred services were set, in particular the application of the first year of the newly developed strategic workforce planning, allowing for improved horizontal talent acquisition. The competency framework of the agency was embedded in the refined recruitment procedures, which were carefully planned and conducted in a timely manner. To ensure a well-established strategic workforce planning, the agency introduced a 360 ° multi-source evaluation and streamlined the process, leading to better insights into staff capabilities and growth potential, and also supporting the streamlined reclassification exercise.

The staff satisfaction survey was refined, as a group effort of the management team, the Staff Committee and staff, leading to a high participation rate of 80 % and generating a rich source of improvement opportunities, increasing the overall staff engagement in the jointly defined follow-up actions. To further increase staff engagement, the unit introduced modern digital solutions to better manage staff engagement and effectively use the feedback, based on real-time reports and interaction opportunities for managers (OfficeVibe). With regard to talent acquisition, the agency further modernised its selection process by introducing an automated IT tool (Allegro). This tool will also be used for the

assessment and management of individual external experts to assist ENISA (CEI experts) falling under the digitalisation of procurement. The agency aims to fully use the central HR services of the Commission, capitalising and reducing costs due to economies of scale, and to allow the agency to focus on the strategic priorities of talent acquisition and talent development, strategic workforce and succession planning. HR dashboards will be developed and maintained on a monthly basis to support middle management.

In the area of procurement, the unit continued its digitalisation path by connecting the PPMT e-tool with the accruals-based accounting (ABAC) LCK module. The implementation of the agency's first contribution agreement related to support action generated a strong demand for the increase of efficiency within procurement processes. Upcoming new contribution agreements will increase the need for further digitalisation and automation to reduce workload and improve anticipating capability. The responsible use of AI in this respect will further support this trend.

The security and infrastructure sector continued to progress in its digitalisation path by the implementation of 'Service Now'. One of the main objectives achieved in this sector in 2024 was to prepare the inspection for ENISA's EU classified information (EUCI) accreditation. The assessment performed by HR.DS and ENISA in autumn 2024 is currently awaiting an assessment report by HR.DS. Overall, the security and infrastructure sector continued its transformation and IT service delivery, while expanding and modernising its services, building on the knowledge library and standardisation, in line with the key objectives set in the work programme.

In the finance and budget area, the preparations for the transition to SUMMA are ongoing. Because of the agency's size growth and the implementation of the support action contribution agreement, the increase in the number of financial transactions also enhances the need for further automation, as resources are limited. Ensuring business continuity planning in key areas is becoming more prominent. As a supporting unit, CSS needs to be able to better anticipate and promptly manage emerging needs. To achieve this, a revision of key financial policies, the simplification of the agency's financial procedures and the continuous monitoring of the budgetary risks, planning and foresight are of key importance. For 2025, an integrated budget and financial planning tool with automated dashboards will be explored, to provide operational activity managers and project managers with up-to-date information and off-the-shelf support services.

In Q4, the agency prepared for the 2025 annual workforce review exercise by assessing workforce needs for the upcoming year. This concerns a series of posts and functions, along with the allocated grades, in order to address short-, medium- and long-term business needs. To meet changing demand and bridge the gap in the required competences, a review of the business operating model, redesigning the strategic, tactical and operational work modalities, is required to better address the work programme priorities and further implement the corporate and HR strategy. When it comes to corporate service provision, smart use of external service providers and the exploration of shared corporate services are on the agenda, not only within the agency, but also in the collaborative inter-agency environment.

ANNUAL					
GENERAL ACTIVITY OBJECTIVES	LINK TO CORPORATE OBJECTIVES	ACTIVITY INDICATORS	FREQUENCY (DATA SOURCE)	TARGET	RESULTS 2024
13.A Enhance people-centric services by implementing the Corporate and HR strategy	Effective workforce planning and management	Implementation of Strategic Workforce Plan / Strategic Workforce Review decisions	Annual	Fully implemented	The workforce is assessed on an annual basis. The exercise concluded with ED Decision No 21/2024. Implementation was partially realised and will be embedded in the 2025 exercise.
	Efficient talent acquisition, development and retainment	Implementation of the Corporate and HR strategy	Annual	Actions implemented according to the timelines	Vacated staff posts in 2024 were fulfilled within 143 days. The indicated KPI was to fulfil posts within 300 days
	A caring and inclusive modern organisation	High participation in the staff satisfaction survey	Annual	75 %	80 %
13.b Ensure sustainable and efficient corporate solutions and promote continuous improvement	• Ensure efficient corporate services • Introduce digital solutions that maximise synergies and collaboration in the agency • Developing service propositions with additional external resourcing • Promote and enhance ecologic sustainability across all agency operations • Develop an efficient framework for ENISA continuous governance to safeguard high level of IT and physical security	Understand best practices in sustainable IT solutions Limited disruption of continuity of corporate services Handling EUCI at the level of SECRET UE / EU SECRET	Annual Annual By Q2 2024	IT strategy updated accordingly Business Continuity Plan for corporate IT, facilities, financial and HR services ensured Has been accredited	In 2024, the IT sector further implemented the ITIL best practices such as: consolidated database of the IT assets has been implemented, IT service management, IT requests and IT incidents). Further deployment of Zerotrust principles and adoption of key policies, such as a helpdesk policy and a smartphone policy. Implementation of a mobile device management solution for managing all mobile devices. Effective disaster recovery is in place to ensure the Business Continuity Plan of core services. EUCI inspection took place and the report will be sent in 2025.

OUTPUTS	OUTCOME
13.1 Manage and provide horizontal, recurrent, quality support services in the area of resources for ENISA staff and partners	Revision of the annual **L & D plan and staff performance:** the L & D plan was revised with contributions from the Staff Committee, the staff and the management team. To allocate the planned L & D budget for the units and horizontal permanent teams in a way that L & D effectively supports addressing the technical and professional expertise and competences of staff, a prioritisation system for L & D requests was introduced and monitored by HR during the year. As this provided a centralised overview of needs, training sessions could be grouped, thus reducing costs. As the appraisal ran over the year 2023 and finished at the beginning of Q3, the full allocation of the trainings needed to take place in Q3 and Q4, generating challenges in the planning of finalising the projects while also performing the planned trainings and implementing the L & D plan. While the L & D data and personal development plans analysis generated better insights into L & D demand and execution, the lesson learned is that the appraisal round needs stricter deadlines to ensure timely L & D execution in the year. The **reclassification** exercise methodology was improved, with support of the Staff Committee, the management team and staff, by introducing a clear scoring mechanism for merits, ensuring a better and more transparent comparison of the merits of staff members in the same grade. In addition, the data analytics were more focused on alignment with the methodology, increasing the quality of the exercise while at the same time increasing the time efficiency of the exercise. No appeal procedures followed, confirming the transparency and fairness of the exercise. Overall, in 2024 a total of 15 staff members were reclassified. For **recruitment,** four selection procedures were advertised and launched throughout the year. One referred to an SNE selection targeting Ukrainian national authorities, and the three others focused on contract and temporary staff and were successfully finalised within an average of 144 calendar days (counted from the date of the vacancy notice publication to the establishment of the reserve list). Additionally, two internal mobility calls were conducted. Other recruitment sources, such as direct hiring via ENISA reserve lists, the EPSO CAST database and exchange of reserve lists with other EU agencies, were also exploited to meet the recruitment needs of the agency. This led to an execution rate of 98 % of the establishment plan. The further optimisation of the digitalisation of the application procedure and its compliance with case law took place and continues to have the full attention of the agency in 2025. The sharing of reserve lists in the EUAN environment has become a common practice. It all started with a pilot in setting up joint vacancy procedures with other EU agencies. ENISA explored the possibility of shared services in other areas. The **annual workforce review (AWR) 2024** was concluded at the beginning of April 2024. To better balance the staffing of the operational and supporting units, ensuring that the agency can meet its increasing mandate due to the development and implementation of new and revised EU cybersecurity legislation, the focus was brought towards the two corporate units: the Executive Director's Office and the Corporate Support Services Unit (CSS). While support needs grew, the needs for efficiency and revision of some of the posts in these units was necessary. Due to unforeseen circumstances, the execution of the CSS review was not possible and will be performed in line with the start of the corporate and HR strategy 2026–2029.

[64] Decision No MB/2024/10, on the establishment of ENISA's internal structures (Recast of the MB Decision MB/2020/09).

OUTPUTS	OUTCOME
13.1 Manage and provide horizontal, recurrent, quality support services in the area of resources for ENISA staff and partners	The MB endorsed **the agency's operational restructuring plans** (64) for all existing the operational units by January 2025. The Staff Committee was consulted and several meetings were organised with staff members for information-sharing purposes and for them to contribute to the process. During its informal MB strategy meeting on 21 March 2024, the MB endorsed the proposed adjustments to the ENISA structure, in order to consolidate its current activities, increase the agility of the agency to address new upcoming tasks and better equip the organisation to tackle the objectives set in ENISA's corporate strategy, as endorsed by the MB in 2023. Administrative Notices 2024-06, 2024-07 and 2024-10 outline the details. The horizontal permanent teams would be dismantled as from January 2025 and, with the existing units, transformed into eight operational units. All middle managers were assigned to these new units by ED Decisions in line with the agency's policy to rotate middle managers. An assignment procedure for staff was put in place, ensuring that staff members were well-informed and given the opportunity to provide their views on their proposed assignment. To ensure business continuity of the agency, senior management was given extra support with the appointment of the Chief Cybersecurity Operations Officer and the Associate Chief Cybersecurity Operations Officer. In addition, heads of sector with more than two years of managerial experience were given the role of Deputy Head of Unit. Using internal mobility calls, six new heads of sector were appointed and assigned to new units. HR ensured that all staff was reassigned to these new units and job roles, and job descriptions were adjusted in line with the new structure. Systems [65] were updated and tested, and related access rights and document management adjusted to ensure a smooth transition. All process flows and standard operating procedures and guidelines were also adjusted. **Staff satisfaction survey 2024** The staff satisfaction survey was reviewed by the Staff Committee, the entire staff and the management team prior to its launch. All input was processed to guarantee the maximum buy-in and trust of all staff. This resulted in a response rate of 80 % percent. The survey touched upon five core areas: • leadership and direction; • authority and empowerment; • respect and wellbeing; • performance management; • L & D. Based on the outcomes, the management team, the Staff Committee and staff jointly drew up a roadmap of actions for improvements for 2025. The roadmap focuses on the main shortcomings in the five respective areas. The most important are the wellbeing and health of staff: workload and stress management, performance management, training of reporting officers in high qualitative CDRs, addressing of under-performance, more attention for signals of inappropriate behaviour, and the importance of cross collaboration between units (synergy-based collaboration). HR will guide and roll out the roadmap of support actions for carrying out improvements.

[65] For example, ARES, ABAC, Mission Processing System (MIPS+), the ENISA Budget, Sysper, the Agency's intranet, TEAMS, OfficeVibe and other applicable systems.

OUTPUTS	OUTCOME
13.1 Manage and provide horizontal, recurrent, quality support services in the area of resources for ENISA staff and partners	**Staff Strategy Days** The Staff Strategy Days took place on 15–19 January 2024 and a number of competency related events were organised including a Staff Assembly **Budget and finance** The finance sector was occupied with budgetary and financial adjustments for the new organisational structure including preparations to move budget management from ABAC to SUMMA system of the Commission see under 13.4. In addition, the FIA tasks were centralised and the implementation of results of an external analysis on the simplification of ENISA financial procedures. During 2024, ENISA took a number of actions to ensure that payments are executed in a timely manner. This led to a significant improvement of the late payment rate, which was 7.4 % for the full year, 2.6 % for Q2–Q4 2024 and 0.4 % for Q4 2024. The agency is committed to continuing the reduction of the late payments and work towards a structural low percentage under 3 %. The procurement plan was drafted and finalised in December, including the information related to the tender procedures to be launched in the next year. A new procurement tool has been used for all open/restricted procedures, and preparations/meetings with an external contractor for a new platform related to the individual external experts to assist ENISA (CEI experts) were conducted. In 2024, two SLAs were signed: one with the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-Lisa) for exercise support, and another with REA concerning the provision of validation services.
13.2 Implement the agency's corporate strategy (including the HR strategy), with an emphasis on initiatives in the talent development, growth and welfare, innovation and inclusiveness areas	The agency made considerable improvements in competency-based performance measurement and planning of related training sessions. The staff satisfaction survey also emphasised the success of the competency framework that was embedded in the L & D planning. In 2024, the framework was embedded in the recruitment procedures, generating a baseline proficiency target for new staff, setting a clear development path for growth in competences in line with career opportunities. The internal mobility call for heads of sector and the role of deputy heads of unit clearly contributed to increasing career opportunities for staff. To enhance key competences and support functional competences, L & D is supporting initiatives in talent development and personal growth. Welfare remains an important element of the corporate strategy. Training sessions were provided in the following areas. • Communication: with a focus on empathetic leadership and communication for the management team; revealing voice (speak and thrive) and story-telling (presentation skills/ building a narrative) to spark innovation and boost confidence for all staff members; • Sessions on how to deal with change and to build resilience were offered, to support ENISA's staff members through all incoming changes. In addition, the HR team and a few other interested colleagues followed a mental health first aid course, preparing them to identify and offer support where needed. • Operational units have opted to further their skills in cybersecurity and keep ahead of all incoming developments. Several courses were taken, with top certifications from the SANS Institute and ISC2. To gain more insights into talent development, the L & D policy was updated and revised. Data collection improved the monitoring of the costs and effectiveness of training sessions. The restructuring of the agency also contributes to the learning opportunities for staff members by the assignments of staff to new units with different or sometimes more similar tasks, but nevertheless increasing the learning process. The new environment will lead to new discoveries, generating innovation and stimulating knowledge-sharing. Also, the collaboration with the Commission in terms of contribution agreements will broaden the service provision of ENISA, generating more growth opportunities for staff.

OUTPUTS	OUTCOME
13.3 Manage and provide horizontal, recurrent, quality support services in the area of facilities, security and corporate IT for ENISA staff and partners	In 2024, significant advancements were made in the provision of horizontal, recurrent and quality support services in the areas of facilities, security and corporate IT for ENISA staff and partners. Key achievements include: • implementation of ServiceNow as the IT service management (ITSM) solution, along with the configuration management database (CMDB), integrating the entire IT portfolio of services and IT assets; • enhancement of the security model to further strengthen the organisation's cybersecurity posture; • completion of an effective disaster recovery site for CSS, ensuring operational resilience; • ongoing implementation of the ServiceNow module for Facilities and Security, streamlining service management in these areas; • deployment of a mobile device management solution to enhance security and control over mobile devices; • modernisation of end-user IT equipment, improving efficiency and user experience; • strengthening IT governance through the implementation of various policies and SOPs to enhance compliance, efficiency and security.
13.4 Enhance operational excellence and digitalisation through modern, safe and secure and streamlined ways of working and introducing self-service functionalities	**Human resources digitalisation** In 2024, the review and digitalisation of all personal files was finalised, in preparation for the planned use of the Sysper personal files module to be activated in Q1 2025 and become operational in Q2 2025. The Sysper probationary period module was tested but deemed unfit for the current ENISA process, due to the agency's integrated competency framework in performance and talent management, which is not applicable within the Commission's approach. The agency is committed to further exploring the implementation of Sysper modules, and more particularly the implementation of HRT, which will further enhance digitalisation and explore the responsible and effective use of AI, in line with European Data Protection Supervisor guidelines. Workleap Officevibe was introduced and implemented in October 2024, to enhance staff engagement and ensure follow-up, encourage staff to provide feedback with regards to their wellbeing, workload and working environment, and to recognise achievements of staff and management. The tool allows for sharing of real-time reports, launching additional surveys and having digital one to one conversations for improvements, encouragement and sharing of ideas. In recruitment, preparations have been made for the planned use of a digital platform service provider to perform and monitor testing on behalf of the agency, further increasing time efficiency in the recruitment procedures. In procurement, the agency explored the enhancement of digitalisation for the selection and maintenance of a platform for registration of individual external experts to assist ENISA (CEI experts). In finance, preparations and initial training sessions were performed in view of the upcoming onboarding of SUMMA.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
13.1	• Implement payroll and recurrent administrative services • Implement annual recruitment plan • Implement annual L & D plan and staff performance • Implement annual procurement plan via PPMT • Implement insource mission service support • Implement the ED decision on strategic workforce review (adopted in May 2023) • Follow up on FIA centralisation and implementation of results of external analysis on simplification of ENISA financial procedures • Analyse procurement services and tenders and propose simplifications • Explore further synergies with PMO SLA (e.g. reimbursement of experts)	• Management team • IT Management Committee • Budget Management Committee • Staff Committee	Turnover rates	Annual	3 %	4.1 %
			Establishment plan posts filled		> 95 %	98 %
			Time from vacancy announcement to candidate selection		< 300 days	143 days
			Percentage of the implementation of the approved recruitment plan		> 90 %	94 %
			Percentage of the implementation of the approved procurement plan		> 90 %	63.63 %
			Percentage of procurement procedures launched via e-tool (PPMT)		> 90 %	100 % (for open, restricted and middle value procedures)
			Percentage of budget implementation		> 95 %	100 %
			Average time for initiating a transaction (FIA role)		< 7 days	7.51
			Average time for verifying a transaction (FVA role)		< 3 days	0.19
			N° of budget transfers		< 4	2
			Late payments		< 8 %	7.4 %

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
13.2	• Establish/review corporate costing models and mechanisms to forecast, anticipate and promptly manage emerging needs • Revise HR-related MB decisions on middle management staff, SNEs, the L & D framework, and the appraisal and reclassification of TA and CA staff, as indicated in the corporate strategy • Set up of key HR policies in the area of L & D and review staff welfare and mission policies • Introduce modern digital solutions for managing talent that give real-time input to managers • Modernise the selection process by introducing automated IT tools in the process	• MB • Manage-ment team • Staff Com-mittee • EUAN • BMC	Nº of policies/ IR revised or adopted	Annual	> 1	L & D; reclassi-fication; SSS, amendment EP; school-ing; travel missions, trainees, VN & competences, restructuring decisions, mobile phone, parking; appraisal admin note, EDD decision on gifts and dinners
			Nº of processes reviewed/ redesigned		> 1	Postponed [66]
			Percentage of staff satisfaction survey with talent development		> 50 %	52 %
			Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time		> 95 %	Partially post-poned in 2024 [67]
			Nº of implemented competency-driven training and development activities		> 1	All training sessions are linked to key competences of ENISA and connected with the CDR
			Nº of multisource feedback evaluations implemented and followed up		> 5	16 360 ° for HoU, HoS and TLs; and 12 360 ° SM for contract renewals

[66] Due to unavailability of budget, no new digital solutions were introduced in 2024.

[67] Due to unavailability of critical HR staff in 2024, the follow up actions for staff satisfaction survey were decentralised in 2024 to the relevant head of unit. However, HR coordination was initiated following the October 2024 staff survey, the results of which will be submitted in the 2025 AAR.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
13.3	• Implement annual IT project plan • Implement annual FM plan, maintenance and upgrades, including physical security service provision • Upgrade infrastructure to improve working conditions and create a conducive work environment to ensure sustained productivity and employee satisfaction • Align the lifecycle of IT services and equipment (servers, used equipment) with objectives • Ensure timely implementation of requirements to maintain EUCI at relevant level • Review ENISA's geographically dispersed IT solutions and systems and propose cost benefit solutions that would maximise ENISA's corporate resilience • Follow up on the ServiceNow implementation and explore further synergies for integrating further services (HR, FM, EDO, etc.) • Follow up on AV implementation and upgrade of meeting rooms	• Management team • IT Management Committee • Budget Management Committee • Staff Committee	Satisfaction survey for working environment	Annual	80 %	N/A [68]
			Safety and security incidents reported at workplace in any of the 3 ENISA offices		< 3	Zero cases
			Average time for dealing with facilities management requests		< 3 days	2 days
13.4	• Explore synergies between FM and security service provision by integrating services via one service provider, hence reducing FWC numbers, and provide all-inclusive services • Implementation of an identity and access management solution to increase the cybersecurity posture of the organisation	• Management team • IT Management Committee	Resilience and quality of ENISA IT systems and services (automated or via surveys). Specific KPIs will be defined for each expected result of the output and will be monitored separately. Generic indicators:	Annual	99 %	99.89 %

[68] This indicator was not measured due to the fact that this indicator is measure biennially and therefore will be measured again in 2025.

OUTPUTS	EXPECTED RESULTS OF OUTPUT	VALIDATION	OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
13.4	• Equipment renewal (laptops/mobiles) to ensure business continuity through updated technology, enhanced security measures and improved equipment performance • Implement an effective backup solution (SAN) to enhance business continuity by safeguarding critical data, mitigating the risk of data loss and ensuring a swift operation recovery in the event of system failures, disasters or cyber-attacks • Implement new A/V and conference equipment to bolster business continuity by facilitating seamless remote collaboration to ensure high-quality communication and collaboration, which is essential to maintain productivity and operational efficiency • Implement of a cloud-based platforms and solutions automate IT delivery services, assure service availability, improve self-service functionalities and provide critical IT-related metrics enabling secure access and sharing of information or device from any location • Upgrade physical security measures to ensure high standards for the other ENISA offices to get EUCI accreditation • Further development of the Athens data centre for high-availability purposes to ensure business continuation and minimisation of downtime risks	• Management team • IT Management Committee	• Critical systems uptime/ downtime • Staff satisfaction with resolution	Annual	85 %	/A (not part of ENISA survey in 2024). ENISA used the ServiceNow ticketing system (from April to December of 2024), whose results are: Percentage of major IT helpdesk requests resolved in a satisfactory way within two business days: 82.53 %

ALLOCATED FTES BASED ON THE FULL ESTABLISHMENT PLAN AT 2024 YEAR END	19.5	Nº OF FTES ACTUALLY USED	16.96
PLANNED BUDGET (EUR) [69]	4 260 911	BUDGET CONSUMED (EUR) [70]	4 966 017
		OF WHICH CARRIED FORWARD TO 2025 (EUR)	2 084 441

[69] [70] Budget includes: staff development, staff welfare, external temporary staffing, building costs, consultancy managed by Activity 13, corporate and administrative expenditure, core and corporate ICT managed by Activity 13.

II

PART II (a)

MANAGEMENT

2.1. Management Board

ENISA is governed by MB members. Each member is a representative of an MS and one member is a representative of the Commission. The term of office for the members of the MB and their alternates is four years, and the term is renewable; there is no set limit for a maximum term in office. The main competence of the MB falls into the composition, review and eventually the approval of the agency's annual work programme. 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 2024, the MB held three meetings. In addition, on two occasions the MB held a vote to fill positions in the ENISA Executive Board. In March 2024, in the MB strategy meeting, the board discussed the revision of the ENISA strategy beyond 2024, the outlook on ENISA's strategic objectives and the implications of the future work programme on ENISA's structure. In total, the MB adopted 17 decisions, including a decision on the extension of the Executive Director's term of office, the establishment of ENISA's internal structures and the general direction of ENISA's operations (revision of the ENISA strategy). In accordance with the Cybersecurity Act and the MB's rules of procedure, the MB's decisions were prepared by the Executive Board and adopted by the MB. The 2023 annual activity report was duly adopted, thus contributing to the discharge of the Executive Director, and the MB also expressed its opinion on the final annual accounts for the financial year 2023. Additionally, the 2025–2027 ENISA SPD, including the 2025 budget and establishment plan, was adopted. Finally, the MB approved two amending budgets for the financial year 2024 and adjusted the 2024 establishment plan.

2.2. Major developments

ENISA: 20 years of strengthening cybersecurity

In 2024, the agency celebrated 20 years since its establishment. Since 2004, ENISA's mission is to achieve a high common level on cybersecurity across the EU.

Revised ENISA strategy

The ENISA strategy, adopted in 2020, was reviewed during the reporting period and the MB adopted the new version in November 2024. The revised strategy is a cooperative effort of the Executive Director, the MB and the ENISA Task Force on supporting the review of ENISA's strategy and mandate. For this purpose, input was gathered from the ENISA Advisory Group, the NLO network and ENISA staff.

The updated strategy refines the seven existing objectives and provides indicators to measure their success.

Stakeholder strategy

In 2024, the agency initiated the review of its stakeholder strategy to seek more efficient engagement with key partners and stakeholders. This process aims to ensure that the approach remains effective, inclusive and aligned with ENISA's strategic objectives. The outcome of the review is expected to be concluded in the course of 2025 and presented to the MB for endorsement.

Structural adjustments and strengthening senior management

In 2024, the agency implemented measures to optimise its operational activities and support structure, focusing on enhancing efficiency and fostering synergies. To ensure the effective execution of its expanding tasks and functions (CRA, CSOA), the MB decided to align its operational structure more closely with its work programme. This included the creation of eight dedicated units, each responsible for one of the work programme's eight operational activities. This consolidation not only leverages existing synergies more effectively, but also increases both the budget and the median FTE count per activity, rising from just under eight FTEs in 2024 to nearly 12 FTEs in 2025 and onwards. This higher median FTE count is critical for providing operational activities with greater operational depth, enabling them to better absorb unforeseen urgent tasks. It also offers increased flexibility, allowing people to be reallocated within activities as new priorities emerge.

In 2024, the agency's management was strengthened with the appointment of a Chief Cybersecurity and Operations Officer and an Associate Chief Cybersecurity and Operations Officer.

The Chief Cybersecurity and Operations Officer bringing extensive experience in national cybersecurity, will lead efforts to enhance operational efficiency and ensure that ENISA remains responsive to emerging cyber threats. His leadership is set to reinforce support for MS and strengthen operational partnerships.

The Associate Chief Cybersecurity and Operations Officer's expertise in stakeholder engagement, strategic planning and cybersecurity policy frameworks will enhance ENISA's access to top-tier expertise. His role will also support the agency's ongoing investment in its visibility and presence within the EU cybersecurity landscape.

Closure of the Heraklion office

Another important step taken by the agency to optimise financial resources has been the planned closure of the office in Heraklion, Crete, Greece by 30 June 2026. Since relocating to the Athens metropolitan area in 2019, Greek authorities have assumed full responsibility for the rental of the headquarters. Maintaining a portion of administrative and operational functions in Heraklion, while the majority of the agency operates in Athens, incurs not only direct costs but also significant indirect expenses against no visible benefit. Closing the Heraklion office will result in additional, albeit modest, financial savings, enabling the agency to redirect these resources toward operational activities more effectively.

New legislative proposals

ENISA's expertise was solicited for a number of significant legislative proposals in the area of cybersecurity developed in the course of 2024.

The CRA entered into force in December 2024, to make Europe's cyberspace safer and more secure. The act introduces greater responsibilities on manufacturers to guarantee the security of hardware and software products. Central to the act are new obligations for manufacturers to provide software updates that fix security vulnerabilities and offer security support to consumers. Products will bear the CE marking to indicate that they comply with the regulation's requirements. The main obligations of the act will apply from 11 December 2027.

The CSA entered into force on 4 February 2025. It aims to strengthen capacities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The act includes a European Cybersecurity Alert System, composed of interconnected security operation centres across the EU, and a comprehensive Cybersecurity Emergency Mechanism to improve the EU's cyber resilience.

DORA became binding in January 2025 for all financial entities across the EU. DORA is a harmonised and comprehensive regulatory framework on digital operational resilience. ENISA signed a multilateral MOU with the ESAs (EBA, EIOPA and ESMA) in June 2024 to strengthen cooperation and information exchange on tasks of mutual interest, which includes policy implementation. This agreement will also help support regulatory convergence and consistency across MS, to reinforce the cybersecurity resilience needed for such essential services in, for example, financial entities.

EUDI Wallet

In line with Regulation (EU) 2024/1183 to establish the EUDI framework, the Commission requested ENISA's support for the certification of the EUDI Wallets, including the development of a candidate European cybersecurity certification scheme in accordance with the Cybersecurity Act (Regulation (EU) 2019/881).

The Commission's request addresses two main work strands. First, it calls for ENISA to support the establishment of national MS certification schemes by providing harmonised certification requirements under the European digital identity framework. In addition, ENISA will be involved in the preparation of the relevant implementing acts, establishing a list of reference standards and, where necessary, specifications and procedures for the purpose of expressing detailed technical specifications of those requirements (addressing primarily security and privacy aspects). Secondly, it requests ENISA to launch the preparation of a candidate European cybersecurity certification scheme for the EUDI Wallets and their eID schemes under the Cybersecurity Act.

Vulnerability disclosure

ENISA expanded its support to EU CSIRTs for CVD and was authorised as a CNA.

Based on its mandate to foster cybersecurity resilience in the EU single market, ENISA worked more actively on developing mechanisms to encourage the use of CVD practices. ENISA promoted CVD and supported EU CSIRTs in the adoption and development of CVD policies at the national level. For this purpose, the agency published guidelines, recommendations and analyses. Many MS have already successfully implemented CVD policies.

ENISA is expanding its CVD support to MS with its new role, offering a vulnerability registry service. After onboarding as a CNA, the agency was authorised to assign CVE Identifiers (CVE IDs) and publish CVE records for vulnerabilities discovered by or reported to EU CSIRTs, in line with their dedicated coordinator roles.

Memorandum of understanding

In June, the EASs (EBA, EIOPA and ESMA) announced a multilateral MOU to strengthen cooperation and information exchange with ENISA. The MOU sets out the framework for cooperation and exchange of information on tasks of mutual interest, including policy implementation, incident reporting and oversight of critical ICT third-party providers. It will also promote regulatory convergence, facilitate cross-sectoral learning and capacity-building in areas of mutual interest, and information exchange on emerging technologies.

Contribution agreements

In 2022, ENISA was tasked to establish and roll out the implementation of the cybersecurity support action programme, a fund for the provision of cybersecurity services to support MS in reinforcing their preparedness (ex ante), and response (ex post) capabilities. These services are intended to complement efforts at both the national and EU levels to further improve prevention and detection capacities, and strengthen situational awareness and response to large-scale cybersecurity incidents or crises.

In 2024, the agency signed two new contribution agreements with Connect for a total of EUR 15.4 million, for implementation of the cybersecurity support action programme, situational centre and CRA SRP actions for the 2025–2027 period.

2.3. Budgetary & financial management

2.3.1. Financial management

During 2024, ENISA operated with a budget of EUR 26.2 million compared with the 2023 budget of EUR 25.2 million.

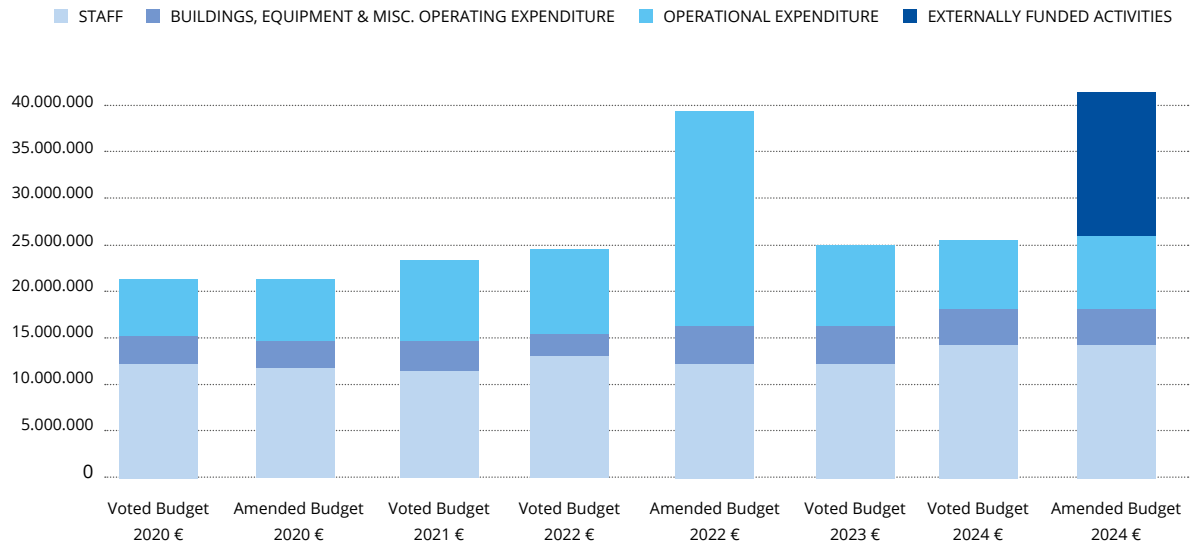
In late December 2023, a contribution agreement between Connect and ENISA was signed, granting a total of EUR 20 million for implementation of cyber support and situational centre actions during 2024–2026. The first instalment amounting to EUR 16 million was received in February 2024 for implementation of the agreed actions.

In December 2024, two new contribution agreements between Connect and ENISA were signed, granting a total of EUR 15.4 million for implementation of cyber support, situational centre and CRA SRP actions during 2025–2027.

During the 2020–2024 period, the EU budgetary contribution (including European Free Trade Association funds) for ENISA increased from EUR 21.1 million to EUR 26.2 million (or by 24 %).

Over this five-year period, ENISA improved its commitment rate from 97.35 % to 100.00 %.

BUDGET EVOLUTION 2020-2024: VOTED/AMENDED BUDGET



In 2024, in addition to the 78 very low-value contracts with direct award (less than EUR 15 000), ENISA concluded 14 public procurement procedures: six using the open procedure (43.0 %), seven through reopening of competitions under framework contracts (50.0 %) and one through a negotiated procedure for medium- and low-value contracts (7.0 %). No restricted procedures were launched.

In 2024, the agency did not pay any interest on late payments.

The table below shows ENISA's budget implementation targets and achievements in 2024, which remained at the same level as 2023.

AREA	OBJECTIVE	2023 LEVEL OF COMPLETION	2024 TARGET	2024 LEVEL OF COMPLETION
Budget implementation (appropriations committed through the year)	Efficiency and sound financial management	100.00 %	95 %	100.00 %
Payments against appropriations of the year (C1 funds)	Efficiency and sound financial management	83.86 %	80 %	83.05 %
Payments against appropriations carried over from previous year (C8 funds)	Efficiency and sound financial management	96.14 %	95 %	96.19 %

2.3.2. Budget execution of EU subsidy (C1 funds of current year 2024)

From 1 January to 31 December 2024, ENISA executed EUR 26 218 721 in commitment appropriations, representing 100.00 % of the total budget for the year, and EUR 21 775 888 in payment appropriations, amounting to 83.05 % of the total budget.

Compared with 2023, commitment execution was maintained at the same high rate – 100.00 % in 2024, compared with 100.00 % in 2023 (99.93 % in 2022). Overall payment execution decreased very slightly to 83.05 % (compared with 83.86 % in 2023).

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 2024 were carried forward to 2025.

The tables on next page summarise the execution of the budget in 2024.

2024 BUDGET IMPLEMENTATION (FUND SOURCE C1)						
AREA OF BUDGET ALLOCATION	APPROPRIATION AMOUNT (EUR)	COMMITMENT AMOUNT (EUR)	PERCENTAGE COMMITTED	PAYMENT AMOUNT (EUR)	PERCENTAGE PAID	AMOUNT CARRIED FORWARD TO 2024 (EUR)
	(1)	(2)	(2) / (1)	(3)	(3) / (1)	(2) - (3)
Title I	14 44 054	14 440 149	99.99%	13 555 811	93.87%	884 338
Title II	4 198 301	4 198.295	100.00%	2 536 755	60.42%	1 661 539
Title III	7 580 447	7 580 278	100.00%	5 683 321	74.97%	1 896 957
TOTAL	26 219 801	26 218 721	100.00%	21 775 888	83 05%	4 442 833

2.3.3. Amending budget / budgetary transfers

According to Article 26 of ENISA's applicable financial rules, 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 limit, the proposed transfers will be deemed to be adopted.

In 2024, ENISA received the first instalment of EUR 16 million for the activities agreed under the contribution agreement signed on 21 December 2023 between Connect and ENISA with the purpose to implement the 'Preparedness and incident response support for key sectors' action under the DEP during 2024–2026. In order to ensure transparency of externally funded projects, Title 4 was established by the MB decision on Amending Budget 1/2024 of 7 June 2024. The received amount of EUR 16 million was accounted as R0 funds under the newly established Title 4.

During 2024, ENISA's budget was increased by a total of EUR 383 000 as part of EU general budget amendments No 4 and No 5: a part of the provided resources (EUR 139 000 and two FTEs) stem from the Cybersecurity Resilience Act [71], which was published in the Official Journal of the European Union on 20 November 2024 and entered into force on 10 December 2024. The other part (EUR 244 326) was allocated to support salary indexation by the decision of the Council in November 2024. The MB decision on Amending Budget 2/2024 of 17 December 2024 was adopted, allocating the additional funding to cover priority projects.

During 2024, the agency made two transfers by Executive Director's decision on the budget (for comparison, the Executive Director also made two transfers on the adopted budget in 2023).

Transfers on the adopted budget included transfer of funds within title and between titles. Funds were moved from Title I and Title III to Title II to finance long-planned corporate ICT related projects, such as ENISA's website revamp, and to ensure business continuity of ICT services and cybersecurity of available devices.

The table on the next page summarises changes to the 2024 budget.

[71] Regulation – 2024/2847 – EN – EUR-Lex.

2024 BUDGET, IN EUR	INITIAL BUDGET	AMENDING BUDGET 1/2024 AND 2/2024	TRANSFERS APPROVED BY THE ED	FINAL BUDGET
Title 1	14 739 106.19	70 000.00	-368 053.07	14 441 053.12
Title 2	3 666 898.43	4 246.00	527 156.52	4 198 300.95
Title 3	7 430 470.72	309 080.00	-159 103.45	7 580 447.27
Title 4		16 000 000,00		16 000 000.00
TOTAL	25 836 475.34	16 383 326.00	0	42 219 801.34

2.3.4. 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 2023 were carried forward to 2024 (C8 appropriations).

In 2024, overall payment execution for C8 funds reached 96.19 %, with payment rates of 86.44 % for Title I, 98.16 % for Title II and 97.03 % for Title III.

Compared with 2023, there is a minor increase in payment execution for implementation of the C8 funds: 96.19 % in 2024 compared with 96.14 % in 2023.

The amount cancelled totals EUR 154 797, which represents 3.81 % of the total amount carried forward.

A large part of the amount cancelled had been provisionally committed to missions, events and pentesting of ENISA assets. This amount had to be modified due to unforeseen circumstances, and to the top-up of schooling allowances, various training sessions, and standby duty expenses which were challenging to estimate, including expenditure for DG Human Resources and Security handling of complaints, DG Budget provision of treasury services, additional security services, Mission Processing System (MIPS) fees, etc.

The table below summarises the execution of the C8 budget per Title in 2024.

IMPLEMENTATION OF C8 FUNDS				
2024 BUDGET (C8) (EUR)	APPROPRIATIONS CARRIED FORWARD FROM 2023 TO 2024 (EUR)	PAYMENT AMOUNT (EUR)	PERCENTAGE PAID	AMOUNT CANCELLED (EUR)
Title 1	464 448.99	401 455.01	86.44%	62 993.98
Title 2	1 338 019.08	1 313 402.24	98.16%	24 616.84
Title 3	2 262 074.64	2 194 888.23	97.03%	67 186.41
TOTAL	4 064 542.71	3 909 745.48	96.19%	154 797.23

2.4. Delegation and sub delegation

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 …' and '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'. In July 2023, the Executive Director adopted a revised decision on a framework for the financial delegation of the authorising officer. This decision sets the financial ceiling applicable to heads of unit and permanent team leaders to EUR 1 000 000 per financial transaction for the budget lines relevant for the performance of their duties and assigned activities or outputs of the SPD. Moreover, Heads of Unit may, with the explicit agreement of the Executive Director, further subdelegate their financial rights to head(s) of sector(s) with a financial limit of up to EUR 500 000 for all relevant budget lines. In 2024, two sub-delegations were granted to two heads of sector. All the delegations and sub-delegations are time-limited. In the event of a change of the person of the Executive Director, all delegations (and sub-delegations) shall become automatically null and void after 90 days from the date the new Executive Director takes up his or her duties, unless the continuation of delegated authority is explicitly confirmed by the newly appointed executive director. Controls on these delegation rights are carried out through a periodic review of the access rights granted to the ABAC system within the main financial system and are shared on an annual basis with the Commission (DG Budget).

2.5. Human resources management

Further to the discussions and consultations during the beginning of the year, on 1 July 2024 the MB endorsed the proposed adjustments of the ENISA structure, in order to consolidate its current activities, increase the agility of the agency to address new upcoming tasks and better equip the organisation to tackle the objectives set in the ENISA Corporate Strategy. All staff were reassigned to the new units and job roles, job descriptions were adjusted in line with the new structure, systems [72] were updated and tested, and process flows and standard operating procedures and guidelines were adjusted. On 1 January 2025 the new organisational structure came into effect.

2024 was the first year the Corporate and HR strategy was completed, where key HR user-centred services were set, with the newly developed strategic workforce planning applied, allowing for improved horizontal talent acquisition. The competency framework of the agency was embedded in the refined recruitment procedures planned and conducted in a timely manner.

The HR team continued to support the operational and administrative goals of the agency in terms of staff acquisition and development. In 2024, ENISA welcomed 26 new staff members: five temporary agents, 17 contract agents (of which 12 contract agents assigned for the activities of the contribution agreement signed in 2023) and four SNEs.

To ensure business continuity of the agency, senior management was enhanced with the appointments of the Chief Cybersecurity Operations Officer the Associate chief Cybersecurity Operations Officer.

Two expansive calls for expression of interest by ENISA in 2024 resulted in reserve lists of 39 candidates for FG IV grade and 41 candidates for AD 6 grade, expected to cater for emerging staffing needs in the next two years.

The further optimisation of the digitalisation of the application procedure and its compliance with case law took place. The sharing of reserve lists within the EUAN environment has become common practice. It all started with a pilot in setting up joint vacancy procedures with other EU agencies.

The following table presents the performance of the HR team in 2024.

[72] For example ARES, ABAC, Mission Processing System (MIPS+), the ENISA budget, Sysper, the agency's intranet, TEAMS, OfficeVibe and other applicable systems.

AREA	OBJECTIVE	2023 PERFORMANCE	2024 PERFORMANCE	2024 TARGET
Efficient management of selection procedures	Reduction of time taken to hire (in line with the standard EU HR definition, this is the time frame set from the deadline of the vacancy for candidates to submit applications until the signing of the reserve list by the executive director)	≤ 5 months	4.8 months	≤ 5 months
Turnover of staff	Reduced turnover rate of statutory staff (temporary agents and contract agents)	4.9 %	4.49 %	< 15 %
Staff performance management	Implementation and monitoring of the appraisal and reclassification exercises (launch and completion of the exercises)	100 %	100 %	100 %

2.5.1. Implementing rules adopted in 2024

In response to Commission Decision C(2023) 8630 entering into force on 12 December 2023 on the prevention of and fight against psychological and sexual harassment, and repealing Decision C(2006) 1624/3, the agency requested the Commission to derogate from this decision, awaiting the draft model decision for agencies that will be negotiated by the Standard Working Party. The agency expects that the model decision for agencies will be ready in the course of 2025.

2.5.2. Brief description of the results of the screening/benchmarking exercise

In 2024, ENISA continued to apply the 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 'administrative support and coordination' decreased slightly, to 24 %. A slight increase can be observed in posts under the 'operational' area, estimated to account for 70 % of posts. The remaining 6 % of posts were defined as 'neutral' posts. In the course of the reporting year, staff posts were counted including staff financed by the contribution agreement as well as interims and intra-muros.

2.6. Strategy for efficiency gains

In 2024, ENISA made progress in its commitment towards the continuous improvement on efficiency across its operational and corporate tasks, as highlighted below:

- developed its talent base and thus increased operational capacities, as outlined in its corporate strategy and HR strategy;
- addressed critical HR needs through reprioritisation and externalisation of administrative tasks, including through shared services and partnerships in corporate and administrative areas;
- used internal and external synergies to gain additional resources and use current resources efficiently, in particular through external operational partnerships;
- maximised to the utmost the use of existing budgetary resources;
- further used joint corporate services with other agencies.

ENISA aimed to build partnerships with MS (including by exploring short- and medium-term secondments

and exchanges of staff with relevant national authorities) and strengthen synergies with a number of EUIBAs. This included proposing joint operational objectives and KPIs in the respective work programmes, thus further resorting to external support and mobilising external resources for the benefit of ENISA operational objectives when those were aligned with the objectives of prospective partners.

The agency continued to implement its work programme by systematically using its statutory bodies (NLO network, ENISA Advisory Group) and other statutory groups it was involved in. These groups include: the SCCG as set out in CSA Article 22, the NISD Cooperation Group and its work streams, and the ECATS Article 18 group based on the eIDAS regulation and expert groups created under EU law. Other groups include ENISA's own ad hoc expert groups, which, where appropriate to avoid duplication of efforts, build synergies and conduct peer reviews of the scope and direction of actions undertaken by the agency to implement its SPD outputs, and serve the purpose to validate results.

This is how the agency fulfilled its obligation as outlined in Article 3(3) of the CSA, to avoid the duplication of MS activities and taking into consideration existing MS expertise.

Another example of the agency seeking to achieve efficiency gains was via joint corporate services with other EU agencies, such as the shared services pilot under the EUAN, where ENISA, EIOPA and the European Institute of Innovation and Technology joined forces to provide shared capabilities for the three agencies on HR, procurement and cybersecurity. In addition, ENISA continued its work on cybersecurity risk management services for EU agencies through a combined service offering with CERT-EU that began in 2024 (pilot phase).

In line with the call for agencies to promote the use of shared services, ENISA continued to seek efficiency gains by building partnerships with other EU bodies. For example, it shares some services, including confidential counselling, with Cedefop and provides accounting and data protection services to the ECCC; it also provides cybersecurity support services to a selected set of Agencies within the scope of the EU Agencies Network.

Within the draft programming period 2026–2028, ENISA will continue to develop and review its operational service packages, to ensure internal alignment and synergies between its structural entities.

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

2.7.1. *Internal Audit Service*

In 2024, the Internal Audit Service (IAS) issued its audit report on procurement and contract management in ENISA. Overall, the IAS concluded that ENISA's governance, risk management and control systems for procurement and contract management activities were adequately designed, efficiently and effectively implemented, and support the agency in achieving its business objectives. That being said, the IAS identified three audit findings (one was assessed as a very important priority and the two others as important). All three underlying corrective actions were submitted for IAS review, of which two were shared by the end of 2024 and the last one in March 2025.

Moreover, the IAS performed ENISA's risk assessment in late 2024 with a view to produce the strategic internal audit plan, which will determine the potential audit topics for the next audit cycle (2025–2027). The IAS shared the strategic internal audit plan with ENISA in March 2025.

2.7.2. *European Court of Auditors*

In October 2024, the ECA issued its report on the 2023 annual accounts of the agency [73]. According to ECA, the accounts of the agency for the year ending 31 December 2023 fairly present the financial position of ENISA at this date. The results of its financial operations, its cash flows and the changes in net assets for that year are in accordance with the financial regulation applicable and with the accounting rules adopted by the Commission's accounting officer. Moreover, the revenue underlying the accounts for the year ended 31 December 2023 is legal and regular in all material respects.

However, the ECA issued a qualified opinion on the legality and regularity of payments underlying the 2023 annual accounts. Following MS' revised requests for cybersecurity support from ENISA at the beginning

[73] https://www.eca.europa.eu/en/publications/SAR-AGENCIES-2023.

of 2023, the ENISA MB adopted a decision to make an However, the ECA issued a qualified opinion on the legality and regularity of payments underlying the 2023 annual accounts. In August 2022 in the wake of the war at Ukraine, ENISA was granted an additional EUR 15 million to increase cybersecurity support at the requests of the Member States, in July 2023. To maximise the impact of this support action, the ENISA MB adopted a decision to exceptionally and temporarily derogate from its financial regulation and, consequently, the corresponding articles of the Framework Financial Regulation. ENISA used this decision as a basis to reassign amounts under a number of individual commitments and their related payment appropriations among the 28 contracts providing the additional cybersecurity support services across the EU. This was duly recorded in ENISA's register of exceptions. However, this exceptional and temporary derogation adopted by ENISA MB has been deemed as irregular by the ECA in its 2023 report. The total irregular payments in 2023 in relation to these reassignments amounted to EUR 1.8 million. This represents 4.1 % of the total payment appropriations available in 2023, exceeding the materiality threshold set for that ECA audit. It is hereby, highlighted that this observation does not apply as such on the regular ENISA budget and it only refers to the budget component availed by means of a contribution agreement.

In 2023 ENISA already took the necessary measures to avoid the recurrence of this exceptional situation and to ensure legal compliance of the implementation of these demand-driven cybersecurity support services, which directly benefit the Member States. In particular, the successor of this cybersecurity support action took the legal form of a formal contribution agreement (for a total maximum value of EUR 20 million with an implementation period ending in 2026) under the Digital Europe Programme signed in December 2023 between DG CNECT and ENISA. This approach is expected to alleviate any legal concerns that impeded the regular implementation of the 2022 cybersecurity support action while at the same time offering greater flexibility to execute operational actions. ENISA is therefore expecting ECA to close this critical audit observation in its 2024 report (to be issued in late 2025).

Moreover, in its 2023 report ECA issued four non-critical observations related to 1) procurement process, 2) late payments, 3) incompatibility of roles and 4) usage of non-staff for initiation of financial transaction. These four observations have been addressed by the agency and their effectiveness shall be assessed by the ECA in its 2024 report.

2.7.3. Ex post control evaluation results

In late 2024, ENISA started to perform its ex post controls of financial transactions made during the 2023 financial year in accordance with Article 45(8) and (9) of the ENISA financial regulation. A total of 155 financial transactions were scrutinised, representing 5.03 % of the agency's financial transactions and 49.64 % of the agency's budget (excluding salaries and related staff expenditure as per the ex post control methodology). Two main weaknesses were identified, neither of which was deemed critical. Two similar weaknesses were identified and further confirmed the findings made by the ECA and the IAS during their previous audits: (1) late payments and (2) lack of adequate documentation supporting payments to ensure a proper audit trail. These two weaknesses were mitigated by (1) the introduction in Q2 2023 of a weekly monitoring of time-to-payment transactions and (2) a revision of the documentation requirements to support the payment of financial transactions (to be implemented in Q2 2025).

2.8a. Follow up of recommendations and action plans for audits and evaluations

Internal Audit Service

No recommendations were opened in 2024, and all recommendations arising from previous internal audits have been formally closed by the IAS in 2023.

European Court of Auditors

The three recommendations arising from previous ECA audits (prior to financial year 2023) have been formally closed by the ECA in 2024.

(74) https://www.europarl.europa.eu/doceo/document/TA-10-2025-0088_EN.html.

2.8b. Follow-up of 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.

2.9. Follow-up of observations from the discharge authority

In May 2025, the Parliament granted 'the Executive Director of ENISA (European Union Agency for Cybersecurity) discharge in respect of the implementation of the Agency's budget for the financial year 2023' and approved 'the closure of the accounts of ENISA (European Union Agency for Cybersecurity) for the financial year 2023.' [74]

2.10. Environmental management

During the course of 2024, the agency worked towards the development of its first environmental statement. To that end, an external verification was successfully concluded in February 2025. The environmental statement presents the data related to the agency's environmental performance in 2021, 2022 and 2023, and highlights the objectives and actions to be implemented to achieve the performance goal, as well as to manage its environmental management in general.

In addition, the agency is fully dedicated to the awareness and training of its personnel in the environmental management issues, while participation in the implementation of the Environmental Management System and other environmental programmes has been enhanced.

Further information on the environmental management of the agency can be found in Annex VII.

2.11. Assessment by management

The agency's operational and corporate activities were implemented in accordance with the 2024 work programme, with the necessary guidance and support of the MB. ENISA conducts its operations in compliance with relevant legal requirements in an open manner via the management team, which monitors the implementation of operational and corporate projects on a weekly basis via the management team meetings.

The agency regularly monitors the implementation of the action plans based on ECA and IAS audit recommendations. In 2024, ENISA implemented corrective actions addressing all the audit recommendations from previous years, and the 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 the underlying controls and control procedures performed by agency staff and supported by the assessment of the effectiveness of the internal control framework presented below. ENISA's management has reasonable assurance that the internal control components and principles have been followed.

II

PART II (b)

EXTERNAL EVALUATIONS

In 2025 ENISA concluded its second biennial stakeholder satisfaction survey for the period 2023 and 2024 of its work programmes. The results of the second stakeholder satisfaction survey shed much important light on how stakeholders perceive the added value of ENISA's work.

The evaluation concluded that ENISA is providing significant added value and that the outcome of its work is taken up by stakeholders in the immediate to medium term. The survey also sought to assess the satisfaction levels of stakeholders in relation to the way the agency implements its projects, specifically how work is organised and managed its work. The results of which demonstrate that the agency values the input received by validators and that it supports community building.

The mandate of the agency requires that the tasks that it carries out do not duplicate MS activities. Therefore, the fact that 89% of stakeholders surveyed considered that ENISA deliverables do not duplicate or only somewhat duplicate MS activities is justification of ENISA's actions to involve stakeholders in all stages of its work and ensure that the outcomes/ results are fit for purpose. An improvement of 6% from the previous survey conducted in 2023 for the work programme years 2021 and 2022.

Aggregate results:

- Aggregate results for added value 88% (down 4%) and take up 82% (down 3%) were slightly lower in 2023-2024 than the resounding results of 2021-2022.
- Aggregate results for non-duplication with MS activities 89% (up 6%) improved in 2023-24 compared to 2021-2022.
- Aggregate results for how ENISA operates with stakeholders improved in the area of taking onboard stakeholder feedback 94% (up 2%) and facilitating community interaction 96% (up 1%) however how ENISA organized its work and processes 89% (down 6%) compared to 2021-2022.
- Finally trust in ENISA's ability to achieve its mandate increased by 1% to 96% in 2023-2024 compared to 2021-2022.

The survey received strong engagement, with over 186 respondents—an increase of 15% compared to the previous survey—and generated more than 250 comments.

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 Management Board Decision No MB/2019/12 and amending Management Board 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 five 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 Management Board 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 2024, 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.

3.1.1. Assessment of the 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.

To increase the rate of participation in such training, the agency should consider a diversity of training plans/programmes to address different levels of staff knowledge/maturity. Nevertheless, various types of information materials are at the disposal of staff, such as training content and the most up-to-date reports by the Commission's Investigation and Disciplinary Office.

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

The ENISA strategy, adopted in 2020, was reviewed during the reporting period and the MB adopted the new version in November 2024. The revised strategy is a cooperative effort of the Executive Director, the MB and the ENISA Task Force on supporting the review of ENISA's strategy and mandate. For this purpose, input was gathered from the ENISA Advisory Group, the NLO network and ENISA staff.

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

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 via various executive director decisions, notably on specifying the roles and responsibilities of ENISA's structural entities and on a framework of 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. This point was further addressed in 2024 with the introduction of a new competence framework for ENISA.

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, and only minor improvements are needed. As part of its internal controls, the agency regularly reviews and monitors its annual objectives to ensure that pre-set objectives will be reached. While midterm reviews are planned, significant effort is expended on the ex ante evaluation and continuous monitoring of projects through the weekly ENISA management team meetings. In particular, each project starts with an inception, meaning that it passes an assessment by the management team, may be further reviewed for guidance and then finally presented to the management team for closure. This ensures that the management team has a clear view of, and is able to follow up on, the agency's annual objectives throughout the year.

3.1.2. Assessment of the 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. Pre-defined 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. [Indicator 26 on 73% of SPD KPIs met or outperformed target set]

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. Since 2022, a centralised risk management approach has been implemented at the agency level. An enterprise risk management (ERM)

framework was adopted based on the Commission's risk assessment guidance. An IT security risk management framework was also formalised and interlinked with the ERM framework. Based on the frameworks adopted, a risk assessment exercise is conducted on an annual basis (entailing an ERM and an IT security risk assessment). The cross-cutting risks were presented in a corporate risk register, and specific risks in each unit/team were also identified. As regards these assessments, no critical risks were identified in 2024.

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 agency's anti-fraud strategy was updated in 2021 and formally adopted by Management Board Decision No B/2021/5. Within 2024, the revision of the anti-fraud strategy took place and a new action plan was put forward for adoption by the MB within 2025. 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 different 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). The establishment of dedicated committees (the IT Management Committee, the Budget Management Committee and the Intellectual Property Rights Management Committee) further supports change management at the corporate level. In 2024, whereas the Cybersecurity Act, which outlines the mandate and tasks of ENISA, has been complemented with the adoption of the NIS2 and conclusion of legislative negotiations on CRA and CSOA, ENISA Management has revised the establishment of ENISA's internal structures via its decision 2024/10. This revision was further complemented by Executive Director Decision No 63/2024, which further specifies the roles and responsibilities of ENISA' s structural entities. In the context of this structural adjustment, three Task Forces were established by the Executive Director, with a view to engage staff members, managers and that agency's HR in the change management process. Several relevant trainings sessions were also organised to that end. This shows ENISA's capacity 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.

3.1.3. Assessment of the 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, but some improvements are needed, in particular the agency's business continuity plan, which needs to be finalised and tested.

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 2024, leading to the downgrading 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.

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. Recurrent weaknesses identified by internal control tools (such as the registry of exceptions) in recent years have not yet been effectively addressed. In addition, ENISA's internal policies and procedures are not always adequately documented or communicated to staff. For example, from the analysis of the 2024 register of exception, out of 15 non-compliant events (i.e. exceptions), the vast majority (11) concerned a posteriori transactions (i.e. the budgetary or legal commitments were not compliant to proceed forward with the transaction). This weakness was identified by previous control activities, but no specific procedure was introduced to further mitigate this usually minor risk.

Nevertheless, none of the 15 identified exceptions was assessed as being of high risk (13 were assessed as low risk and two as medium risk) and only four exceptions were deemed to be of material relevance. Out of these four exceptions, two were related to non-compliance with the contractual terms for the supply of services (i.e. 1) price indexation required by national laws was not foreseen in the original contract and 2) contract extension was not formally signed), one was related to a late budgetary commitment (a posteriori transaction) and the last one was related to non-compliance with procurement rules.

3.1.4. Assessment of the 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 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 the compliance with 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. There is transparency in the agency regarding objectives, challenges, actions taken or to be taken and results achieved. Minutes of the weekly management team meeting are made available by email to all staff. In addition, frequent question-and-answer sessions for all staff on various relevant topics were held during 2024. Midterm reviews are used to communicate objectives achieved and ongoing, and substantial effort is put into ex ante evaluation of the projects, starting with a detailed inception presentation during management team meetings. The same projects may then be reviewed for guidance during management team meetings and are then presented to the management team for finalisation. This ensures that the management team has a clear view of and is able to follow up on the annual objectives throughout the year. Moreover, there is a separate communication line for whistleblowing arrangements. The basic principles, relevant definitions and the reporting mechanism are described in ENISA's Management Board Decision No MB/2018/10 on whistleblowing.

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. Moreover, ENISA has an up-to-date communication strategy and stakeholder strategy in place.

3.1.5. Assessment of the 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.

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 demonstrated.

3.2. Conclusions of the assessment of internal control systems

Weaknesses identified by ENISA's internal and external auditors, respectively IAS and ECA [75], are duly taken into account when assessing ENISA's internal controls. In its 2024's assessment, ENISA concluded that appropriate corrective actions have been internally

implemented to address the audit observations raised by IAS and ECA. In particular, the implementation of the enhanced cybersecurity support action which originally triggered the 2023 ECA's qualified opinion on the legality and regularity of payments [76] is, since late 2023, governed by a contribution agreement signed between DG CNECT and ENISA. This formal agreement adequately removed any legal barrier impeding a smooth and efficient operational deployment of the cybersecurity support action in order to best meet the requests and needs of the Member States.

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 areas, in order to increase effectiveness and ensure proper implementation of the internal controls in the future.

3.3. 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.

Athens, 30th June 2025

[Signed]

Andreas Mitrakas
Head of Unit for Executive Directors Office

[75] For more details, please see also section "2.7. Assessment of audit and ex post evaluation results during the reporting year"
[76] For more details, please see also section "2.7.2. European Court of Auditors"

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, management has sufficient assurance that ENISA is adequately managed so as to safeguard its financial resources and to pursue the tasks which it was entrusted with.

4.2. Reservations

Considering the results of the 2024 annual audits performed by the ECA and the IAS, the 2024 results of the internal controls (ex post controls, review of the register of exceptions, the internal controls framework assessment) and the 2024 results of the key financial and operational indicators, the authorising officer can conclude that ENISA operated in 2024 in such a way as to appropriately manage the risks.

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 [77] 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 Internal Audit Service and the lessons learnt from the reports of the Court of Auditors 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, 30th June 2025

[Signed]

Juhan Lepassaar
Executive Director

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

A

ANNEX I

CORE BUSINESS STATISTICS

Activity 1. Providing assistance on policy development

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction [78]	Biennial (survey)	> 90 %	90 %
Nº of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	30	37
Nº of EU policies supported by ENISA	Annual (internal report)	5	6
Nº of contributions to policy development activities (reports, papers, opinions, participation in workshops, etc.)	Annual (internal report)	30	37

Activity 2. Supporting implementation of Union policy and law

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction [79]	Biennial (survey)	> 90 %	92 %
EU register for digital entities is used by all MS	Biennial (survey)	Used by all MS	N/A – in production from 2025
CVD guidance is implemented by MS and all MS are on the CVD map	Biennial (survey)	Used by all MS	N/A – map pending ENISA website update
Nº of stakeholders involved in the NIS360	Annual (internal count)	120	1 480
Nº of sectorial situational awareness reports	Annual (internal count)	12	24
Nº of critical sectors with a high level of cybersecurity maturity (NIS sector 360)	Annual (internal count)	4	4 (electricity, banking, telecom, core internet)
Number and frequency of services delivered to NIS sectors according to the maturity of the sector	Annual (internal count)	24	28 services + 8 workflows

[78] Stakeholder satisfaction survey conducted every two years to measure the uptake of results/outcomes, added value, duplication of ENISA work, etc. by stakeholders.

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

Activity 3. Building capacity

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	90 %	92%
Maturity of national cybersecurity strategies, ISACs, SOCs, etc.	Annual (report)	N/A	N/A
Stakeholder satisfaction	Biennial (survey)	90 %	**95.5 %**
Evaluation of capacity-building measures by participants in exercises and training	Annual (report)	> 50 % high use-fulness	**52.5 %**
Nº of participants in training sessions organised by ENISA	Annual (report)	> 500 (including online training)	**~ 5 000**
Nº of participants in training and in challenges organised by ENISA	Annual (report)	> 1 000 (including online training)	> 2 047 (1 970 self-paced operational trainings + 77 in three learning and training events)

Activity 4. Enabling operational cooperation

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	> 90 %	88%
Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)	N/A	99.95 % up time
Continuous use and durability of platforms (including prior to and during large-scale cyber incidents)	Annual (report)		Not yet launched in 2024
Nº of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA	Annual (report)	> 5 % increase	
CSIRTs active users, % increase year-on-year			+ 27 %
CSIRTs number of exchanges/interactions, % increase year-on-year			+ 35.46 %
EU-CyCLONe active users, % increase year-on-year			+ 14.55 %
EU-CyCLONe number of exchanges/interactions, % increase year-on-year			– 6 %

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

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	> 90 %	88%
Timeliness and accuracy of reports	Annual (survey)	Above 4	4.14 out of 5 for accuracy and 4.21 out of 5 for timeliness
N° of contributing MS and relevant EUIBAs	Annual (report)		EUIBAs: 4 out of 4 (Commission, CERT-EU, EC3 & EEAS) MS: 11 [80] out of 27
N° of new and total partners in the ENISA partnership programme	Annual (report)	10/4	4 new and 10 in total
Percentage of RFI answered by members of the partnership programme	Annual (report)	80 %	84 %

Activity 5b. Contribute to cooperative response at the EU and Member State levels through *ex ante and ex post* services provision

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
% of MS requesting the service Satisfaction score [81]	Annual	50 % > 4	81.5 % N/A see relevant footnote
% of MS requesting the service Satisfaction score [82]		50 % > 4	44 % N/A see relevant footnote
% of MS requesting the service Satisfaction score [83]		50 % > 4	30 % N/A see relevant footnote
% of MS requesting the service Support was provided promptly Satisfaction score [84]		50 % > 4	55.5 % N/A see relevant footnote

[80] Contribution to JCAR.

[81] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.

[82] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.

[83] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.

[84] Evaluation results will be provided at the end of the action in 2026, therefore annual measurement will not be provided until then.

Activity 6. Development and maintenance of the EU cybersecurity certification framework

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	75 %	72%
Nº of opinions of stakeholders managed	Annual (report)	100 opinion items per scheme	27 MS and the Commission delivered through ECCG [85]
Nº of people/organisations engaged in the preparation of certification schemes	Annual (report)	At least 20 AHWG members from third-party experts; at least 15 MS joining AHWG	EUCS scheme: 17 EU5G: 25 EUDI Wallet: 25 MS: 15
ENISA response to consolidated monitoring and maintenance requirements of schemes adopted	Triennial (survey)	75 %	N/A
Satisfaction of ENISA's role in NCCA peer reviews	Triennial (survey)	75 %	N/A
Feedback from statutory bodies including NCCAs on ENISA's role	Biennial (survey)	75 %	72%
Users satisfaction concerning the certification website services	Annual (survey)	75 %	N/A [86]
Usage of certification website	Annual (report)	75 %	N/A [87]

Activity 7. Supporting the European cybersecurity market and industry

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	60 %	67 %
Cybersecurity market analysis; cybersecurity product and services analysis; analysis on vulnerabilities and dependencies in ICT products and services as appropriate; analysis of other relevant market areas	Annual (report)	All reports produced as planned	One report delivered on MSS [88]
Reports on analysis of standardisation aspects on cybersecurity including cybersecurity certification.	Annual (report)	All reports produced as planned	One report delivered on MSS [89]

[85] Indicator to be reconsidered going forward.

[86] Annual survey postponed in 2024.

[87] Figures not available

[88] Pending publication of the 'MSS market analysis' report.

[89] Pending publication of the 'Digital Identity Standards – Analysis of current situation in standardisation related to the EU Digital Identity Framework Regulation' report.

Activity 8. Knowledge on emerging cybersecurity challenges and opportunities

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	> 5 % compared with 2023	98 %
Uptake of the cybersecurity index	Biennial (survey)	20 MS representatives 60 % satisfaction rate Agreement by all validating bodies	27 MS were represented in the 2024 EU-CSI 88% All validating bodies (NIS CG, COM) agreement on NIS2 Article 18 report
Nº of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	± 5 % compared with 2023	1 012 challenges, recommendations and security controls identified (ENISA Threat Landscape 2024)
Uptake of reports generated in Activity 8	Annual (report)	± 5 % compared with 2023	88 %
EU incident reporting maturity	Annual (report)	EU Average > 50 %	'Incident reporting implementation' indicator: 60.43 % 'Establishment of a national reporting scheme for major cyber incidents' indicator: 69.27 %
Nº of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	± 5 % compared with 2023	NIS (17) eIDAS (7) European Electronic Communications Code (9 – to be published in 2025)
Uptake of reports generated in activity 8	Annual (report)	± 5 % compared with 2023	88 %
Nº of recommendations, analyses and challenges identified and analysed (reports)	Annual (report)	± 5 % compared with 2023	62 for the 'Generative AI' report (to be published in 2025) 10 for the updated 'Foresight 2030 Threats' report 471 for space threat landscape (to be published in 2025)
The influence of foresight on the development of ENISA's work programme	Biennial (ENISA SPD)	> 2 emerging areas identified	10 areas identified
Uptake of reports generated in activity 8	Annual (report)	± 5 % compared with 2023	88 %

Activity 9. Ooutreach and education

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	> 1 % increase (from previous year – decrease in duplication)	87 %
Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics			
Total social media impressions	Annual (report)	> 5 % increase	464 900
Total social media engagement			506 000
Total video views			N/A
Total website visits			9 967
Total participation at events			16 events (total of ~ 800–1 000 participants)
N° of download of materials and overall use of AR tools (i.e. AR-in-a-Box and SME tool	Annual (ENISA website)	> 4 000 per semester	SME Maturity Tool: 1 610 visitors, 10 745 pageviews AR-in-a-Box: 2 725 visitors, 68 694 pageviews, 4 352 downloads
N° of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics	Annual (report)	> 5 % increase	C-Days Portugal (~ 70 people) Cyber 4.0 Conference (~ 500 people) NCC Cyprus (~ 70 people) 1st Awareness Conference (~ 250 people) Cyber Bazaar – NCCs LT, EE, LV (~ 250 people)
Staff satisfaction with international coordination	Annual (survey)	> 80 %	N/A [90]
N° of international engagements	Annual (report)		156 engagement requests, 112 engagements approved, 44 declined
Total n° of students enrolled in the first year of the academic programmes	Annual (cyberhead platform)	1–2 % increase	9 765
Student gender distribution (% female: % male)			79% male / 21% female
Total n° of cybersecurity programmes			162
N° of master's degree programmes			37
N° of bachelor's degree programmes			125
N° of entities included in ECSF registry (i.e. number of MS adopting ECSF, number of ECSF implementations/ pledges)	Annual (register of activities)	30 % of MS to adopt ECSF, At least 15 organisations to have endorsed ECSF	14 MS adopted or endorsed ECSF at the national level

[90] The internal survey was postponed. However, the work undertaken within the output was endorsed by the management team during the closure of the project for the year.

Activity 10. Advise on R & I needs and priorities

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Stakeholder satisfaction	Biennial (survey)	> 90 %	91 %
Evaluation of the trends, wild cards and weak signals on emerging cybersecurity challenges leading to R & I needs and priorities	Annual (annual work programme)	3	20 trends identified in the ENISA foresight study
Number of contributions to EU funding programmes	Annual (reports)	5	10/17 ENISA proposals in the DEP 2025–2027 WP

Activity 11. Performance and sustainability

ACTIVITY INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Proportion of SPD KPIs meeting targets	Annual	> 80 of indicators outperformed	73% [91]
Results of Internal control framework assessment	Annual	Effective (Level 1/2)	Effective (Level 2)
High satisfaction with essential corporate services in the area of compliance and coordination	Annual	> 60 %	75 %
EU Eco-management and Audit Scheme (EMAS) established	Annual	Adopted by end 2024	EMAS audit conducted on 27/2/25
Agency IT strategy aligned with corporate strategy Proportion of total IT budget allocated to information security proportional to the level of risks across various IT systems within the agency	Annual	Revised IT strategy by 2024 20 % by 2024	Revised IT strategy proposal submitted end 2024; strategy to be adopted by Q2 2025 18 % of total IT costs

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Efficiency and effectiveness of project management procedures and tools (survey)	Annual	> 80 %	77 % Survey results were used to recalibrate the internal processes and planning for increased efficiency

[91] Of the 149 indicators 37 met and 72 outperformed the target set, whilst 23 underperformed, 10 where postponed and 5 found not applicable

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Nº of high risks identified in annual risk assessment	Annual	≤ 3	3
Percentage of identified internal controls deficiencies addressed within timelines		100 % for critical, 80 % for major, 60 % for moderate	No critical recommendation issued in 2023 ICF assessment. Out of 3 moderate and 2 major – the recommendations remain valid as the deficiencies have not been fully mitigated
Nº of complaints filed against ENISA / number of identified legal or regulatory breaches		≤ 3	4 complaints; 2 identified breaches
% of revised and up to date corporate rules (MBD, EDD, policies, processes)		60 % corporate rules which have not been reviewed less than three years ago; 80 % corporate rules which have not been reviewed less than four years ago	23 MBDs on corporate rules from before 2019
MOU with Greek authorities for carbon dioxide reduction in ENISA HQ in place		MOU process initiated by the end of 2024	Process has not started
Efficiency and effectiveness of ITMC/BMC processes (survey)		> 60 %	ITMC: 75 % BMC: 63 %
Percentage of identified high risk mitigation measures addressed within timelines	Annual	90 %	All high risks addressed within timelines and/or accordingly reported and planned
Cybersecurity training session for staff and managers	Annual	At least two trainings per year	Two training sessions by ISO; training programme and phishing exercise (via dedicated training platform)
Satisfaction within the EU agency network with ENISA support services	Annual	> 80 %	High satisfaction expressed by the agencies that received ENISA's services
Percentage of staff considering that the information they need to do their job is easily available/ accessible within ENISA	Annual	55 %	66 % of staff survey respondent agree that ENISA's internal communication is timely and clear (result of last year was 39 %)
Response timeliness to external parties (internal reporting)	Annual	48h	High response rates in accordance with ENISA's code of conduct

Activity 12. Reputation and trust

ACTIVITY INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Level of trust in ENISA (as per the biennial stakeholder survey)	Biennial	95%	96 %
High satisfaction with essential communication and assistant services	Annual (MT survey)	60 %	63%
High satisfaction with demand-driven communication and assistant services	Annual (MT survey)	60 %	50%
Limited disruption of continuity of internal and external communications	Annual (business continuity plan)	Target set in business continuity plan and agreed response time objectives	6–12 hours (before reaching maximum tolerable downtime) for ENISA's website

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
N° and types of activities at each engagement level (stakeholder strategy implementation)	Annual (internal report)	N/A	Total engagements: 391 40% Partner 11% INVOLVE/ ENGAGE 18% Consult 31% Inform
N° of social media engagement	Annual (media monitoring)	> 80 000	66 300
Stakeholder satisfaction with ENISA outreach	Biennial (survey)	> 80 %	96%
N° of total ENISA website visits	Annual (website analytics)	> 2.5 million	2.3 million
Staff satisfaction with the quality and timing of ENISA internal communications [92]	Annual (survey)	> 50 %	65 %
N° of feedback received per NLO consultation	Annual (Internal report)	> 2	27 for NLO subgroups (3.6 as average for validations in NLO Network)
Number of feedback received per AG consultation	Annual (Internal report)	> 2	11.3 average
Satisfaction of statutory bodies with ENISA support to fulfil their tasks as described in CSA	Annual (survey)	> 80 %	97%
Satisfaction of statutory bodies with ENISA portals	Annual (survey)	> 80 %	83%

[92] The question in the 2024 staff satisfaction survey was phrased slightly differently.

Activity 13. Effective and efficient corporate services

ACTIVITY INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Implementation of Strategic Workforce Plan / Strategic Workforce Review decisions	Annual	Fully implemented	The workforce is assessed on an annual basis. The exercise concluded with ED Decision No 21/2024. Implementation was partially realised and will be embedded in the 2025 exercise.
Implementation of the Corporate and HR strategy	Annual	Actions implemented according to the timelines	Vacated staff posts in 2024 were fulfilled within 143 days. The indicated KPI was to fulfil posts within 300 days
High participation in the staff satisfaction survey	Annual	75 %	80 %
Understand best practices in sustainable IT solutions Limited disruption of continuity of corporate services Handling EUCI at the level of SECRET UE / EU SECRET	Annual Annual By Q2 2024	IT strategy updated accordingly Business Continuity Plan for corporate IT, facilities, financial and HR services ensured has been accredited	In 2024, the IT sector further implemented the ITIL best practices such as: consolidated database of the IT assets has been implemented, IT service management, IT requests and IT incidents). Further deployment of Zerotrust principles and adoption of key policies, such as a helpdesk policy and a smartphone policy. Implementation of a mobile device management solution for managing all mobile devices. Effective disaster recovery is in place to ensure the Business Continuity Plan of core services. EUCI inspection took place and the report will be sent in 2025.

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Turnover rates	Annual	3 %	4.1 %
Establishment plan posts filled		> 95 %	98 %
Time from vacancy announcement to candidate selection		< 300 days	143 days
Percentage of the implementation of the approved recruitment plan		> 90 %	94 %
Percentage of the implementation of the approved procurement plan		> 90 %	63.63 %
Percentage of procurement procedures launched via e-tool (PPMT)		> 90 %	100 % (for open, restricted and middle value procedures)
Percentage of budget implementation		> 95 %	100 %
Average time for initiating a transaction (FIA role)		< 7 days	7.51
Average time for verifying a transaction (FVA role)		< 3 days	0.19
Nº of budget transfers		< 4	2
Late payments		< 8 %	7.4 %
Nº of policies/IR revised or adopted	Annual	> 1	L & D; reclassification; SSS, amendment EP; schooling; travel missions, trainees, VN & competences, restructuring decisions, mobile phone, parking; appraisal admin note, EDD decision on gifts and dinners
Nº of processes reviewed/redesigned		> 1	Postponed [93]
Percentage of staff satisfaction survey with talent development		> 50 %	52 %
Percentage of actions implemented as follow up on staff satisfaction survey results and implemented on time		> 95 %	Partially postponed in 2024 [94]
Nº of implemented competency-driven training and development activities		> 1	All training sessions are linked to key competences of ENISA and connected with the CDR
Nº of multisource feedback evaluations implemented and followed up		> 5	16 360 ° for HoU, HoS and TLs; and 12 360 ° SM for contract renewals

[93] Due to unavailability of budget, no new digital solutions were introduced in 2024.

[94] Due to unavailability of critical HR staff in 2024, the follow up actions for staff satisfaction survey were decentralised in 2024 to the relevant head of unit. However, HR coordination was initiated following the October 2024 staff survey, the results of which will be submitted in the 2025 AAR.

OUTPUT INDICATOR	FREQUENCY (DATA SOURCE)	TARGET 2024	RESULT 2024
Satisfaction survey for working environment	Annual	80 %	N/A [95]
Safety and security incidents reported at workplace in any of the 3 ENISA offices		< 3	Zero cases
Average time for dealing with facilities management requests		< 3 days	2 days
Resilience and quality of ENISA IT systems and services (automated or via surveys). Specific KPIs will be defined for each expected result of the output and will be monitored separately. Generic indicators: • Critical systems uptime/downtime • Staff satisfaction with resolution	Annual	99 % 85 %	99.89 % N/A (not part of ENISA survey in 2024). ENISA used the ServiceNow ticketing system (from April to December of 2024), whose results are: Percentage of major IT helpdesk requests resolved in a satisfactory way within two business days: 82.53 %

[95] This indicator was not measured due to the fact that this indicator is measured biennially and therefore will be measured again in 2025.

A

ANNEX II

STATISTICS ON FINANCIAL MANAGEMENT

Budget outturn and cancellation of appropriations (in EUR)

BUDGET OUT-TURN	2022	2023	2024
Reserve from the previous years' surplus (+)			
Revenue actually received (+)	39 227 392	25 293 934	42 473 035
Payments made (–)	– 20 396 780	– 21 118 392	– 25 690 066
Carryover of appropriations (–)	– 18 836 095	– 4 228 452	– 16 945 798
Cancellation of appropriations carried over (+)	248 745	149 739	154 797
Adjustment for carry-over of assigned revenue appropriation from previous year (+)	33 743	53 469	163 909
Exchange rate differences (+/–)	– 17		
Adjustment for negative balance from previous year (–)			
TOTAL	**276 988**	**150 298**	**155 877**

Execution of commitment appropriations in 2024

N EUR	CHAPTER	COMMITMENT APPROPRIATIONS AUTHORISED (*)	COMMITMENTS MADE	% COMMITMENT RATE
A-11	Staff in active employment	11 023 274	11 023 274	100.00%
A-12	Recruitment/departure expenditure	265 321	265 321	100.00%
A-13	Socio-medical services and training	1 034 063	1 033 886	99.98%
A-14	Temporary assistance	371 000	371 000	100.00%
TITLE I		**12 693 659**	**12 693 482**	**100.00%**
A-20	Buildings and associated costs	1 188 215	1 171 715	98.61%
A-22	Current administrative expenditure	465 252	453 839	97.55%
A-23	ICT	2 095 952	2 074 447	98.97%
TITLE II		**3 749 419**	**3 700 001**	**98.68%**
B-30	Activities related to outreach and meetings	506 134	490 669	96.94%
B-37	CSA core operational activities	8 398 192	8 358 389	99.53%
TITLE III		**8 904 326**	**8 849 058**	**99.38%**
TOTAL		**25 347 404**	**25 242 541**	**99.59%**

(*) 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 2024

N EUR	CHAPTER	PAYMENT APPROPRIATIONS AUTHORISED (*)	PAYMENT MADE	% PAYMENT RATE
A-14	Temporary assistance	695 428	37 998	5364%
TITLE I		12 024 669	11 348 572	94.38%
A-20	Buildings and associated costs	1 044 795	726 652	69.55%
A-21	Movable Property and Associated Costs	64 137	15 290	23.84%
A-22	Current administrative expenditure	952 915	214 614	22.52%
A-23	ICT	1 873 073	1 055 815	56.37%
TITLE II		3 934 920	2 012 372	51.14%
B-30	Activities related to outreach and meetings	563 440	481 631	85.48%
B-37	CSA core operational activities	8 384 397	6 554 205	78.17%
B-38	Core operational activities – assistance funds	14 353 668	-	0.00%
TITLE III		23 301 505	7 035 836	30.19%
TOTAL		39 261 094	20 396 780	51.95%

Carry forward to 2025 (open amounts as of 31 December 2024)

IN EUR	CHAPTER	COMMITMENTS MADE (*)	PAYMENTS MADE (**)	AMOUNT TO BE PAID IN 2023	% AMOUNT TO BE PAID
A-11	Staff in active employment	9 859 760	9 859 760	-	0.0%
A-12	Recruitment/departure expenditure	287 409	252 896	34 513	12.0%
A-13	Socio-medical services and training	1 181 581	862 918	318 663	27.0%
A-14	Temporary assistance	695 428	372 998	322 430	46.4%
TITLE I		12 024 178	11 348 572	675 606	5.6%
A-20	Buildings and associated costs	1 028 295	726 652	301 643	29.3%
A-21	Movable property and associated costs	64 137	15 290	48 847	76.2%
A-22	Current administrative expenditure	952 259	214 614	737 644	77.5%
A-23	Information and communication technologies	1 851 568	1 055 815	795 753	43.0%

(*) 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).

IN EUR	CHAPTER	COMMITMENTS MADE (*)	PAYMENTS MADE (**)	AMOUNT TO BE PAID IN 2023	% AMOUNT TO BE PAID
TITLE II		3 896 259	2 012 372	1 883 887	48.4%
B-30	Activities related to outreach and meetings	542 365	481 631	60 734	11.2%
B-36	CSA core operational activities	8 366 604	6.554 205	1 812 398	21.7%
B-38	Core operational activities – assistance funds	14 350 000	-	14 350 000	100.0%
TITLE III		23 258 969	7 035 836	16 223 133	69.8%
TOTAL		**39 179 406**	**20 396 780**	**18 782 626**	**47.9%**

Revenue and income during 2024 (in EUR)

TYPE OF REVENUE	ENTITLEMENTS ESTABLISHED	REVENUE RECEIVED	OUTSTANDING AT THE END OF THE YEAR
Subsidy from the EU budget	29 219 801	29 219 801	0
Other contributions	16 000 000	16 000 000	0
Revenue from administrative operations	260 673	253 234	7 439
TOTAL	**45 480 474**	**45 473 035**	**7 439**

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

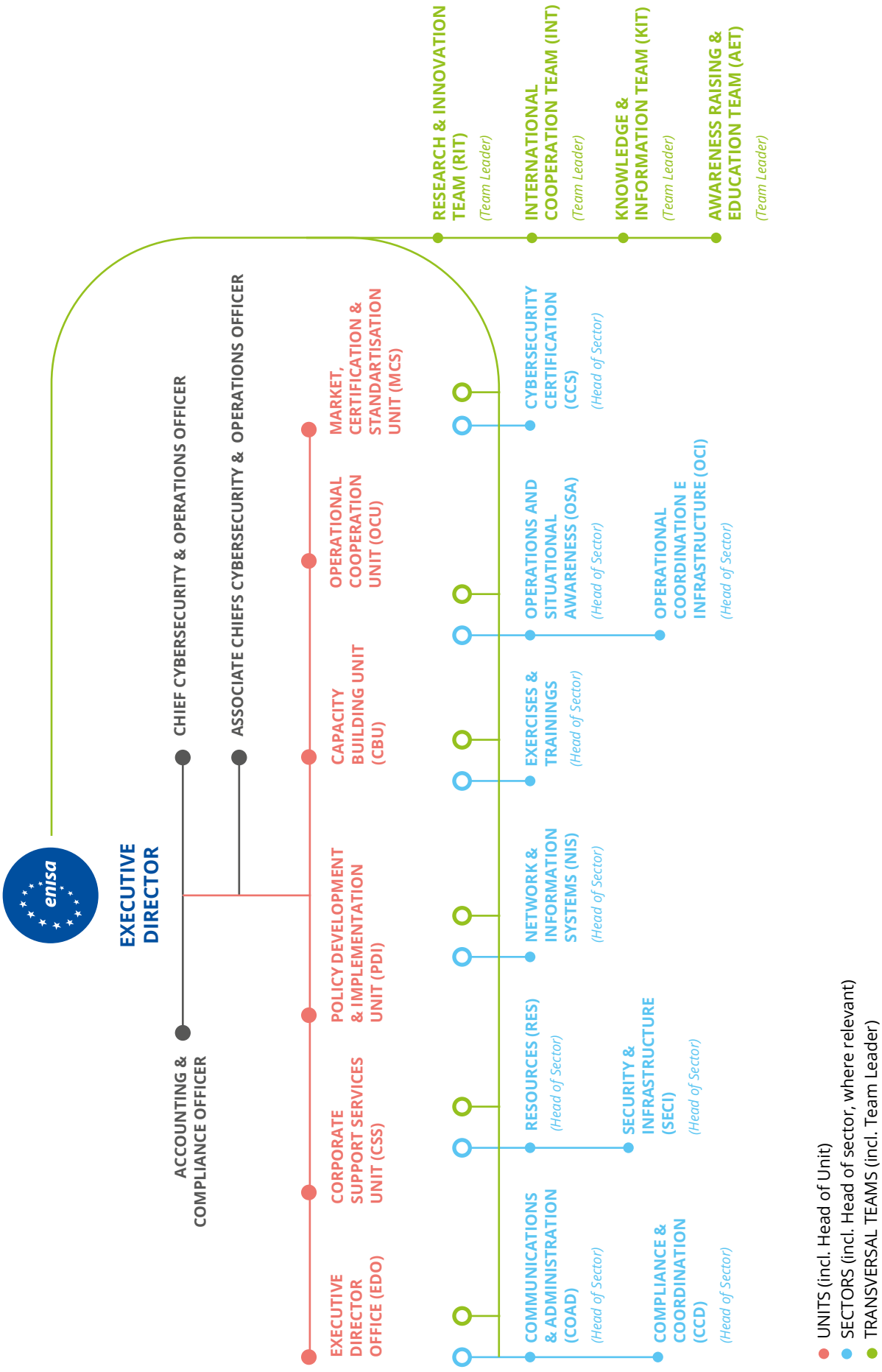
(*) All fund sources are included in the figures.

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
CHIEF CYBERSECURITY & OPERATIONS OFFICER
ASSOCIATE CHIEFS CYBERSECURITY & OPERATIONS OFFICER
ACCOUNTING & COMPLIANCE OFFICER
EXECUTIVE DIRECTOR OFFICE (EDO)
CORPORATE SUPPORT SERVICES UNIT (CSS)
POLICY DEVELOPMENT & IMPLEMENTATION UNIT (PDI)
CAPACITY BUILDING UNIT (CBU)
OPERATIONAL COOPERATION UNIT (OCU)
MARKET, CERTIFICATION & STANDARTISATION UNIT (MCS)
COMMUNICATIONS & ADMINISTRATION (COAD) (Head of Sector)
RESOURCES (RES) (Head of Sector)
NETWORK & INFORMATION SYSTEMS (NIS) (Head of Sector)
EXERCISES & TRAININGS (Head of Sector)
OPERATIONS AND SITUATIONAL AWARENESS (OSA) (Head of Sector)
CYBERSECURITY CERTIFICATION (CCS) (Head of Sector)
COMPLIANCE & COORDINATION (CCD) (Head of Sector)
SECURITY & INFRASTRUCTURE (SECI) (Head of Sector)
OPERATIONAL COORDINATION E INFRASTRUCTURE (OCI) (Head of Sector)
RESEARCH & INNOVATION TEAM (RIT) (Team Leader)
INTERNATIONAL COOPERATION TEAM (INT) (Team Leader)
KNOWLEDGE & INFORMATION TEAM (KIT) (Team Leader)
AWARENESS RAISING & EDUCATION TEAM (AET) (Team Leader)
UNITS (incl. Head of Unit)
SECTORS (incl. Head of sector, where relevant)
TRANSVERSAL TEAMS (incl. Team Leader)

A

ANNEX IV

2024 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT

2024 establishment plan

FUNCTION GROUP AND GRADE	ESTABLISHMENT PLAN IN 2024 VOTED EU BUDGET [96]		POSITIONS FILLED AS OF 31.12.2024	
	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		2
AD 10		4		3
AD 9		14		15
AD 8		15		11
AD 7		13		12
AD 6		7		13
AD 5		1 [97]		
TOTAL NUMBER OF ADS		64		62
AST 11				
AST 10				
AST 9		2		2
AST 8		1		1
AST 7		0		0
AST 6		9		7
AST 5		4		5
AST 4		2		2
AST 3		1		1
AST 2				1
AST 1				
TOTAL NUMBER OF ASTS		19		19
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		81

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

[96] The 2024 Establishment Plan was modified by Management Board Decision No MB/2024/13 of 14 November 2024 to increase two AST 9 slots, applying the flexibility rule set out in Article 38(1) of the Framework Financial Regulation.

[97] A new post has been added to the 2024 Establishment Plan as per Management Board Decision No MB/2024/17 of 17 December 2024 following EU general budget amendment No 4 which, subsequent to the adoption of the CRA, granted ENISA an additional temporary agent post. In 2025, it was confirmed by budgetary authorities that for the EU general budget 2025, this is an AD 8 post.

Information on entry level for each type of post

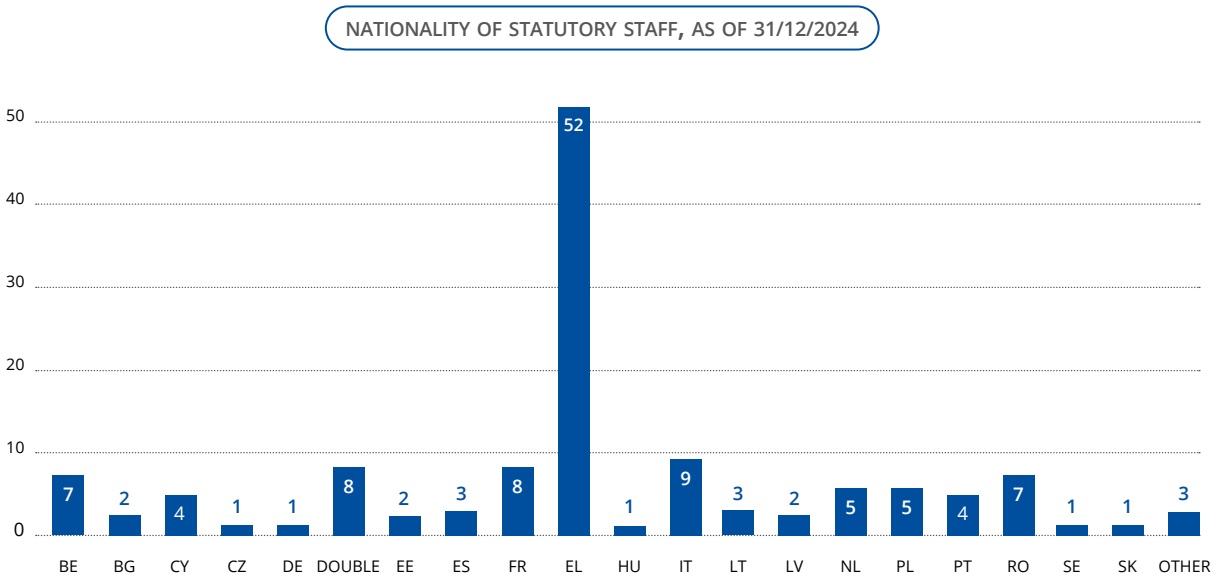
NO	JOB TITLE	TYPE OF CONTRACT (OFFICIAL, TEMPORARY AGENT, CONTRACT AGENT OR SNE)	FUNCTION GROUP / GRADE OF RECRUITMENT	FUNCTION (ADMINISTRATIVE SUPPORT OR OPERATIONS)
	Executive director	Temporary agent	AD 14	Top operations
	Adviser	Temporary agent	AD 12	Administrative
	Head of unit	Temporary agent	AD 9	Administrative/operations
	Head of Sector	Temporary agent	AD 6	Administrative/operations
	Team leader	Temporary agent	AD 7	Operations
	Senior Cybersecurity Expert	Temporary agent	AD 9	Operations
	Cybersecurity Expert	Temporary agent	AD 6	Operations
	Cybersecurity Officer	Contract agent	FG III/IV	Operations
	Officer	Contract agent	FG IV	Administrative
	Assistant	Contract agent	FG III	Administrative/operations
	Assistant	Contract agent	FG I	Administrative/operations
	Coordinator	Temporary agent	AST 6	Administrative
	Cybersecurity Officer	Temporary agent	AST 6	Operations
	Officer	Temporary agent	AST 3	Administrative/operations
	Assistant	Temporary agent	AST 2	Administrative
	Lead certification expert	Temporary agent	AD 12	Operations
	Legal Adviser on Cybersecurity	Temporary agent	AD 6	Operation
	Spokesperson	Temporary agent	AD 6	Administrative
	Legal Adviser	Temporary agent	AD 7	Administrative
	Data Protection Officer	Temporary agent	AD 7	Administrative
	Information Security Officer	Temporary agent	AD 7	Administrative
	Administrator	Temporary agent	AD 8	Administrative
	Accounting	Temporary agent	AD 8	Administrative
	Seconded national expert	Seconded national expert	n/a	Operations

Information on benchmarking exercise

JOB TYPE	2022	2023	2024
TOTAL ADMINISTRATIVE SUPPORT AND COORDINATION	20.97 %	25.76 %	23.69 %
Administrative support	14.19 %	19.05 %	17.69 %
Coordination	6.77 %	6.72 %	6.00 %
TOTAL OPERATIONAL	71.21 %	66.55 %	70.25 %
Total operational coordination	11.05 %	11.27 %	9.69 %
Programme management and implementation	58.39 %	53.64 %	56.06 %
General operational activities	1.77 %	1.64 %	4.50 %
TOTAL NEUTRAL	7.82 %	7.69 %	6.06 %
Finance and control	7.42 %	7.31 %	5.75 %
Linguistic activities	0.40 %	0.37 %	0.31 %

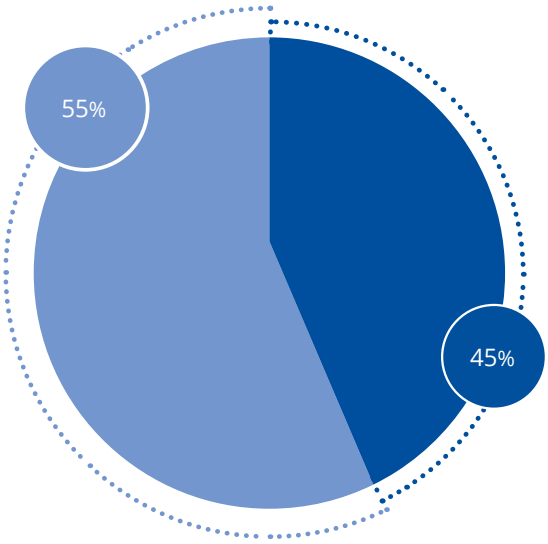
Human resources statistics

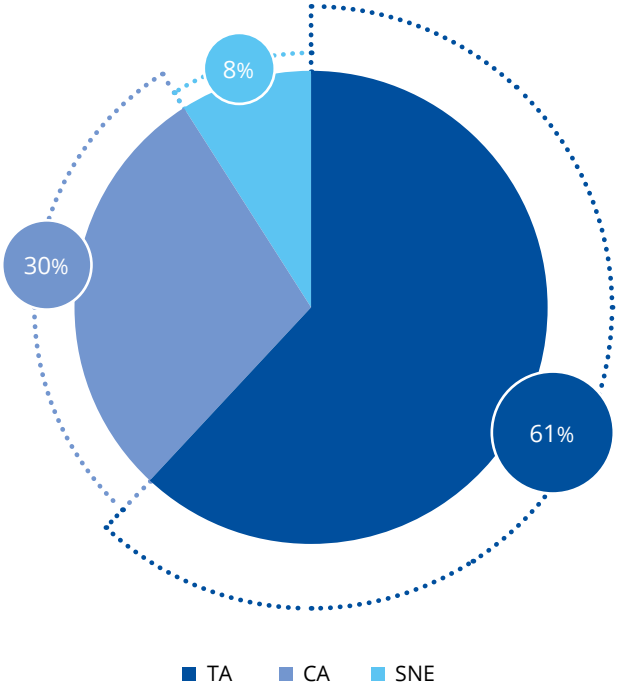
On 31 December 2024, the agency had a total of 121 statutory staff members (temporary agents and contract agents) in-house.



MOST REPRESENTED NATIONALITY	2023		2024	
	Number	%	Number	%
Greek	48/105	45.7	52/121	43.0

GENDER DISTRIBUTION OF STATUTORY STAFF, AS OF OF 31/12/2024





STAFF DISTRIBUTION BY CONTRACT TYPE, AS OF 31/12/2024

MANAGEMENT	2023		2024	
	Number [98]	%	Number [99]	%
Female managers	3	27	2	29
Male managers	8	73	5	71

Implementing rules

MB/2024/11	On the request for the Commission Agreement for derogation from implementing rules to the Staff Regulations related to of Commission Decision C(2023) 8630 final on the prevention of and fight against psychological and sexual harassment anti-harassment

[98] The managers are the Executive Director (1), heads of unit (6) and team leaders (3).

[99] 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	YEAR 2020 (REFERENCE YEAR 2019)	YEAR 2021 (REFERENCE YEAR 2019)	YEAR 2022 (REFERENCE YEAR 2021)	YEAR 2023 (REFERENCE YEAR 2022)	YEAR 2024 (REFERENCE YEAR 2023)	ACTUAL AVERAGE OVER 5 YEARS	AVERAGE OVER 5 YEARS
AD 5	-	-	-	-		-	2.8
AD 6	-	1	1	1	2	3.15	2.8
AD 7	1	-	2	1	3	3.5	2.8
AD 8	2	1	3	1	2	3.9	3
AD 9	-	-	-	2		2.75	4
AD 10	-	-	2	-		10.5	4
AD 11	-	-	-	-		-	4
AD 12	-	1	-	-		10	6.7
AD 13	-	-	-	-		-	6.7
AST 1	-	-	-	-		-	3
AST 2	-	-	-	-		-	3
AST 3	-	-	1			6.75	3
AST 4	1	-	-	1	1	2.76	3
AST 5	-	1	-	1	-	4.05	4
AST 6	1	1	-	-	-	3.5	4
AST 7	-	1	1	1	-	3.92	4
AST 8	-	-	-	-	2	-	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 31.12.2024	STAFF MEMBERS RECLASSIFIED IN 2024 (REFERENCE YEAR 2023)	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
Function group IV	17	3	–	–	Between 6 and 10 years
	16	9	2	-	Between 5 and 7 years
	15	4	-	4.5	Between 4 and 6 years
	14	14	-	3.3	Between 3 and 5 years
	13	3	-	4.2	Between 3 and 5 years
Function group III	11	3	-	-	Between 6 and 10 years
	10	1	2	2	Between 5 and 7 years
	9	2	1	3	Between 4 and 6 years
	8	0	-	4.9	Between 3 and 5 years
Function group II	6	0	-	4.8	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
Function group I	3	-	-	-	n/a
	2	1	-	-	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 2024 for the operational and corporate activities described in Part I of this report is presented in table 5 below. The allocation was determined according to the direct budget and number of FTEs reported for each activity, with the indirect budget being assigned based drivers such as direct FTEs.

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

- The direct budget is the actual cost under for each of the nine operational activities described in Part I of this report in terms of services, goods and missions.
- 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 activity in 2024.
- For the purpose of the allocation of human and financial resources, an Executive Director's Office activity (Activities 11 and 12 as described in Part I) (budget and FTEs), which includes coordination, compliance, communication and administration, was allocated for all of the agency's operational activities.
- For the purpose of the allocation of human and financial resources, the Corporate Support Service activity (Activity 13 as described in Part I), including human resources, IT services, procurement and finance, and facilities and logistics, was allocated for all of the agency's operational activities.

ALLOCATION OF HUMAN AND FINANCIAL RESOURCES	ACTIVITIES AS REFERRED TO IN PART 1	BUDGET ALLOCATION (IN EUR)	FTE ALLOCATION
Providing assistance on policy development	Activity 1	840 266.83	3.29
Supporting implementation of Union policy and law	Activity 2	2 293 362.76	9.90
Building capacity	Activity 3	2 944 951.11	10.83
Enabling operational cooperation	Activity 4	3 103 844.35	8.81
Contribute to cooperative response at Union and Member States level	Activity 5	2 854 659.00	13.22
Development and maintenance of EU cybersecurity certification framework	Activity 6	1 763 664.55	8.13
Supporting European cybersecurity market and industry	Activity 7	998 729.06	5.08
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	1 879 102.03	7.62
Outreach and education	Activity 9	1 633 620.09	8.34
Research and innovation	Activity 10	455 501.81	2.29
Performance and sustainability	Activity 11	2 360 523.21	11.48
Reputation and trust	Activity 12	795 811.95	4.47
Effective and efficient corporate services	Activity 13	4 294 684.64	17.28
TOTAL		26 218 721.39	110.74

A

ANNEX VI

GRANTS, CONTRIBUTIONS AND SERVICE-LEVEL AGREEMENTS

ENISA does not receive any form of grant.

	SLA	DATE OF SIGNATURE	TOTAL AMOUNT	DURATION	COUNTERPART	SHORT DESCRIPTION
1	SLA with ECCC (Activity 9)	20/12/2022	54 604	1 year	ECCC	The scope of this SLA covers support services offered by ENISA to ECCC: Data Protection Officer, Accounting Officer
2	SLA with eu-Lisa M-CBU-23-C35 (Activity 3)	13/7/2023	120 000	31/12/23	eu-Lisa	The scope of this SLA covers support services offered by ENISA to eu-Lisa on the planning, execution and evaluation of upcoming annual exercises
Contribution agreements						
1	Support action fund and situation centre contribution	21/12/2023	Up to EUR 20 million (prefinancing rate 80 %)	Until 31/12/2026	Connect	The purpose of this agreement is to provide a financial contribution to implement the action 'Incident response support and preparedness for key sectors', which is composed of three activities: 1) EU-level Cyber Reserve with services from trusted private providers for incident response; 2) pentests in key sectors, and 3) contribution to the Cyber Analysis and Situation Centre.

Detailed breakdown of contribution agreements planned resource consumption

CONTRIBUTION AGREEMENTS		2024	
Support action fund	**Planned**	**Committed amount (authorised)**	**Payment amount (authorised)**
Budget	EUR 4 703 891.16	5 204 461.11	3 843 160.01
FTE	Head count of FTEs: 10 activity 5.B + 2 activity 5.A	0,41 FTEs activity 5.A and 4,5 FTEs activity 5.B	

SLAs with other EU entities that were active in 2024 (non-income-generated agreement) are as follows:

- with Cedefop for legal services,
- with BEREC for the provision of electronic data backup services,
- with CERT-EU for structured cooperation,
- with CISA on working arrangements,
- with the ECCC on increasing cooperation
- with the European Defence Agency for an establishment of a structured cooperation;
- with the European Defence Agency, EC3 and CERT-EU for cooperation supported by all the parties' respective mandates,
- with the ERA for increasing cooperation,
- with EUIPO for disaster recovery services,
- with eu-LISA on working arrangements,
- with Europol for cooperative relations in order to support MSs,
- with Europol for the EC3 working group on security and safety online,
- with the EASA for a permanent secretariat,
- with the European Food Safety Authority for shared support office under the EU agencies network,
- with the EDPS on increasing cooperation,
- with the JRC on the EU Academy.
- with the NCCC of Ukraine for working arrangements.

A

ANNEX VII

ENVIRONMENTAL MANAGEMENT

While ENISA's overall mandate is to contribute to achieving a high common level of cybersecurity across the EU, the agency bears social and environmental responsibility for its operations and aims to achieve climate neutrality by 2030. It also has an obligation to support the Commission' Green Deal initiative, in line with its SPD objectives and the values set by the MB.

In 2021, ENISA's MB included in the agency's 2022–2024 SPD the objective for ENISA to achieve climate neutrality (defined as zero carbon dioxide, methane and nitrous oxide emissions) across all its operations by 2030.

Starting in 2021 and following the technical study carried out in 2023 to calculate the agency's carbon footprint, the service took several actions to reduce greenhouse gas emissions. With the development and the implementation of the Environmental Management System started in 2024, ENISA has set specific environmental purposes and quantitative targets for the significant environmental implications of the agency, in agreement with the strategies and objectives that are dully monitored.

Through the 2022–2024 SPD, the ENISA MB is committed to implement a more strategic target towards climate neutrality by 2030. The areas for action as set by the Commission for the achievement of the neutrality are:

- More sustainable and durable building and working areas;
- Decrease of emissions from corporate travelling, and increase of the use of more sustainable means of travel;
- Optimisation of functions and information elements;
- Reduce greenhouse gas emissions from digital operations;
- Offsetting remaining emissions with carbon removals;
- Supporting a green and circular economy;
- Preserving and restoring nature and biodiversity;
- Promoting a healthy and sustainable food system.

Throughout 2022, 2023 and 2024, various measures were implemented in view of reducing the ENISA greenhouse gas emissions, including the collection and recycling of office waste based on material made, the installation of a garden irrigation system, and the integration of specific provisions on greenhouse emissions into procurement procedures and tenders.

The measures implemented in the context of reducing ENISA's carbon footprint and its environmental impact include:

- Promoting online and hybrid meetings instead of in-person meetings.
- Replacing conventional light bulbs with new LED technology bulbs in all areas of the building.
- Modifying the air conditioning system and in particular by separating the installations by period of use.
- Intervention in the corridor lighting, and in particular reducing the number of light bulbs on by 1/3.
- Use of recycled paper.
- Enhance digitalisation in view of reducing paper use.
- Introduce 'green features' in ENISA branded items and corporate gifts by using recycled materials.
- Ban of single-use plastics.
- Separate and recycle waste, including batteries.
- Provide glass water bottles and ceramic coffee cups to staff.
- Install filtered water dispensers in all kitchens and meetings.
- Intergrade 'green information' into ENISA's intranet as one important tool to enhance staff engagement in actions.
- Introduce 'green' clauses to reduce greenhouse gas emissions in ENISA's procurement procedures.

In February 2025, the development of the first environmental statement of the agency and the evaluation of an external verification was successfully concluded. The environmental statement presents the data related to the agency's performance in 2021, 2022

and 2023, and highlights the objectives and actions that will be implemented for their achievement, as well as to manage its environmental management in general.

In addition, the agency is fully dedicated to the awareness and training of its personnel in the environmental management issues, while the participation in the implementation of the Environmental Management System and other environmental programs is enhanced.

To achieve the set objectives, it is essential to ensure all ENISA personnel, suppliers, partners and visitors enhance and support the effort to achieve such goals. In addition, the principles of the ENISA Environmental Policy will be communicated to the relevant third parties operating within ENISA's scope and to other interested parties.

ENISA shall take into account the following basic principles regarding its operations and activities:

- The environment has priority in every activity within the financial justified limits.
- Environmental protection must be addressed professionally.
- The implementation of these principles must be regularly reviewed by the Management.
- It is a generic responsibility to ensure, within the limits of responsibility, expertise and level of knowledge, that these principles are respected.

ENISA is pursuing in particular the following objectives:

- Compliance with the National and European environmental legislations, standards and regulations.
- Implementation and maintenance of the Environmental Management System in all relevant activities, operations and processes.
- Control and monitoring of the implementation of the Environmental Management System.
- Preventing and reducing environmental impacts during its activities, through designing and implementing environmental programmes.
- Continuously confirming that the probability of adverse events or negative impacts on the environment is acceptably low.
- Monitoring and control of resource and energy consumption, with emphasis on the efficient and sustainable use.
- Protection and respect towards the environment by implementing good practices for the reduction of waste production, minimisation of environmental risks, conserving energy and resources, reducing greenhouse gas emissions, enhancing the circular economy, and support biodiversity.
- Increase awareness within the organization in relation to environmental issues, encouragement and continuation of environmental management initiatives, and encouragement of the active participation of employees in relevant initiatives, with the adoption of best practices.
- Effective communication with internal and external stakeholders on environmental issues.
- Informing stakeholders about the implementation of the Environmental Management System, and about ENISA's commitment towards the environmental protection.
- Monitoring, reviewing, and evaluating performance against goals and objectives to ensure improvement.

The implementation of the above general objectives is carried out by planning and implementing the following actions:

- Adoption of an Environmental Management System in accordance with the EMAS Regulation, which shall be monitored, maintained, and improved through measurements, assessments, inspections and reviews.
- Ensuring the availability of the required resources, facilities, equipment, knowledge, and specialised personnel.
- Use of new environmentally friendly technological equipment and means, where possible.
- Continuous communication, awareness raising and training of the ENISA personnel.
- Continuous and transparent communication with external parties.

- Establishment of environmental objectives, for which their implementation is regularly reviewed and evaluated.
- Identification and assessment of critical environmental aspects and processes to reduce or eliminate negative environmental impact.
- Development and implementation of appropriate environmental management programmes
- Monitoring and continuous improvement of the environmental performance.

In 2024, ENISA consolidated its position towards environmental management.

Looking forward, in 2025 ENISA seeks to pursue the consolidation of the results and the achievements of its efforts to fill the gap and earn the EMAS certification. Staff information, education and at times, training are priorities in an effort to ensure continuous compliance and meaningful use of resources including natural resources.

As ENISA continues adapting its practices to improve efficient use of information technology and cybersecurity posture and services, it is also likely that environmental aspects will play a discreet role. For instance, using certified hosting sites on the Cloud is such an option.

Finally in terms of supply chain and provisioning and as ENISA seeks to phase out one of its office's buildings, thus gaining in efficiencies, it will continue prioritising environmental performance on all services it requires and pursues for its office building, provided that suitable options are offered in the local market in Athens and Brussels.

A

ANNEX VIII

ANNUAL ACCOUNTS

Statement of financial position

IN EUR	31.12.2024	31.12.2023
I. Non-current assets	977 984	1 453 737
Intangible fixed assets	0	0
Tangible fixed assets	977 984	1 453 737
II. Current assets	17 647 925	1 849 496
Short-term receivables	17 647 925	1 849 496
Cash and cash equivalents	0	0
TOTAL ASSETS (I. + II.)	**18 625 909**	**3 303 233**
III. Non-current liabilities	6 078 420	0
Long-term Commission pre-financing received	6 078 420	0
IV. Current liabilities	7 341 690	1 512 131
Short-term Commission pre-financing received	6 234 297	150 298
Accounts payable	66 136	84 717
Accrued liabilities	1 041 257	1 277 116
TOTAL LIABILITIES (III. + IV.)	**13 420 110**	**1 512 131**
V. Net assets	5 205 799	1 791 102
Accumulated result	1 791 102	5 328 730
Surplus/(deficit) for the year	3 414 697	-– 3 537 628
TOTAL LIABILITIES AND NET ASSETS (III. + IV. + V.)	**18 625 909**	**3 303 233**

Statement of financial performance

IN EUR	2024	2023
Revenue from the Union Subsidy	29 063 924	36 756 208
Revenue from administrative operations	4 067 815	104 840
Total operating revenue	33 131 739	36 861 048
Administrative expenses	– 19 453 036	– 18 611 406
Staff expenses	– 14 354 476	– 12 614 825
Fixed asset related expenses	– 675 054	– 783 056
Other administrative expenses	– 4 423 506	– 5 213 525
Operational expenses	– 10 264 006	– 21 786 370
Total operating expenses	– 29 717 042	– 40 397 776
Surplus/(deficit) from operating activities	3 414 697	– 3 536 730
Financial revenue	0	0
Financial expenses	0	– 898
Exchange rate loss	0	0
Surplus/(deficit) from non-operating activities	0	– 898
Surplus/(deficit) from ordinary activities	3 414 697	– 3 537 628
Surplus/(deficit) for the year	3 414 697	– 3 537 628

A

ANNEX IX

LIST OF ACRONYMS, INITIALISMS AND ABBREVIATIONS

ABAC	Accruals-based accounting
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
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CERT-EU	Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CNA	CVE Numbering Authority
CPP	Cyber partnership programme
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer security incident response team
CSOA	Cyber Solidarity Act
CSS	Corporate Support Services
CTI	Cyber threat intelligence
CVD	Coordinated vulnerability disclosure
CVE	Common Vulnerabilities and Exposures
Cyclone	Cyber crisis liaison organisation network
DEP	Digital Europe programme
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EC3	Europol's European Cybercrime Centre
ECA	European Court of Auditors
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECSC	European Cybersecurity Challenge
ECSF	European Cybersecurity Skills Framework
ECSM	European Cybersecurity Month
EEAS	European External Action Service
eID	Electronic identification
eIDAS	Electronic Identification and Trust Services Regulation
EIOPA	European Insurance and Occupational Pensions Authority
EMAS	Eco-management and Audit Scheme
ENISA	European Union Agency for Cybersecurity
ESCO	European skills, competences, qualifications and occupations
ESMA	European Securities and Markets Authority
ETSI	European Telecommunications Standards Institute

EU	European Union
EU5G	European Union certification scheme for 5G networks
EU-CSI	EU Cybersecurity Index
EU-JCAR	EU Joint Cyber Assessment Report
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
EUCI	EU classified information
EUCC	EU cybersecurity certification scheme on Common Criteria
EUDI	European Digital Identity
EUDIR	EU Digital Infrastructure Registry
EUIBAs	European Union institutions, bodies and agencies
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
L & D	Learning and development
MB	ENISA's Management Board
MOU	Memorandum of understanding
MS	Member States
MSS	Managed security services
NCSS	National cybersecurity strategy
NIS	Network and information security
NIS CG	NIS Cooperation Group
NISD	NIS directive
NLO	National Liaison Officers
OCA	Ownership and control assessment
Q & A	Question and answer
R & I	Research and Innovation
REA	European Research Executive Agency
SCCG	Stakeholder Cybersecurity Certification Group
SLA	Service-level agreement
SME	Small and medium-sized enterprises
SNE	Seconded national expert
SOP	Standard operating procedure
SPD	Single programming document
SRP	Single reporting platform
WG	Working group

TP-01-25-020-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, cooperat es 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

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union

ISBN 978-92-9204-715-3