enisa 20 years!

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2023 CONSOLIDATED ANNUAL ACTIVITY REPORT

JUNE 2024

CONTACT

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

LEGAL NOTICE

This publication presents the consolidated annual activity report of ENISA for 2023. The report is based on the 2023 work programme as approved by the management board of ENISA in Decision No MB/2022/14. The 2023–2025 ENISA programming document was adopted as set out in Annex 1 to that decision.

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

COPYRIGHT NOTICE

PDF ISBN 978-92-9204-673-6 ISSN 2314-9434 doi:10.2824/44117 TP-AB-24-001-EN-N

2023 CONSOLIDATED ANNUAL ACTIVITY REPORT

EUROPEAN UNION AGENCY FOR CYBERSECURITY

TABLE OF CONTENTS

FOREWORD 6
ENISA MANAGEMENT BOARD ASSESSMENT 8

Executive summary 12

PART I
ACHIEVEMENTS OF THE YEAR 16

PART II(A)
MANAGEMENT 105

2.1 Management board 105
2.2 Major developments 105
2.3 Budgetary and financial management 106
2.4 Delegation and subdelegation 110
2.5 Human resources management 110
- Implementing rules adopted in 2023
- Brief description of the results of the screening/benchmarking exercise

2.6 Strategy for efficiency gains 112
2.7 Assessment of audits and ex post evaluation results during the reporting year 112
- Internal Audit Service
- European Court of Auditors
- Ex post control evaluation result

2.8 Follow-up of recommendations and action plans for audits 113
2.9a Follow-up of recommendations issued following investigations by the European Anti-Fraud Office 114
2.9b Follow-up of observations from the discharge authority 114
2.10 Environmental management 114
2.11 Assessment by management 115

PART II(B)
EXTERNAL EVALUATIONS 117

PART III
ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS 118

3.1 Effectiveness of internal control systems 109
- Assessment of the control environment component
- Assessment of the risk assessment component
- Assessment of the control activities component
- Assessment of the information and communication component
- Assessment of the monitoring activities component

3.2 Conclusions of assessment of internal control systems 124
3.3 Statement of the internal control coordinator in charge of risk management and internal control 124

PART IV
MANAGEMENT ASSURANCE 127

4.1 Review of the elements supporting assurance 127
4.2 Reservations 127

PART V
DECLARATION OF ASSURANCE 129

ANNEX I
CORE BUSINESS STATISTICS 131

ANNEX II
STATISTICS ON FINANCIAL MANAGEMENT 150

ANNEX III
ORGANISATION CHART 154

ANNEX IV
2023 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT 156

ANNEX V
HUMAN AND FINANCIAL RESOURCES BY ACTIVITY 163

ANNEX VI
GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENT 165

ANNEX VII
ENVIRONMENTAL MANAGEMENT 167

ANNEX VIII
ANNUAL ACCOUNTS 168

ANNEX IX
LIST OF ABBREVIATIONS 170

FOREWORD

by the Executive Director

In 2023, the European Union Agency for Cybersecurity (ENISA) continued to work to strengthen the preparedness and resilience of Member States (MSs) and EU institutions, bodies and agencies in the area of cybersecurity.

Among the numerous accomplishments of the year, the following milestones could be emphasised: the support for the NIS2 implementation; the ENISA cybersecurity support action; our international cooperation and the new ENISA corporate strategy.

In 2023, ENISA made significant efforts in order to achieve a harmonised implementation of the NIS2 Directive. The agency provided technical advice to the Commission for implementing NIS2 security measures drafted guidelines for national coordinated vulnerability disclosure policies. The agency supported the NIS2 implementation by handling 12 individual Member State requests for advice on the directive's transposition to national legislation and organised risk management trainings for national authorities to help build up knowledge and expertise. The agency supported various NIS sectors with targeted bundles of different ENISA products and services and developed a NIS360 methodology to assess the overall maturity and criticality of the NIS sectors. Furthermore, ENISA collaborated with European Supervisory Authorities to align incident reporting provisions under DORA with those under NIS2.

The agency delivered on the 'Nevers 'joint call for a comprehensive risk assessment and recommendations report in response to the Russian war of aggression. To implement the Nevers process, ENISA collaborated with relevant telecom stakeholders and the NIS Cooperation group to make practical recommendations for the follow up of the Nevers risk assessment

The agency's efforts to build joint cybersecurity situational awareness and building up cyber preparedness across the Union received positive acclaim. The agency continued to offer operational assistance to Member States by implementing the ENISA Cybersecurity Support Action in 2023, which helped to enhance the resilience and capacity of critical entities in the EU to tackle cyber threats. A new contribution agreement was signed with the Commission in 2023, with an approximate value of.20 million euros, continuing the service up to and including 2026.

2023 saw significant strides with regards to our international cooperation. We formalised two working arrangements - one with Ukrainian counterparts and another with the Cybersecurity and Infrastructure Security Agency (CISA) of the US. By fostering deeper cooperation, sharing best practices and fortifying capacity building through structured collaboration, we can address some of our common challenges in the cyber threat landscape.

The agency saw the endorsement by the Management Board of its new corporate strategy 2023-2026. The corporate strategy aims to shape ENISA into a dynamic, service-oriented organisation and an appealing workplace, by establishing a long-term vision for resource planning and management, aligned with baseline requirements and priorities set by the ENISA Management Board and EU law.

Changes to the leadership of ENISA's Management Board also took place in 2023. Both the outgoing chair, Jean-Baptiste Demaison (France), and the outgoing vice-chair, Krzysztof Silicki (Poland), demonstrated relentless commitment and guidance during their tenure. Thanks to them, ENISA has been able to contribute significantly to the goal of achieving a high common level of cybersecurity across the EU. The agency has already benefited greatly from the valuable expertise of the new chair, Fabienne Tegeler (Germany), and vice-chair, Stefan Lee (Finland).

The agency's accomplishments during the year were made possible by the support of the European and global cybersecurity community. I am immensely thankful to all of our experts, advisors, partners and staff members who contributed to ENISA's mission in 2023

June 2024

Juhan Lepassaar
Executive Director

ENISA MANAGEMENT BOARD ASSESSMENT

The Management Board (MB) performed the analysis of the AAR and completed its assessment.

The conclusions of the Management Board are as follows:

1. 2023 built on the work of the previous year especially in the area of cooperative response with the continued implementation of the ENISA cybersecurity support action. The MB congratulates the agency with the execution of the support action demonstrated by the high take up of services by the Member states (MS). The MB calls on the agency to take on board lessons learned from the pilot to further enhance services to MS during the delivery of support action from 2024 onwards.

2. The MB acknowledges the augmented and expanded suite of situational awareness products provided to MS in cooperation with EU institutions, bodies and agencies such as the Joint Cyber Assessment Report (EU-JCAR) and calls on the agency to further build on the common Union situational picture with a view to extend it to all MS, including enriching the cyber private partnership programme.

3. In the area of policy development, the MB acknowledges the support and advice provided to policy makers (Member States, European Parliament, Horizontal Working Party and European Commission) for the development of the Cyber Resilience Act (CRA), the Cyber Solidarity Act (CSOA), and the EU Cybersecurity Act (CSA) amendment via products such as the NIS investment study. Nevertheless, the MB calls on the agency to strengthen relationships with stakeholders to further support with the coherence and harmonisation of policy files before adoption. The MB also supports the proposal to integrate national cybersecurity strategies and the work on the EU cybersecurity index including the peer review methodology, as per NIS2 (article 19) into policy development activity.

4. 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 guidelines) and calls the agency to continue its focus of supporting the MS with best practices and by providing a greater overview of solutions, including options on how the incoming ENISA obligation to build a vulnerability and incident reporting database under the CRA, could be utilised for the benefit of incident reporting obligations under the NIS2.

5. The MB acknowledges the development of the exercises and training platforms and solutions that allow stakeholders to organise their own exercises and trainings with the support of ENISA, thus leveraging existing resources to expanding capacity and success of both the European cybersecurity challenge (ECSC) and international challenge (ICC) with improving skills and expanding young talent in the Union. The MB urges the agency to enhance collaboration with the European Cybersecurity Competence Centre in this domain.

6. The MB acknowledges the support provided to operational communities (CSIRTs Network and EU- CyCLONe) and calls on the agency to step up its relationship with operational communities and encourage cooperation among them and with the NIS Cooperation Group and the Council's horizontal working party. In addition, the MB takes note on the initial preparations of the European vulnerability database (EUVDB) for NIS2 and also the consolidation of IT infrastructure that supports operational cooperation that was launched in 2023 and calls on the agency to further exploit synergies and improve support to MS via building synergies between various operational cooperation platforms that ENISA manages.

7. The MB acknowledges the valuable support provided to the Commission for the first implementing regulation adopted for the EU common criteria and the support provided to MS for the draft candidate schemes on Cybersecurity Certification Scheme for Cloud Services (EUCS) and EU5G and the valuable impact of standardisation in its support of certification.

8. The MB concludes that the initial steps undertaken in the area of market and industry were necessary but not sufficient for the forthcoming work in relation to the CRA from 2024 onwards and acknowledges the proposal to integrate research and innovation with the market and industry from 2025 onwards and calls on the agency to develop closer ties with the European Cybersecurity Competence Centre and Network (ECCC) in this area.

9. The MB acknowledges the excellent execution of the second pilot of the EU cybersecurity index, with all 27 MS taking part. The MB anticipates the operationalisation of the index in 2024 to contribute to the delivery of NIS2 (art.18) report on state of cybersecurity Union report. The MB supports the proposal to integrate cybersecurity index with policy development activity. In addition, the MB takes note of the outreached achieved by the Threat landscapes and sectorial landscape and looks forward to explore the additional sector threat landscapes in support of NIS2 implementation in synergy with overall situational awareness work under activity 5 within the SPD2025.

10. The MB recognises the success of the development of the European Cybersecurity Skills Framework (ECSF) and its adoption by MS and professional certification bodies to address the skills gap, and the proposal to integrate outreach and education outputs with capacity building activities under activity 3 within SPD2025 to enhance synergies going forward. The MB calls on the agency to further collaborate with ECCC and National Cybersecurity Coordination Centre's (NCCs) in this area.

11. The MB congratulates the agency on the instigation of working arrangements with US and Ukraine, as well as on the advanced stages of preparing working arrangements with NATO- NCIA and urges the agency to do more international cooperation in line with the ENISA international strategy in synergy with activity 4 within the SPD2025.

12. The AAR2023 outlines in detail those outputs that didn't make as sufficient an impact as planned, more specifically the MB notes the following outputs:

    - **output 3.5** support to Security Operational Centres (SOCs) and the MB supports the proposal to absorb this work under activity 4 within SPD2025 in conjunction with the forthcoming Cyber Solidarity Act which sees a need for close coordination between the CSIRT network and Pan European network of cyber hubs / European cybersecurity alert system (SOC);

    - **output 7.3** guidelines and good practices on cybersecurity in ICT products, processes and services, as well as the relevant functions of the Agency should be reviewed in the context of obligations of the Agency stemming from the CRA under the renewed market activity within the SPD2025.

    - **output 9.2** promote cybersecurity topics, education and good practices on the basis of the ENISA stakeholder strategy that had a lower-than-expected impact for its actions in the area of certification and support to SMEs. The MB supports the proposal to absorb this work under activity 3.

13. The MB calls on the agency to review and revise its current post allocations, functions and tasks within its two corporate units (EDO and CSS) to better address its changed needs, including by externalizing administrative and technical support functions and focusing existing staff posts on functions to ensure business continuity and objectives as outlined in the corporate strategy.

14. During 2023, ENISA committed a total amount of EUR 25 182 935 representing 100 % of the total budget for the year. Payments made during the year amounted to EUR 21 118 393 representing 83.86 % of the total budget. The MB take notes of the exceptional payment rate (99.99%) made in 2023 for the EUR 15 000 000 Cybersecurity support action. Although this exceptional significant amount carried forward to 2023 constituted a major risk to the 2023 budget execution it was successfully executed. As compared to 2022, there was a slight increase in commitment execution 100 % in 2023 as compared to 99.93 % in 2022. Overall payment execution has very slightly decreased and reached 83.86 %, compared with 84.11 % in 2022. The target of 95 % for commitment rate set by the Commission (DG Budget) was reached. The turnover of staff was increased slightly compared to 2022 from 4% to 4.9% in 2023. The ratio remains low below 5 % percent which shows good ability to retain staff members in the agency, to a large extent thanks to the Agency's flexible teleworking and hybrid work regime, which the MB fully supports.

15. The AAR also provides information on the internal control assessment for 2023. This section notes the main categories of deviation that led to exceptions reported. In 2023 the agency reported 24 exceptions in the AAR. None of these exceptions was assessed as high risks. Whilst some improvements are required the internal control are present and functioning better than ever before. The 2023 assessment of the internal controls shows adequate management of risks, a high level of transparency, clear governance structures and improved performance monitoring. The Board concludes that necessary actions were undertaken within 2023 to improve the overall efficiency of the agency in abiding to its principles and congratulates ENISA for all the efforts engaged to that end.

16. 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, as well as performance information. Overall, the Management Board takes note of the successful achievements of ENISA in 2023.

17. The Management Board notes with satisfaction that ENISA could shift priorities and resources to manage escalated cybersecurity challenges without jeopardising significantly the objectives as planned in the 2023 work programme. The MB reiterates that insufficient human resources of the agency is a detriment to the agency's ability to achieve a high common level of cybersecurity across the Union and fulfil all its tasks as prescribed by the Union law. In this context the MB repeats its call to the European 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.

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

EXECUTIVE SUMMARY

The mission of the European Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the EU, in cooperation with the wider community. It does this by acting as a centre of expertise on cybersecurity and by providing independent, high-quality technical advice and assistance to Member States (MS) and EU bodies on cybersecurity. It contributes to the development and implementation of the EU's cybersecurity policies.

The agency persisted in its efforts as directed by the Cybersecurity Act, working towards a robust and transparent approach to enhance Europe's cybersecurity. It adjusted ENISA's operations to meet evolving conditions and thus effectively fulfilled its responsibilities by supporting the Union through the following activities:

In 2023, the agency was actively involved in policy development related to cybersecurity legislation, engaging with various legislative bodies and providing technical advice on specific provisions. The agency conducted over ten interactions with the European Parliament, eight with the Horizontal Working Party on Cyber Issues (HWPCI), and over 20 with the Commission. Additionally, ENISA produced the NIS Investments report, analysing data from over 1000 operators and supporting Commission initiatives on skills development and cybersecurity frameworks.

ENISA also conducted a comparative analysis of seven policy areas and three international policy developments to identify overlaps, gaps, and inconsistencies, contributing to harmonisation efforts. ENISA's efforts were referenced in EU policy documents, including those on the Cyber Resilience Act and Cyber Solidarity Act. Moreover, ENISA organised the first EU Cybersecurity Policy Conference in cooperation with DG CNECT and planned the second conference for April 2024 under the auspices of the Belgian Presidency. The efforts in this domain form the foundation of our commitment to offering proactive guidance and support to all relevant stakeholders at the EU level, to ensure the integration of cybersecurity aspects into the policy development process through practical and customized technical guidelines.

In 2023, ENISA made significant strides in advancing cybersecurity policy implementation across the EU. Key achievements include providing crucial technical advice to the Commission for implementing NIS2 security measures, drafting guidelines for national Coordinated Vulnerability Disclosure policies, and led the data collection and drafted of the development of the 2nd 5G toolbox progress report.

Additionally, the agency delivered a comprehensive risk assessment and recommendations report in response to the Russian war of aggression and introduced the NIS360 methodology for assessing sector maturity. ENISA supported various NIS sectors with tailored bundles of products and services, initiated sectorial awareness reports, and organized public-private conferences. Furthermore, ENISA analysed cybersecurity challenges in the EU data spaces proposal and collaborated with ESAs to align with NIS2 incident reporting provisions under DORA.

Work to build capacity in cybersecurity has seen significant advancements, to develop cyber exercises, such as the Blue Room solution to support national exercises in Portugal. ENISA has played a pivotal role in developing cyber exercises and cybersecurity training across the EU, facilitating initiatives such as the EU Cyber Crisis Liaison Network (EU-Cyclone), the EU-Cyclone Standard Operating Procedure Exercise, the Blueprint Operational Level Exercise and the annual joint awareness and preparedness cybersecurity exercise (Jasper). Notably, Cyber Europe, a major biennial exercise, is organised by ENISA. As a result of rising demand for its services, ENISA's strategy now focuses on empowering communities to conduct their own exercises using ENISA's platforms thereby maximising impact and leveraging ENISA expertise. The large number of individuals participating in the European Cybersecurity Challenge and the International Cybersecurity Challenge (around 20 000 in 2023) is also a promising sign, suggesting increased interest in cybersecurity as a career, leading to an expansion of the cybersecurity talent pool in Europe and a larger skilled workforce in the future.

During the course of 2023 ENISA continued to implement the cybersecurity support action to support MS in the short term in view of the immediate and elevated threat of malicious cyber activities due to the ongoing Russian war of aggression against Ukraine. This mechanism aims to complement, rather than duplicate, endeavours to improve the capability of MS and the EU to prevent and respond to cyber threats and incidents. The cybersecurity support action provides MS with knowledge and expertise and increased preparedness in key sectors

ENISA also strengthened its capacity to monitor, analyse and respond to cybersecurity threats and incidents, building on its 2022 initiatives. This involved launching new services and enhancing its capacity to analyse cyber events. Collaborations with the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies and the EU Agency for Law Enforcement Cooperation resulted in the release of EU joint cyber assessment reports and joint rapid reports to warn businesses of ongoing threats. These achievements emphasise ENISA's commitment to strengthening Europe's cybersecurity preparedness through shared situational awareness, improved monitoring and timely reporting, thereby contributing to the EU's overall resilience.

ENISA successfully supported the Commission and the MS in several key endeavours. Firstly, it facilitated the adoption of the initial cybersecurity certification scheme through the dedicated Commission implementing regulation on EU common criteria. Secondly, ENISA diligently analysed all available options to fulfil the digital sovereignty needs within the draft EU cybersecurity certification scheme for cloud services. Thirdly, it consolidated requirements for the draft candidate scheme pertaining to 5G. In addition, ENISA conducted thorough studies on diverse aspects of cybersecurity certification requirements, including artificial intelligence, managed security services, the EU digital identification wallet and vulnerabilities handling for certified products, services and processes, demonstrating ENISA's commitment to the promotion of the voluntary cybersecurity certification framework in the EU.

The EU Cybersecurity Index has emerged as a pivotal tool in assessing cybersecurity maturity across the EU, consolidating qualitative and quantitative data from ENISA activities. In 2023, all 27 MS participated in the pilot programme, with validation from key bodies such as the NIS Cooperation Group and the Computer Security Incident Response Teams Network. While initial work focused on preparation, ENISA plans to increase the relevance of the index under the NIS 2 Article 18 report from 2024 onwards. Moreover, ENISA's work on analysing threat landscapes and predicting emerging challenges has led to an increase in outreach,

media coverage and citations of ENISA publications, highlighting the significance of this endeavour.

On 18 April 2023, as part of a cyber package, the Commission adopted a communication on the Cybersecurity Skills Academy, inviting relevant actors to take action to close the cybersecurity workforce skills gap. The academy aims to foster knowledge generation through education and training by working on a common language on cybersecurity role profiles and associated skills, namely the European Cybersecurity Skills Framework. In 2023, ENISA launched numerous actions in this area. These included a review of the framework, to ensure its ongoing relevance and effectiveness, and, in association with its stakeholders, and defining cybersecurity indicators. Furthermore, ENISA developed a concept paper giving an overview of MS' current status, as regards the creation of repositories of training programmes and certifications from both the public and private sectors with the aim of providing a single access point to the resources available for professional skills development.

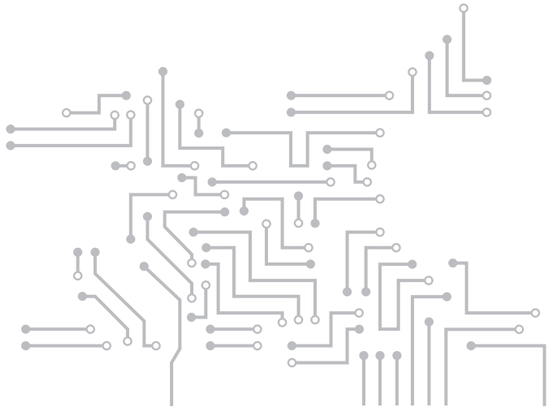
In 2023, ENISA established a working arrangement with its Ukrainian counterparts, including the Ukrainian National Cybersecurity Coordination Centre and the Administration of the State Service of Special Communications and Information Protection of Ukraine. This agreement focuses on capacity building, sharing best practices and improving situational awareness. It involves short-term cooperation actions and aims to align cybersecurity policies and approaches in the long term. In 2023, ENISA also signed a working arrangement with the US Cybersecurity and Infrastructure Security Agency, again emphasising capacity building, the exchange of best practices and increased situational awareness. ENISA's international strategy emphasises strategic engagement with international partners, focusing on areas with high added value. Its arrangement with the US Cybersecurity and Infrastructure Security Agency strengthens existing cooperation and opens the door to new collaborations, covering both short-term actions and long-term alignment in cybersecurity policies and implementation approaches.

In 2023, ENISA's management board underwent changes, with Fabienne Tegeler (Germany) becoming the new chair and Stefan Lee (Finland) the new vice-chair. The board's responsibilities include approving the agency's work programme and budget, appointing the executive director and ensuring compliance with the Cybersecurity Act. ENISA also completed the selection process for its advisory group, which comprises 33 experts representing various stakeholders (excluding the EU cybersecurity certification framework). This group advises ENISA on its tasks and annual work programme and provides expertise. ENISA's new corporate strategy for 2023–2026, approved by the Management board, aims to transform the agency into a dynamic organisation aligned with ENISA's priorities.

In 2023, ENISA fully executed its annual budget and achieved 83.86 % payment execution of the annual budget. Commitment execution was at 100 %, exceeding the Commission's target of 95 % and representing a slight increase from 2022 (99.93 %). The EU subsidy appropriations (C1) not paid in 2023 were carried forward to 2024. Similarly, C1 appropriations not fully paid in 2022 were carried forward to 2023 (C8 appropriations).

Overall payment execution for C8 funds in 2023, including the assistance fund, was at 99.20 %. Payment execution for ENISA's 'normal' budget (excluding the assistance fund) increased to 96.14 % in 2023, up from 95.07 % in 2022. The payment execution for the assistance fund alone reached 99.99 %.

In terms of human resources, corporate services continued to support the operational and administrative goals of the agency in terms of staff acquisition and development. In 2023, ENISA welcomed 19 new staff members and maintained the proportional allocation of resources between its operational units and those that support the administrative and corporate functions.



PART I
ACHIEVEMENTS OF THE YEAR

The following sections of the annual activity report are based on the structure of the 2023–2025 ENISA programming document. Each activity undertaken during the course of 2023 is described in detail and its outcomes are reported.

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. During the course of 2023 the activity achieved the following:

- **Policy development.** ENISA engaged with the co-legislators of the Cyber Resilience Act (CRA), the Cyber Solidarity Act (CSOA) and the Cyber Security Act (CSA) amendment by means of technical consultations/meetings/workshops (e.g. 10 interactions with the European Parliament, eight with the Horizontal Working Party on Cyber Issues (HWPCI) and over 20 with the European Commission) and delivered, in a holistic and evidence-based manner, technical advice on particular provisions of these instruments (e.g. Articles 11, 41, 45, 48 and 49 and Annexes I and III of the CRA and Articles 12, 13 and 14 of the CSOA).
- **The 2023 NIS Investments report.** The agency produced its annual NIS Investments report, and in doing so analysed data from over 1 000 operators, from all sectors, in the scope of NIS 1. Findings from the report have also supported the Commission's initiatives on skills and the European Cybersecurity Skills Framework (ECSF), as well as the EU Cybersecurity Index (EU CSI), the network and information security (NIS) 360 project (NIS 360) and ENISA's work on the NIS 2 Article 18 report. The report is referenced 13 times in EU policy documents, including policy documents on the CRA and the CSOA.
- **Policy landscape.** In 2023, ENISA developed a comparative analysis of **seven policy areas under implementation and three key international policy developments.** The analysis, shared and validated with the NIS Cooperation Group and the European Commission, identifies overlaps, gaps and inconsistencies that affect harmonisation and coherence at the implementation level. Findings from this analysis are also used as input to the NIS 2 Article 18 report. In January 2023, ENISA, in cooperation with the Directorate-General for Communications Networks, Content and Technology (DG Connect), organised the first EU Cybersecurity Policy Conference. The agency also, in cooperation with DG Connect and under the auspices of the Belgian Presidency, helped to organise the second **EU Cybersecurity Policy Conference** (which took place in April 2024).

The impact of ENISA's work in supporting policy development has been acknowledged by stakeholders in several ways. For example, activity 1, jointly with activity 2, topped the ENISA management board's list of priorities. In addition, the agency's work on the upcoming CSA review has received positive feedback from stakeholders, and the agency's work was also acknowledged at the top management level during bilateral discussions with cybersecurity agencies (1).

In 2023, 100 % of the EUR 330 000 budget was committed; however, delayed recruitment and staff departures resulted in a significant resource gap, of about 1.95 full-time equivalents (FTEs). This had a significant effect, as the sensitive nature of the tasks carried out under activity 1 makes it necessary to use internal resources for this activity.

The overall assessment of activity 1 is as follows:

- Its impact is significant because it involves offering **targeted evidence-based technical advice to policymakers.**
- ENISA has been asked to **contribute to a host of new horizontal and sectorial cybersecurity policy initiatives**, but, although its input would be beneficial, resource constraints mean that the agency is unable to meet all such requests.
- Member States (MSs) have increasingly expressed the need to **align horizontal and sectorial cybersecurity legislation.**
- There are overlaps, gaps and inconsistencies in existing policies. By working together, relevant stakeholders and ENISA can implement good practices, thereby increasing harmonisation and reducing costs for competent authorities as well as liable private stakeholders.
- The impact of ENISA's work in policy development is multiplied when **the agency is involved from the start of the policy development process** (e.g. the CRA). This enables the agency to provide policymakers with actionable evidence in a timely manner.
- The way forward is to leverage the use of business intelligence tools to make the data easier to reuse in other ENISA activities, and eventually to make the available datasets public.
- The next step in supporting policy monitoring will **focus on emerging areas** and the identification of areas where policy interventions may be considered, an exercise that can greatly benefit from close synergies with ENISA's work on foresight.
- Activity 1 will also benefit from **stronger synergies with the EU CSI and national cybersecurity strategies** in the future.

Objectives

- Foster cybersecurity as an integral part of EU policy (existing and new)
- Ensure that EU policymakers are regularly informed about the effectiveness of existing frameworks and that EU policymakers and stakeholders are provided with timely and tailor-made policy recommendations on future cybersecurity challenges and opportunities

Results

- Cybersecurity aspects are considered and embedded across EU and national policies

Link to strategic objective (ENISA strategy)

- Cybersecurity as an integral part of EU policies

(1) For example, at the cybersecurity directors' meeting, organised by the Bundesamtes für Sicherheit in der Informationstechnik, on 14–15 February 2024.

Outputs	Outcome
1.1. Assist and advise the Commission and Member States in reviewing the effectiveness of current cybersecurity policy frameworks	• ENISA published the fourth NIS Investments report, providing policymakers with insights into the cybersecurity budgets of operators of essential services and digital service providers and how these budgets were influenced by the NIS directive, in order to inform future policy decisions. Data from the report were also used to support the Cyber Skills Academy policy initiative, as well as several ENISA activities, such as the EU CSI and the NIS 360 sectorial assessments. • ENISA provided technical advice/consultancy to the Estonian Information System Authority on the development of a cost model for public sector cybersecurity investments. • The agency took steps to enable NIS investments data to be easily reused across ENISA's teams and units and, eventually, through a business intelligence dashboard, by external stakeholders. Work on a prototype of the dashboard is ongoing, and the dashboard is expected to be completed in 2024. The NIS Investments report is available online. The output achieved its objectives in 2023. As this output consistently demonstrates the positive impact of data availability on policymaking, stronger synergies with other ENISA activities collecting data relevant to the impact of policies could be explored in future iterations of the SPD. Specifically, increased impact and efficiencies can be achieved through stronger integration of output 1.1 with the EU CSI and national cybersecurity strategies (NCSSs), providing an expanded evidence base to support policymaking.

1.2. Assist and advise the Commission and Member States on new policy development, as well as carrying out preparatory work	ENISA followed a holistic approach, with internal coordination of contributions from all relevant ENISA activities. Expertise across the agency was utilised as needed, and technical advice was coordinated and consolidated to provide comprehensive input in the policy development process.
	• ENISA supported the European Commission, the European Parliament and the HWPCI with regard to the CRA in the following ways.
	  • It provided technical advice to the Commission on topics such as vulnerability/incident notification, scoping of critical products, EU common criteria (EUCC) relevance and product evaluations.
	  • It provided opinion and technical advice to the European Parliament (Members of the European Parliament (MEPs) / rapporteurs and European Parliament technical staff) on topics including Article 11, voluntary notification, etc.
	  • It provided opinions to the HWPCI on aspects associated with the projected role of the agency in the CRA.
	  • In supporting the CRA, **ENISA had over 25 interactions with DG Connect and the European Parliament** (including with MEPs/rapporteurs) in order to provide technical advice on a number of topics, as well as the role for ENISA envisaged in the CRA. Furthermore, extensive internal coordination across different ENISA units was necessary to develop the agency's position on the CRA and to assess the requirements to be met for the agency to fulfil its envisaged role under the CRA. The positions and public opinions of ENISA were taken into consideration by the co-legislators, as is evident from the agreed CRA text, which is close to ENISA's position.
	• ENISA supported the European Commission, the European Parliament and the HWPCI with regard to the CSOA in the following ways.
	  • It analysed the capacity of the security operation centres (SOCs) of operators of essential services /digital service providers in the EU to provide technical advice and data to DG Connect (through the NIS Investments report).
	  • It interacted with MEPs/rapporteurs and European Parliament technical staff in the preparation of the European Parliament position, by providing its opinion and technical advice.
	  • It interacted with the HWCPI on topics related to the role envisaged for ENISA in the CSOA.
	  • In supporting the CSOA and the proposed CSA amendment, **ENISA had seven technical meetings/workshops with DG Connect and the European Parliament** (including with MEPs/rapporteurs) in order to provide independent opinion on several topics as well as to provide data on SOC capabilities in the EU (through the NIS Investments report). In parallel, and through cross-agency coordination, ENISA developed its position vis-à-vis these two legislative initiatives and particularly concerning ENISA's envisaged role in the CSOA and the necessary resource requirements.
	• In the context of the proposed CSA amendment, ENISA supported the Commission and the European Parliament by providing technical advice on the alignment of the definition of managed security service providers across different legislative instruments (the NIS 2, the CSOA and the CSA amendment).
	• In 2023, ENISA continued to support the Commission in the development of the Artificial Intelligence (AI) Act through monthly interactions to provide advice on cybersecurity aspects of the AI Act and by liaising with different DG Connect units on aligning market surveillance aspects for notifications and security measures and to discuss the role of ENISA in AI Office.
	• In 2023, ENISA continued its support to the Commission in its review of the revised electronic identification (eID) and trust services regulation (eIDAS2) and the EU Digital Wallet ToolBox process.

- ENISA participated in several European Strategic Coordination Platform activities, in particular within the scope of Opinion No 03/2021: Management of information security risks, drafted by the European Union Aviation Safety Agency (EASA). ENISA provided EASA with technical advice on the development of the horizontal rule policy, contributed to discussions on NIS 2 v part information security (Part-IS) policy gaps and overlaps, and, through an NIS investments deep dive, helped it explore the maturity of operators in the aviation sector.

The output achieved its objectives in 2023. Its scope remains timely and relevant. Based on ENISA's assessment, it should be included in the 2024 SPD. This output benefits substantially from synergies with output 1.1, which provides data to support evidence-based policymaking for the various policy files in scope.

1.3. Support policy monitoring of existing and emerging policy areas and maintain a catalogue of all relevant cybersecurity legislation and policies at the EU level

- In 2023, ENISA developed a policy landscape report, to be shared with the Commission, the NIS Cooperation Group and the National Liaison Officers (NLOs) Network. The policy landscape provides a comparative analysis of policy files under implementation based on nine categories of reference, interplay analysis with NIS 2 and international policy scouting (by presenting three cases of new cybersecurity policy developments outside the EU).
- In order to provide timely information to the NIS Cooperation Group, ENISA provided updates of progress in policy monitoring (policy updates) addressing both regulations under negotiation and those that have been implemented.
- ENISA organised, in cooperation with DG Connect, the first EU Cybersecurity Policy Conference, which took place in January 2023. In total, 220 participants attended the conference, and the subsequent satisfaction survey revealed zero negative opinions and high satisfaction values (91 % high / very high overall satisfaction, 94 % high / very high satisfaction for both content quality and organisation by ENISA and 100 % high likelihood of participation in future iterations of the conference).
- Following the success of the first conference, ENISA, in collaboration with DG Connect and under the auspices of the Belgium 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.

The output achieved its objectives in 2023. Its scope remains timely and relevant. Based on ENISA's assessment, it should be included in the 2025 SPD. This output stands to benefit substantially from stronger synergies with ENISA's work on foresight, in order to expand its scope to monitoring emerging policy areas and identifying likely new topics that may warrant early policy interventions.

Key performance indicator ENISA's added value to EU institutions, bodies and MSs in providing support for policymaking (ex ante)	**Unit (of measure-ment)**	**Frequency**	**Data source**	**2022 results**	**2023 results/ target**
1.1. Number of relevant contributions to EU and national policies and legislative initiatives (2)	Number	Annual	Manual collection from staff members	314	172/215

(2) For example, at the cybersecurity directors' meeting, organised by the Bundesamtes für Sicherheit in der Informationstechnik, on 14–15 February 2024

Key performance indicator	**Unit**	**Frequency**	**Data source**	**2022 results**	**2023 results/ target**
Contributions to task forces and bodies	%	Annual	Manual collection from staff members	9 % of 314 total contributions	17 % of 172 total contributions
Contributions to workshops and conferences	%	Annual	Manual collection from staff members	87 % of 314 total contributions	77 % of 172 total contributions
Support actions/contributions to Commission and MSs for policies and legal initiatives following relevant requests	%	Annual	Manual collection from staff members	4 % of 314 total contributions	6 % of 172 total contributions
1.2. Number of references to ENISA reports, analysis and/or studies in EU policy documents		Biennial		16	13/NA
1.3. Satisfaction with value added by ENISA's contributions	%	Biennial	Survey	93 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	92 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	92 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	90 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	95 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	91 %	NA
1.4. Number of EU policy files under development and supported by ENISA	Num-ber	Annual	Report	NA	6

Allocated FTEs as per SPD, based on full establishment at 2023 year end (3)	4.75	Number of FTEs actually used	2.49
Planned budget (EUR) (4)	330 262	Budget consumed (EUR) (5)	329 957.62
		Of which carried forward to 2024 (EUR)	66 309.32

(3) Allocated FTEs in SPD refer to head count, whilst actual FTEs is calculated based on person work days of a full year
(4) Direct costs only.
(5) Direct costs only

ACTIVITY 2:
Supporting implementation of Union policy and law

Under activity 2, ENISA focuses on supporting MSs with the implementation of NIS 2, advising finance sector stakeholders on the implementation of the Digital Operational Resilience Act (DORA) and addressing cybersecurity technical needs in the area of personal data protection.

- ENISA in consultation with the NIS Cooperation Group delivered detailed technical advice to the Commission on the NIS 2 implementing acts on security measures, a crucial and time-critical milestone in the NIS 2 transposition process, helping to achieve harmonised implementation of NIS 2.
- ENISA in consultation with the NIS Cooperation Group, draft guideline on national coordinated vulnerability disclosure (CVD) policies was adopted by the NIS Cooperation Group. In this way ENISA helped MSs to meet an important new requirement under NIS 2.
- The second 5G toolbox progress report was published in 2023. ENISA led the data collection and drafted the technical parts. ENISA also launched the ENISA 5G security controls matrix, to help relevant authorities understand the technical aspects of the 5G toolbox.
- Implementing a new NIS 2 task, ENISA developed a pilot system for the EU Digital Infrastructure Registry (EUDIR). EUDIR lists digital infrastructure entities. Its aim is to help MS implement the main establishment concept (one-stop shop principle).
- The Nevers joint call asked for a union-wide risk assessment and recommendations, responding to the Russian war of aggression against Ukraine. In 2023, ENISA delivered the full report, which included risk scenarios and recommendations.
- ENISA developed the NIS 360 methodology to assess the overall maturity and criticality of NIS sectors. NIS 360 was conceived as an instrument for steering ENISA's NIS strategy and national strategies, covering 10 NIS 1 subsectors.
- ENISA supported eight NIS sectors (telecoms, trust, internet infrastructure, energy, health, rail, finance and aviation), providing them with targeted bundles of different ENISA products and services, depending on the needs of each sector.
- ENISA started providing bimonthly sectorial awareness reports to stakeholders in six NIS sectors working with ENISA's situational awareness team (activity 5), providing open source intelligence (OSINT) threat information to national/sectorial authorities.
- ENISA organised eight large public–private (ENISA flagship) conferences for the EU's critical sectors, to facilitate a dialogue and exchange of good practices between relevant authorities and industry.
- To support the implementation of the personal data protection policy, ENISA analysed and reported on cybersecurity challenges in the EU data spaces proposal, and joined the European Data Innovation Board, established under the Data Governance Act.
- To support the implementation of DORA, ENISA assisted the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) with aspects of DORA, advising on alignment with
- NIS 2 incident-reporting provisions. A memorandum of understanding (MoU) with the European supervisory authorities is being finalised.

This activity experienced a significant resource gap in 2023 (see below). In addition, some resource was consumed by some small, unplanned, tasks required to further promote EU collaboration and harmonisation on cybersecurity, supporting the workstreams for WHOIS, supervision and elections cybersecurity.

- For activity 2, in 2023, 99.99 % of the budget of EUR 773 000 was committed.
- Compared with the 2023 plans for this activity, there was a resource gap of about 2.6 FTEs, as a result of ongoing recruitment and staff departures in the spring. This gap was addressed by scaling back work in areas receiving fewer requests, such as the once only technical system (OOTS).
- Work under this activity follows a 3-year ENISA NIS strategy, adopted in 2022 and designed to address the NIS 2 challenges. To implement this strategy, ENISA allocated more resources at the start of 2023.
- Having adopted several new and important cybersecurity policy files in recent years, there is now a need to focus on the implementation of these cybersecurity policies, making NIS 2 and DORA work in practice.
- The NIS Cooperation Group work programme was updated for the forthcoming period, 2024– 2026. The group now comprises approximately 700 experts from MSs and has 15 active workstreams. It is important to consolidate these workstreams where possible.

Looking ahead to 2024, this activity will continue with a similar level of resources, but some changes to streamline this activity are planned:

- Output 2.4 (Transversal policies) will be discontinued and some of this work will be integrated into the horizontal and sectorial outputs;
- Increased resources will be allocated to horizontal outputs 2.1 And 2.2, Following the guidance of the enisa management board;
- Output 2.2 Will focus more on eu coordinated risk evaluations and toolboxes, which is an emerging area;
- The resources allocated to output 2.3 (Sectorial nis implementation) will remain stable.

Objectives

- Ensure consistent development of sectorial and horizontal EU policies, to avoid implementation inconsistencies
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in MSs
- Effectively implement cybersecurity policy across the EU and ensure consistency between sectorial and horizontal cybersecurity policies
- Improve cybersecurity practices by taking on board lesson learned from incident reports

Results

- Consistent implementation of Union policy and law in the area of cybersecurity
- EU cybersecurity policy implementation reflects sectorial specificities and needs
- Wider adoption and implementation of good practices

Link to strategic objective (ENISA strategy)

- Cybersecurity as an integral part of EU policies

Outputs

2.1. Support the activities of the NIS Cooperation Group, including its work programme

Outcome

- Supporting the NIS Cooperation Group, ENISA is the secretariat for six workstreams and supports four additional workstreams: the 5G workstream, the information and communications technology (ICT) supply chain workstream, the elections workstream and the workstream for EU coordinated risk evaluations.
- To support the Commission, ENISA, working with the NIS Cooperation Group, provided the Commission with detailed technical advice to enable it to draft the NIS 2 implementing acts on security measures for digital infrastructures. This advice was delivered to the Commission, on time, in Q3 2023.
- To support NIS 2 transposition by MSs, ENISA organised 'NIS 101' risk management training for national authorities, to help build up knowledge. It also handled 12 individual MS requests for advice on NIS 2 transposition.
- Developing and hosting the EUDIR is a new ENISA task under NIS 2. In 2023, ENISA developed a pilot version of the EUDIR and started the implementation of the production system ahead of the expected launch in Q3 2024.
- The CVD policy guideline was adopted – report drafting and technical workshop on CVD policies, as well as ENISA internal coordination on vulnerabilities with other ENISA units were carried out however the CVD map is postponed to 2024.
- The agency organised eight workshops for stakeholders and performed sectorial assessments using its NIS 360 methodology. ENISA validated the maturity and criticality scores for each sector and a report covering all NIS 2 sectors is expected to be published in Q2 2024.

ENISA delivered all of its objectives under this output. The implementation of NIS 2 is a high priority for 2024, meaning that it is pertinent to (1) support MSs with NIS 2 transposition where possible and (2) implement new tasks under NIS 2. For 2024, horizontal work remains a priority, and this output will grow, utilising some of the resources previously allocated to output 2.4, which has been discontinued.

2.2. Support MSs and the Commission in the implementation of horizontal aspects of the NIS directive

- ENISA continued to support the 5G toolbox progress report. The agency was heavily involved in collecting data and drafting the 5G progress report, which was adopted in June 2023. ENISA also launched the ENISA 5G matrix in May 2023 at the ENISA Telecom Security Forum in Lisbon, atter completing a first update of the 5G control matrix content, adding a set of non-technical controls. The ENISA 5G matrix is essential to MSs' implementation of the technical parts of the 5G toolbox. In 2024, the matrix will be updated, to bring it into alignment with NIS 2.
- The Nevers process delivered its follow-up paper. The Nevers process is strongly supported by ENISA, which collaborates with all relevant stakeholders, including the European Competent Authorities for Secure Electronic Communications (Ecasec) group of telecom authorities and the Body of European Regulators for Electronic Communications (BEREC), empowering the NIS Cooperation Group to make practical recommendations to follow up on the Nevers risk assessment. ENISA delivered a mature draft in June 2023, then addressed comments from MSs in the second half of 2023, ahead of formal adoption and publication in early 2024. In 2024, the agency will create a Nevers action plan, aiming to address all recommendations in 2 years.
- ENISA developed a technical NIS 2 security measures framework, updating the NIS 1 reference document on security measures, to support MSs and the NIS Cooperation Group with NIS 2 transposition. ENISA established a drafting team and organised several meetings, including a physical meeting in Athens. ENISA will keep this technical framework updated in 2024 and is ready to publish this framework as a technical guideline, to complement the NIS 2 implementing rules on security measures.
- ENISA supported the follow-up to the Council conclusions on cyber risk posture. ENISA drafted risk scenarios, which were adopted as part of the cyber risk posture deliverable, using a physical scenario-building workshop with MSs at ENISA's premises.
- ENISA supported the NIS Cooperation Group in its work on the ICT supply chain toolbox, intended to mitigate supply chain issues. The recently adopted CRA will be an important tool in the future for dealing with ICT supply chain issues.

Output 2.2 delivered all of its objectives. The area of EU coordinated risk assessments and toolboxes is growing, with three more processes being supported, besides the 5G toolbox: the Nevers process, the cyber risk posture process and the ICT supply chain toolbox process. The proposed CSOA will trigger new work in the area of EU coordinated stress tests and sectorial risk posture assessments, for example to support the Commission's situation centre. To support these new initiatives, ENISA is allocating additional resources to this output in 2024, using some of the resources previously allocated to the discontinued output 2.4.

2.3. Support Member States and the Commission to increase the security and resilience of the NIS sectors via targeted service package identified in the ENISA NIS strategy	In 2023, as part of the ENISA NIS strategy, the agency started to support the NIS sectors with targeted packages/bundles of services: 'build', for immature sectors that need to improve; 'sustain', for mature sectors that need continued support and ENISA leadership; 'involve', for mature sectors where sectorial stakeholders take the lead; and 'prepare', for new NIS sectors that may require ENISA's support in the future. Some highlights from these packages/bundles: • **Health (build package).** The 8th ENISA eHealth Security Conference took place in Luxembourg in 2023. ENISA acts as the secretariat for NIS Cooperation Group workstream 12, on health. ENISA organised a tabletop exercise to support this group and is also supporting the e-health Information Sharing and Analysis Centre (ISAC). It also delivered a health cybersecurity threat landscape (together with knowledge & Information team, organised an awareness-raising campaign (together with the awareness raising & education team and conducted a survey on sectorial research/funding priorities together with the research and innovation team. • **Rail (build package).** The 3rd ERA–ENISA Conference for the Cybersecurity in Railways took place in Athens. ENISA, together with the European Union Agency for Railways (ERA), organised a webinar for relevant authorities and is supporting preparatory work for the update of the European Rail Traffic Management System technical systems for interoperability. ENISA also, with ARET, organised an awareness-raising campaign for the railway sector and, with KIT, updated the transport threat landscape. ENISA supports the Landsec Working Party on Rail Security and did preparatory work for the implementation of the EU skills framework for the railway sector. Through meetings and workshops, the agency engages with relevant expert groups, such as the Rail Chief Information Security Officers' Forum, the International Union of Railways Cybersecurity Solution Platform, the International Association of Public Transport, the European Committee for Electrotechnical Standardisation (CENELEC), the European Rail ISAC and the Europe Rail Joint Undertaking System Pillar. In addition, working together with the market, certification and standardisation unit (MCS), ENISA is supporting the creation of International Electrotechnical Commission standard 63452, on railway cybersecurity. • **Telecoms (sustain package).** The ENISA Telecom and Digital Infrastructure Security Forum took place in Lisbon. ENISA acts as the secretariat for the ECASEC group of EU telecom authorities, organising and hosting their meetings. The ECASEC group is an important stakeholder in the Nevers process (output 2.2). ENISA initiated two NIS 2 task forces within the ECASEC group, one on security measures and one on incident reporting, to support the work of the NIS Cooperation Group on NIS 2 provisions. The ENISA report on subsea cables cybersecurity was published in 2023, supporting the follow-up EU policy action on the security of submarine cables. ENISA also did a deep dive on low Earth orbit satcom security, a new topic for the group, relevant in the context of Nevers, drafting a first report with cybersecurity challenges for this emerging new segment of the EU telecom market. • **Digital infrastructures (sustain package).** ENISA is the secretariat for the NIS Cooperation Group workstream 10, on digital infrastructures, and has hosted several meetings. The group provides important input to the Commission on the implementing rules on incident-reporting and security measures for the NIS 2 digital infrastructure sector. ENISA is also working closely with this group on the EUDIR (see output 2.1), and many of the same stakeholders are involved in the work on the new NIS 2 provisions on WHOIS (see output 2.1) • **Trust (sustain package).** The ENISA Trust and eID Forum 2023 took place in Vienna. ENISA supports the European Competent Authorities for Trust Services (ECATS) group of EU trust services security authorities, by acting as its secretariat (in 2023 hosting two ECATS meetings) and by supporting three ECATS task forces (on cryptographic algorithms, NIS 2 security measures and NIS2 incident reporting). NIS 2 changes the policy framework for these authorities, by moving security measures for trust services out of the eIDAS regulation and into NIS2. • **Energy (sustain package).** ENISA, together with the European Network of Transmission System Operators for Electricity, European Distribution System Operators and the European Network for Cyber Security, co-organised the Energy Cybersecurity Conference in Athens. ENISA also supports the European Energy ISAC, by providing situational awareness updates, and hosted a European Energy (ISAC) meeting in Athens. In 2023, the agency also organised a sectorial awareness workshop (train-the-trainer) and awareness campaign for gas and electricity. • **Finance (involve package).** ENISA supports the main finance sector stakeholders by participating in their groups and giving advice. ENISA is a member of the Joint Committee on DORA, and supports the EBA, ESMA and EIOPA by defining a cybersecurity framework for the financial sector. • **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, and implemented the ECSF by applying it to the aviation sector, supporting aviation authorities. • **Gas and water (prepare package).** In the gas subsector ENISA engages with DG Energy and the European Network of Transmission System Operators for Gas, and ran an awareness campaign for gas operators. In the drinking water subsector, ENISA engaged with Eureau, Water ISAC and the European Water Association, and published a brief threat landscape for the drinking and waste water sector. Output 2.3 delivered all of its objectives. This was the first year in which ENISA delivered NIS service packages/bundles. In 2024, there will be will one small change, namely the inclusion of two new NIS 2 sectors: space (involve) and public administrations (prepare).
2.4. Provide advice, issue technical guidelines and facilitate the exchange of good practices to support MSs and the	• **eIDs and wallets.** ENISA supported the EU digital wallets process, needed for the deployment of a new EU identify framework (defined in the eIDAS2 proposal) and supported the eIDAS Cooperation Network. ENISA continued to provide technical advice on the cybersecurity aspects of remote video identification and to promote good practices. This important new eID technology became essential during the COVID-19 crisis and is increasingly being used for legitimate reasons, but is also exploited by criminals, for instance to create deepfakes**.** • **Privacy and data protection.** ENISA's recommendations and good practices are being taken up by data protection authorities. The agency analysed the cybersecurity challenges facing the EU's data spaces and published its findings, and it engaged with the data protection community on 'how' to engineer data protection solutions. • **OOTS.** ENISA participated in the OOTS security subgroup meetings, presenting relevant past ENISA work. No further requests for engagement or support were received. • **DORA.** ENISA supported the EBA, EIOPA and ESMA in the implementation of DORA and gave advice on aligning DORA with NIS 2. • **Cybersecurity network code for cross-border electricity flows.** ENISA supported DG Energy and the Agency for the Cooperation of Energy Regulators with cybersecurity aspects of the code for cross-border electricity flows, providing advice on alignment with NIS 2, and preparing for future ENISA tasks under the code. The code is expected to be adopted in 2024. Output 2.4 delivered all of its objectives. However, this output has been discontinued, to improve overall efficiency and to enable the agency to focus more on NIS 2 implementation.

Key performance indicator Contribution to policy implementation and implementation monitoring at the EU and national levels (ex post)	Unit (of measure-ment)	Frequen-cy	Data source	2022 results	2023 results/ target
2.1. Number of EU policies and regulations implemented at the national level supported by ENISA	Number	Annual	Manual collection from staff members	5	6/5
2.2. Number of ENISA reports, analyses and/or studies referred to at the EU and national levels	Number	Biennial	Survey	65	NA
2.3. Satisfaction with ENISA added value of support	%	Biennial	Survey	94 %	NA
% of stakeholders rating the outcome/ results of ENISA's work as providing high or some added value	%	Biennial	Survey	93 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	87 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	90 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	97 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	93 %	NA
2.4. Number of critical sectors with a high level of cybersecurity maturity (NIS 360 methodology)	Number	Annual	Internal analysis (NIS sector 360)	NA	6/NA
Allocated FTEs based on the full establishment plan at 2023 year end	12.95	**Number of FTEs actually used**			9.9
Planned budget (EUR) (6)	793 404	**Budget consumed (EUR) (7)**			773 113.69
		Of which carried over to 2024 (EUR)			119 225.18

NA, not applicable

(6) Direct costs only.
(7) Direct costs only.

ACTIVITY 3: Building capacity

Three achievements in 2023 had a particularly significant impact.

In the area of **cyber exercises and training**, ENISA developed a new exercise solution, known as the Blue Room, utilising it for the first time during the organisation of national exercises in Portugal. Both activities are good examples of ENISA's approach to supporting the organisation of cyber exercises in the light of the provisions of the CSA. ENISA helps a number of stakeholder communities in the EU to organise such exercises, either annually or every other year. The most notable examples are the exercises organised for the Computer Security Incident Response Teams (CSIRTs) Network and the EU Crisis Liaison Network (EU- Cyclone) (the Cyclone Standard Operating Procedure Exercise (Cysopex) and the Blueprint Operational Level Exercise (Blue OLEX)), as well as the annual exercise organised in collaboration with the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), which targets EU institutions, bodies and agencies (EUIBAs) and the joint awareness & preparedness cybersecurity exercise (Jasper).

ENISA is also responsible for organising Cyber Europe, which takes place every other year and is one of the largest exercises of its kind in the world. Moreover, every year the need for the organisation of one or more ad hoc exercises arises due to the EU policy priorities at the time. An example is the exercise on EU elections, held in November 2023.

ENISA can no longer meet the ever-increasing demand for different types of exercises (national exercises, sectorial exercises, etc.) from a range of communities. The agency has, therefore, adopted a new approach to exercises: rather than organising and running and/or supporting an ever-increasing number of exercises, it will support communities to reach a maturity level that will enable them to organise their own exercises in the future. However, it is important to stress that the organisation of the exercises mentioned earlier (Cysopex, Blue OLEX, Jasper, Cyber Europe) will remain a priority for the agency. ENISA's aim is to continue to organise these exercises while helping relevant stakeholders to organise exercises along the lines of what is described in the CSA (e.g. ISACs, national exercises) without the need to commit additional resources.

This is why the development of the Blue Room exercise solution and its utilisation during the national exercises carried out in Portugal are considered important achievements in 2023: they pave the way for ENISA's new exercise and training strategy. Finally, it should be noted that, in spite of its attempts to support other communities, ENISA expects that members of the ENISA constituency will continue to ask for ENISA's full support in organising cyber exercises. With its current resources, ENISA can agree to such a request only if the requesting organisation meets the additional costs that ENISA will incur. For example, ENISA has signed a service-level agreement (SLA) with the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) for the organisation of eu-LISA's annual exercise.

Based on information collected from the organisers of national competitions, ENISA estimates that, across Europe, each year around 20 000 young people take part in the **European Cybersecurity Challenge (ECSC)** or **International Cybersecurity Challenge (ICC)**. The main objective of this is to try to increase the talent pool in the hope that this will eventually lead to the increased availability of skilled cybersecurity professionals.

This is a significant achievement for ENISA in an area of work that is not explicitly mentioned in the CSA (although the CSA does stress the need to address the increasing shortage of skills in Europe). Competitions such as the ECSC and ICC as well as national competitions, held throughout the EU, are an excellent way to promote the development of young cybersecurity talent. More and more European companies, authorities and organisations are recognising the value of these events and supporting the development of all these successful competitions, national and international. Competitions give organisations valuable insights into the education and skill levels of young people in their country and the capacity of their educational institutions, as well as the opportunity to attract young talent. Competitions not only inspire young people to consider a career in cybersecurity but also raise overall awareness of cybersecurity among the general public.

The EU has already recognised the shortage of skilled cybersecurity workers and has recently launched a number of initiatives to address the problem. One of the most promising initiatives is undoubtedly the establishment of the European Cybersecurity Competence Centre (ECCC), which aims to increase Europe's capacity and competitiveness in the field of cybersecurity and works with the network of national coordination centres (NCCs) to build a strong cybersecurity community in Europe. The ECCC, in collaboration with ENISA, and based on ENISA's experience of organising competitions since 2015, can help build a sustainable pan- European cybersecurity competition and related national competitions in European countries. ENISA needs to ensure that the competitions (at least the European and international finals) are well financed. Since ENISA first became involved in the ECSC, back in 2015, the competition has, with the help of the organisers of national competitions across the EU, grown considerably, and it is now the largest event of its kind worldwide. This success is reflected in the performance of Team Europe, which came first in each the last two ICC finals. These European initiatives clearly set the standard for the rest of the world to follow. By partnering with ECCC we can ensure that the ECSC (and, more importantly, the national competitions that 'feed into' to ECSC) can grow further in the future.

For a number of years ENISA has been supporting MSs to develop, implement and assess their national cybersecurity strategies (NCSSs). In 2023, ENISA worked closely with experts in MSs, helping them to incorporate into their NCSSs new concepts introduced in NIS 2, such as peer learning events and peer review. In the coming years ENISA will continue to work on these new initiatives, fine-tuning the concepts piloted in 2023. Another important achievement during 2023 was the establishment of working methods and priorities for the NIS Cooperation Group's workstream on NCSSs.

Resources

Throughout the year, ENISA's Capacity Building Unit continued to support MSs in the implementation of the cybersecurity support action. This is deemed necessary because a considerable number of the activities funded under the support action relate to capacity building (namely exercises and training). This context is relevant for consideration of resource constraints.

The need to support MSs in the implementation of the cybersecurity support action had an impact on the unit's capacity to develop exercises and training for MSs and EUIBAs utilising ENISA's own training platforms/solutions. Progress could be accelerated by appointing project managers dedicated to coordinating the capacity-building activities of MS and EUIBAs (one project manager for each) and by the allocation of more financial resources to fund further outsourcing of development work. In this regard, it is relevant to mention the national exercise conducted in Portugal in 2023, which was supported by ENISA. Although this exercise was not part of ENISA's work programme, it gave ENISA the opportunity to test and further develop a new approach to supporting MSs, that is by in setting and conducting a cyber exercise using ENISA's platforms, with ENISA playing the role of the service provider. The experience of this exercise helped the agency to further develop the model and its associated training. This new service can be made available to EUIBAs that want to develop their own exercises.

In 2023, the agency accommodated the need to reallocate some resources to support other activities across the organisation, mainly related to the contribution to horizontal teams. This resulted in variations in available resources and in differences between the number of FTEs planned and the number actually allocated.

Overall assessment

Overall, capacity-building activities had a significant impact, especially the use of the new service models and platforms developed by ENISA. This new approach also led to the development of a new service offering for MSs and EUIBAs (the Blue Room).

The assessment of activities outputs reveals a commendable alignment with strategic objectives, demonstrating a well-balanced performance and justifying its continuation. The results achieved are commensurate with the resources invested, reflecting a good balance that should be maintained, although additional resources could further increase the impact and help meet the growing demand. The assessment of key performance indicators (KPIs) reveals an overall positive trend, reflecting the effectiveness of ENISA activities.

In 2025, activity 3 (building capacity) will be merged with activity 9 (outreach and education). Over the last 3 years ENISA has explored opportunities for synergy between these two activities.

Objectives

- Increase the level of preparedness, capabilities and cooperation within and between Member States and sectors and EU institutions, bodies and agencies
- Prepare and test capabilities to respond to cybersecurity incidents
- Foster interoperable, consistent European risk management, methodologies and risk assessment practices
- Increase skill sets and align cybersecurity competencies

Results

- Enhanced capabilities across the community
- Increased cooperation between communities

Link to strategic objectives (ENISA strategy)

- Cutting-edge competences and capabilities in cybersecurity across the EU

Outputs	Outcome
3.1. Assist MSs to develop, implement and assess NCSSs	The output focuses on assisting MSs to develop, implement and assess NCSSs through ENISA's NCSS services catalogue. In 2023, ENISA provided training to 30 national stakeholders from 15 MSs on national-level risk assessment based on the *Interoperable EU Risk Management Toolbox* (https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox). In addition, ENISA, in collaboration with the Slovakian Cybersecurity Competence and Certification Centre, organised a peer learning session on cybersecurity skills within the NCSS context, attracting 20 participants from five MS. These endeavours have significantly contributed to fostering community building and knowledge exchange among NCSS stakeholders, one of the core strategic objectives of the agency. Moreover, ENISA research on best practices in active cyber protection and peer reviews at the national level helped establish a shared understanding of the topics, that will serve as a foundation for advocating active cyber protection policies and implementing peer review initiatives at the national level and assist NIS Cooperation Group workstream 9 in its attempts to establish related policies. To enhance visibility and assist MSs more effectively, ENISA once more redesigned its central reference point, the NCSS interactive map. These repeated redesigns enable centralised storage and dynamic sharing of best practices, lessons learned and shared experiences in a user-friendly manner. Finally, significant effort was devoted to establishing a work method and priorities for the NIS Cooperation Group's workstream on NCSSs. In this respect, ENISA, in its role as secretariat of the workstream, actively supported the chair to set the group's priorities for 2024–2026 in support of NIS 2. ENISA's activities in this area in 2023 included the following. • It established a working method and priorities for the relevant workstream of the NIS Cooperation Group. • It supported the use of its good practice guide (*NCSS Good Practice Guide – Designing and implementing national cyber security strategies*; https://www.enisa.europa.eu/publications/ncss-good-practice-guide), for example during the Swedish Audit Office's review of government measures to bolster information and cybersecurity. The report is publicly accessible in Swedish (8). • It organised the first training session on national level-risk assessment, drawing 30 national experts from 15 MSs. • In collaboration with the Slovakian Cybersecurity Competence and Certification Centre, it facilitated the first ever peer learning session in Bratislava, focusing on cybersecurity skills development. In addition to the activities originally planned for 2023 under the NCSS activity, considerable effort was expended in planning and leading the work of the NCSS workstream under the NIS Cooperation Group.

(8) https://www.riksrevisionen.se/download/18.4aeb2da8187b22973fb2828/1682339418438/RiR_2023_8_rapport.pdf.

3.2. Organise large-scale biennial exercises and sectorial exercises	Output 3.2 involves running small- and large-scale sectorial exercises, simulating crises at the national and EU levels. In 2023, ENISA exceeded its target of running five exercises. Owing to high demand from stakeholders, seven exercises were carried out. The exercises planned for 2023 were four technical exercises (CyberSopex the cyber standard operating procedure exercise (Cysopex), Jasper and the EU LISA VIS) and one tabletop exercise (Blue OLEX), for all types of stakeholders like the MSs, the two networks (EU-Cyclone, CSIRTs Network) and EUIBAs. Two more exercises not originally planned, one technical exercise (a national exercise in Portugal) and one tabletop exercise (the European Parliament elections exercise), were also carried out. To achieve these results, ENISA developed a new exercise solution, with testing at intermediate stages, in anticipation of Cyber Europe 2024. Overall, more than 1 000 participants, from all 27 MSs and 10 EUIBAs, engaged in exercises organised by ENISA. This success suggests very high added value and an immediate uptake, suggesting that allocating more resources could further amplify its impact and meet the growing demand. In summary, in 2023, ENISA: • exceeded its target of running five exercises by running seven exercises, the two additional, unplanned, exercises being a national exercise in Portugal and an exercise related to the European elections (with the participation of 25 MSs); • developed a new exercise solution (the Blue Room); • engaged more than 1 000 participants from 27 MSs and 10 EUIBAs in the exercises.
3.3. Organise trainings and other activities to support and develop maturity and skills of CSIRTs (including NIS sectorial CSIRT), NIS cooperation group (NIS CG) and work streams, information sharing and analysis centres (ISACs) and other communities	In 2023, ENISA made significant strides in enhancing cybersecurity skills across Europe through a comprehensive training programme spanning online and physical formats. This initiative, rooted in output 3.3, aimed to empower diverse communities with the knowledge and capabilities necessary to navigate the ever- evolving digital landscape. **Reaching thousands online** The self-paced online training (SPOT) initiative proved immensely successful, attracting over 3 500 learners, who engaged with diverse courses tailored to their specific needs and backgrounds. This high engagement rate reflects the programme's accessibility and attractiveness. Moreover, ENISA, leveraging cybersecurity support action funding, provided access to the platform for approximately 1 600 individuals from authorities in MSs and for critical sector staff. This resulted in the completion of over 20 300 modules during the year, indicating that professionals on the frontline of cyber defence have a deep commitment to upskilling. **Training beyond the digital platform** Beyond the virtual realm, ENISA hosted two on-site Letra (learning and training) events, one at each of its Athens and Heraklion premises. These gatherings, adhering to the 'train the trainer' approach, equipped 59 participants with valuable knowledge and skills, further expanding the programme's reach. ENISA also collaborated with the European Security and Defence College to deliver training to 30 military personnel, showcasing the initiative's adaptability to cater to diverse audiences.

	Collaboration and specialisation Recognising the evolving needs of specific communities, ENISA partnered with the workstream on health, the NLO subgroup meeting on NCSS and the NIS Cooperation Group on Energy to deliver targeted training workshops. These sessions reached 27, 30 and 25 participants, respectively, demonstrating ENISA's commitment to addressing unique sector-specific challenges. **Looking ahead** Through this activity, ENISA has shown that it remains committed to building on its strong training foundation by expanding its training offering, for example by developing SPOT content so that it caters for specialised needs such as those of the CSIRTs Network and by leveraging the expertise of trained 'Letra' alumni through events co-organised with authorities in MSs. This initiative, meticulously mapped to the ECSF, represents a vital step towards establishing a skilled and resilient European cybersecurity workforce. If provided with sufficient funds and resources,
3.4. Develop coordinated and interoperable risk management frameworks	In accordance with the 2023 SPD, this output was not covered by the 2023 work programme due to insufficient resources.
3.5. Support the reinforcement of Security Operational Centres (SOCs) as well as their collaboration, assisting the Commission and Member States initiatives in this area in line with the objectives of the EU Cybersecurity Strategy in the building and improving of SOCs	The Ad Hoc Working Group (AHWG) on SOCs continued to support ENISA in providing valuable support to the Commission and MSs. Notably, the AHWG's three task forces (on SOC maturity, cyber threat intelligence (CTI) data exchange and playbooks) made significant progress, with public reports expected in 2024. Pre-publication versions were shared with the Commission and MSs through their participation in the AHWG. In addition, engagement with cross-border SOC consortia fostered dialogue on commonalities and how to promote CTI/data exchange between SOC ecosystems and hubs. Given the maturity of the digital Europe programme-funded cross-border projects, requests for assistance from the Commission and MSs have been less frequent, as more focus is placed on ongoing funded projects. Hence, it is proposed that output 3.5 be deprioritised in 2024 and that its budget be reduced and reallocated to outputs demonstrably aligned with the strategic objectives that are deemed by the Commission and MSs to be of higher priority. In summary, during 2023: • ENISA provided support to DG Connect on the cross-border SOC cybershield; • the AHWG's task forces on SOC maturity, CTI data exchange and playbooks made significant progress, and public reports (pre publication versions of which were shared with stakeholders such as DG Connect and MSs) are expected in 2024; • ENISA supported dialogue on commonalities and how to promote CTI/ data exchange between SOC ecosystems and hubs.-
3.6. Organise and support cybersecurity challenges including the European Cyber Security Challenge (ECSC)	In 2023, the European Cybersecurity Challenge (ECSC) reached new heights, with the event hosted in Hamar, Norway, from 24 to 27 October marking a significant milestone in the collective European endeavour to bolster cybersecurity skills and capabilities. A total of 34 teams participated, 29 from EU and European Free Trade Area (EFTA) countries and six from guest nations. Of the 340 contestants, 28 were women. The scale of participation in the challenge shows the growing importance of cybersecurity worldwide. The ECSC 2023 finalists were Germany, Switzerland and Denmark. This iteration of the ECSC not only facilitated the development of critical cybersecurity skills among young people, but also served as a vital platform for networking, sharing knowledge and fostering international collaboration. Moreover, the introduction of a new initiative, a training boot camp specifically for female participants, held just after the ECSC final, is an example of the ECSC's commitment to promoting diversity and inclusiveness within the cybersecurity domain. ENISA estimates that about 20 000 young people participate in national cybersecurity competitions each year. In addition to the main competition, the ECSC also featured OpenECSC, an open online platform that allows the public to practise and improve their cybersecurity skills by participating in an online capture the flag (CTF) competition. OpenECSC offers a wide range of challenges, designed to cater to different skill levels and interests. OpenECSC was used for ECSC promotion and was also used by some MSs as a qualifier platform for their national selection. OpenECSC also provided members of the public, regardless of age (ECSC has an upper age limit of 25 years), with the opportunity to hone their cybersecurity skills. The success of Europe's attempts to address the global cybersecurity talent gap is exemplified by Team Europe's performance at the ICC. Team Europe, a European team assembled by ENISA and composed of top performers from the ECSC and OpenECSC, showcased European cybersecurity expertise on the world stage, participating in, and winning, the ICC in San Diego, United States, in August 2023. Team Europe participated in various training and other preparatory activities, including boot camps, online training, public CTF competitions and CTF qualifiers. The aims of the preparatory activities, including qualifying competitions, were to assess candidates' strengths and weakness, to select the team members and to build team spirit. The activities were subsequently assessed to identify recommendations for future activities Overall, the 2023 ECSC and Team Europe's participation in the ICC demonstrates Europe's continued commitment to identifying and developing young cybersecurity talent and promoting collaboration and networking within the global cybersecurity community. The ECSC is the biggest competition of its kind worldwide and established the blueprint that ENISA used for the organisation of the ICC. ENISA's objectives for the ECSC are to improve the governance structure and future organisation through improvements in decision-making, sponsorship and funding programmes, and support for participating countries. In addition, ENISA hopes to improve the ECSC by offering additional types of challenges using online platforms such as Attack/Defence and OpenECSC, communication channels, and by linking it to the ECSF to identify potential skills gaps. ENISA also aims to support Team Europe's participation in the ICC by assembling a European team, holding boot camps and online qualifiers and providing training activities for young people.

Key performance indicator	Unit (of measurement)	Frequency	Data source	2022 results	2023 results/ target
Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents					
3.1. Increase/decrease in maturity indicators (9)					
Maturity of national cybersecurity strategies					
MSs' rating of the overall maturity of their cybersecurity strategy					
High maturity	Number	Annual	Survey	6	7/5
Medium maturity	Number	Annual	Survey	5	3/5
Low maturity	Number	Annual	Survey	0	4/0
Number of MSs using or planning to use ENISA's framework to measure the maturity of their national cybersecurity capabilities					
Already using	Number	Annual	Survey	2	1/3
Not using but planning to use	Number	Annual	Survey	9	7/7
Don't know or will not use in the foreseeable future	Number	Annual	Survey	2	3/4
Number of MSs that have set KPIs to measure progress in and the effectiveness of the implementation of their strategic objectives when drafting their NCSSs					
Already using	Number	Annual	Survey	9	7/5
Not set but planning to use	Number	Annual	Survey	5	3/5
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	0	0/3
The frequency in which MSs update their strategy to adapt to technological advancements and new threats					
Every 2–3 years	Number	Annual	Survey	1	1/3
Every 4–5 years	Number	Annual	Survey	12	7/8
Every 6 years or less often or don't know	Number	Annual	Survey	1	3/2
Sectorial ISACs coverage					
Percentage of NIS 2 sectors having an EU ISAC	%	Annual	Report	60 %	60 %
3.2. Outreach, uptake and application of lessons learned from capability-building activities					
Cysopex (number of improvements proposed by participants)	Number	Per exercise		5	5/3
3.3. The number of exercises executed annually					
Number of exercises executed annually	Number	Annual	Report	5	7/5
3.4. Stakeholder assessment of the usefulness, added value and relevance of ENISA's capacity- building activities					
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	97 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	77 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	80 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	96 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	97 %	NA
SOPEX series (CyberSOPEX, CYSOPEX, BLUEOLEX)					
Usefulness low	%	Per exercise	Survey	6 %	0 %
Usefulness medium	%	Per exercise	Survey	54 %	25,56 %
Usefulness high	%	Per exercise	Survey	40 %	74,44 %
Relevance low	%	Per exercise	Survey	7 %	5.93 %
Relevance medium	%	Per exercise	Survey	53 %	31.11 %
Relevance high	%	Per exercise	Survey	40 %	62.96 %
Cyber Europe exercise series (biannual)					
Usefulness low	%	Per exercise	Survey	6 %	NA
Usefulness medium	%	Per exercise	Survey	54 %	NA
Usefulness high	%	Per exercise	Survey	40 %	NA
Relevance low	%	Per exercise	Survey	7 %	NA
Relevance medium	%	Per exercise	Survey	53 %	NA
Relevance high	%	Per exercise	Survey	40 %	NA

(9) This KPI should be viewed as a reflection of performance over a number of years and not just in 2022. The 2022 KPI establishes the 'baseline' that allows us to gauge the evolution of the maturity indicator over the next few years

Jasper series					
Data to be made available as from 2023	%	Per exercise	Survey	NA	NA (10)
Usefulness low	%	Per exercise	Survey	NA	0 %
Usefulness medium	%	Per exercise	Survey	NA	41.5 %
Usefulness high	%	Per exercise	Survey	NA	58.95 %
Relevance low	%	Per exercise	Survey	NA	0 %
Relevance medium	%	Per exercise	Survey	NA	30.77 %
Relevance high	%	Per exercise	Survey	NA	69.23 %
3.5. ISACs maturity					
Number of exercises organised by EU ISACs	% (11)	Report		NA	
Number of training events organised by EU ISACs	%	Report		NA	2
Allocated FTEs as per SPD, based on full establishment at 2023 year end	13.75	**Number of FTEs actually used**		12	
Planned budget (EUR)	1 709 239	**Budget consumed (EUR)**		1 714 606.06	
		Of which carried over to 2024 (EUR)		331 204.55	

NA, not applicable.

(10) Pilot implementation; indicators not relevant for tracking.
(11) The percentage out of a total of 10 EU ISACs (as per NIS and NIS 2)

ACTIVITY 4: Enabling operational cooperation

Activity 4 is intended to promote operational cooperation among MSs and EUIBAs. The goal is to foster synergies across various cybersecurity communities, including civilians, law enforcement agencies and the cyber diplomacy and cyber defence sectors, as well as EU actors. The activity focuses on providing tools and platforms, exchanging best practices, offering advice and issuing guidance. In doing so, the activity contributes to the fulfilment of the strategic objective of effective cooperation among operational actors within the EU in event of massive cyber incidents.

In the context of this activity, in 2023, ENISA played a pivotal role in supporting the operations of the CSIRTs Network and EU-Cyclone and successfully carried out its scheduled tasks to facilitate the daily functions of these EU's incident response and crisis management networks.

In 2023, ENISA advanced operational cooperation between the CSIRTs Network and EU-Cyclone by orchestrating joint sessions under the Spanish and Swedish Presidencies. In addition, a team collaboration platform, operating as a unified platform for both networks, facilitated a seamless exchange of information, best practice and guidance, enriching the cybersecurity community's collective knowledge. ENISA further developed and maintained tools and platforms that serve both networks, ensuring ongoing support and enhanced functionality.

ENISA offered strategic guidance to the presidencies, emphasising the importance of concentrating on key deliverables that significantly contribute to the EU's cybersecurity landscape.

Furthermore, the initiation of the European vulnerability database (EU VBD) project marked a strategic move by ENISA to consolidate cybersecurity work across the EU. Starting as a common vulnerabilities and exposures numbering authority (CNA), ENISA is now able to assign identifiers to all EU companies requesting such a service. The development of the EU VBD enabled ENISA to integrate and repurpose existing databases and technical solutions, with the aim of presenting high-quality information to the public by the end of 2024.

The reallocation of resources from activity 4 to activity 5, to support the execution of the cybersecurity support action, significantly affected the operational capacity of the agency to carry out of this activity, particularly output 4.1, and necessitated a renewed focus on the development of internal expertise for output 4.2. Despite these constraints, the team adapted and maintained essential services, ensuring no interruption to the critical support provided to the CSIRTs Network and EU-Cyclone.

Considering the demand-driven nature of some services performed by the activity, certain tasks – particularly those requiring specialised knowledge – may in the future need to be handled by intra-muros contractors or project-focused staff (e.g. contract agents). However, it remains imperative that the majority of tasks are carried out internally, by staff with the necessary security clearance and seniority.

Stakeholders and users have consistently expressed high satisfaction with the activity's deliverables, as evidenced by the substantial increase in exchanges/interactions and the growth of the active user base for both EU-Cyclone and CSIRTs. The work on the EU VDB promises to be impactful and has been carried out in close collaboration with MSs.

It should be noted that this activity should look forward to 2025 and beyond; ENISA should further facilitate introspection and forward looking among the networks by preparing for the changed and changing ecosystem arising from NIS 2, the CRA, incident-reporting requirements and the CSOA. All of these work areas should be brought together in a coherent way, seeking synergies also by consolidating tools and infrastructures under an operational information technology (IT) umbrella. While limited consolidation has already taken place in 2023, further synergies in this area should be sought.

Looking beyond 2024, the 2025–2027 SPD has introduced adjustments to enhance operational effectiveness, notably by transferring two outputs to activity 4 – namely the cyber partnership programme and ENISA's international strategy and outreach work. This reorganisation aims to bolster efficiency and ensure a more cohesive approach to international cybersecurity collaborations. In line with this strategic evolution, the 2023 strategic workforce review stresses the need for the operational cooperation unit to expand, projecting a gradual increase in headcount of 4–7 FTEs through to 2026 to accommodate growing operational demands.

Objectives

- Enhance and improve incident response capabilities across the Union
- Enable effective European cybersecurity crisis management by continuously improving the cyber crisis management framework
- Ensure coordination in cybersecurity crisis management among relevant EUIBAs (e.g. CERT-EU, the European External Action Service (EEAS) and the European Union Agency for Law Enforcement Cooperation (Europol))
- Improve maturity and capacities of operational communities (CSIRTs Network, EU-Cyclone)
- Contribute to preparedness, shared situational awareness and coordinated response to and recovery from large-scale cyber incidents and crises across different communities (e.g. by providing *ex ante* services).

Results

- All communities (EU institutions and MSs) use a streamlined and coherent set of standard operating procedures (SOPs) for the management of cyber crises
- Efficient tools (secure & high availability) and methodologies for effective cyber crisis management

Link to strategic objectives (ENISA strategy)

- Effective cooperation among operational actors within the EU in case of massive cyber incidents

Outputs

4.1. Support the functioning and operations of the operational networks and communities and cooperation with relevant stakeholders including blueprint actors (12)

Outcome

In 2023, work undertaken within this output continued to facilitate seamless cooperation among CSIRTs Network and EU-Cyclone members to foster efficient EU operational networks and prompt incident response and cyber crisis management.

The output goals were to strategically advance information sharing and collaboration among CSIRTs Network and EU-Cyclone members, aligning with NIS 2 and CSA Article 7. This involved enabling strong cooperation and prioritising tools for efficient information exchange.

In the case of the CSIRTs Network, this involved supporting daily operations and 24/7 information exchange for 600 members.

- The technical support provided included arranging three plenary meetings of the CSIRTs Network and multiple meetings of working groups, as well as onboarding all new members of the CSIRTs Network.
- The coordination support provided included the organisation of Cybersopex, a shared session between CNW and EU-Cyclone under the Spanish Presidency and an informal session under the Swedish Presidency.
- The content support provided included the drafting of SOPs to facilitate crisis coordination. Three internal studies were also produced (on incident response in the EU, CVD guidelines and the CTI team kick-off).

Other important activities focused on improving situational awareness and threat research. For example, OSA, using tailored products, carried out research for the CSIRTs Network and EU-Cyclone and ENISA liaised between the two network**s** and produced foresight threats reports.

For EU-Cyclone, 2023 was a pivotal year as a result of NIS 2 coming into force and the consequent formalisation of the network. The ENISA EU-Cyclone secretariat team ensured daily operations and 24/7 information exchange and organised various meetings (four plenary meetings of EU-Cyclone officers, multiple working group meetings for officers and the EU-Cyclone executive meeting under the Swedish Presidency. This is also reflected in the two exercises in which EU-Cyclone members participated, namely Cysopex, for testing the SOP compliance and the readiness of EU-Cyclone officers, and Blue OLEX, to test interactions with high level executives,which was a significant success thanks to co-hosting with the EC and co-location with The One Conference in The Hague.

In 2023, the EU-Cyclone secretariat team worked on several deliverables based on stakeholders' surveys and requests from MSs during the Swedish and Spanish Presidencies.

Following the coming into force of NIS 2, the focus of the EU-Cyclone secretariat team's support was on rules of procedure and SOP (13) developments and products resulting from actions agreed upon with EU-Cyclone and needed to fulfil the requirements of NIS 2, such as reporting or fostering trust in the EU ecosystem and sectorial approaches.

(12) The CSIRTs Network, EU Cyclone, the SOCs network

(13) The rules of procedure are a set of rules governing the general operation of EU-Cyclone and cover topics such as decision- making and the roles of officers, executives, the Commission, observers, etc. The SOPs provide instructions related to escalation within the network. The added value of both documents is that they help structure internal processes, bring clarity and consistency among participants, and reduce ambiguity, especially in cases of escalation.

Both secretariat teams received positive feedback on their various activities from the CSIRTs Network, EU-Cyclone, the HWPCI, EUIBAs, and CSIRT/law enforcement. The feedback recognised the impressive work done by ENISA and also provided ideas for improvement. These will be considered, and depending on the availability of resources, may be implemented in the future.

It is important to highlight the work undertaken by the ENISA secretariat to prioritise and implement effective solutions, thus ensuring the continued delivery of services to the CSIRTs Network and EU-Cyclone. In 2023, this included the establishment of a backup function using existing resources that concentrated on content and coordination tasks.

4.2. Support coordinated vulnerability disclosure efforts by designing and deploying the EU Vulnerability Database (VBD)

Under NIS 2, ENISA is tasked with building a database of known vulnerabilities –the EU VDB – consisting of three components: (1) a description of the vulnerability; (2) a score / severity rating; and (3) information on patching and guidance from CSIRTs or competent authorities. Through this output, ENISA bolsters the EU's role in the CVD ecosystem because the database services will offer an alternative solution to EU companies looking for vulnerability management services. Following a successful onboarding process with MITRE (14), ENISA now has the authority to assign CVE identifiers for vulnerabilities reported by EU-based companies and will be able to assist European entities in becoming CNAs.

Overall, this action seeks to consolidate relevant data in a single location and provide an alternative for EU vendors disclosing vulnerabilities.

In 2023, ENISA carried out the following tasks in this area.

- It helped MSs to develop guidelines for implementing national CVD policies and established a CVD working group within the CSIRT Network to facilitate the update of CVD procedures and CNA policy. The agency also reached out to individual CNAs in the Netherlands, Poland, Slovakia and Finland, to learn from them and benefit from their experience in assessing vulnerabilities.
- It collaborated with MITRE to understand the vulnerability disclosure process in the United States and complete the onboarding process to become a CNA.
- It gathered input from MSs on the new EU VDB through a workshop in June 2023 attended by 60 individuals (CNW, external experts and representatives from industry partners from the EU, the United States and Japan).
- It worked with the members of the NIS Cooperation Group (dedicated workstream) and validated plans for setting up the database.
- It initiated a study on the concept of a vulnerability database (comparing MSs' current vulnerability databases).

In 2024, ENISA aims to finalise the procedures for reporting vulnerabilities and complete the design and features of the EU VDB, building on what was put in place in 2023 under this output. Beta testing before database release, as well as a technical and security (hosting) assessment, is also planned. Following the release, a user survey will be launched, to gather feedback.

(14) MITRE is a not-for-profit organisation that manages the common vulnerabilities and exposures (CVE) system, which catalogues publicly disclosed cybersecurity vulnerabilities and exposures in a standardised format for easy reference and analysis.

With additional resources, ENISA can further enhance the EU VDB and its internal expertise to assess vulnerabilities.

To facilitate the launch of the new EU VBD, a strategic shift in resource allocation was implemented. This realignment, which began in Q4 2023, aims to enhance staff capabilities and define key skills, guided by the ENISA competencies map, ensuring that the team is capable of assessing CVEs and assigning of identifiers to EU companies, in line with the established resources.

As mentioned in the adopted draft 2025–2027 SPD, by the end of 2024, the first parts of the EU VDB will be operational. This is a new system/service for operational tools, and additional budget will be needed for the effective deployment and operation of the two environments (pre-production and production).

4.3. Deploy, maintain and promote operational cooperation platforms and tools including preparations for a secure virtual platform for EU-Cyclone

In 2023, ENISA continued to support and maintain the tools and services provided to its operational stakeholders. This included hosting the MeliCERTes 2 (a CSIRTs collaboration platform) Tools Suite, also known as the CSIRTs Network central services, for the CSIRTs Network, as well as the infrastructure and tools for EU- Cyclone. The focus has remained on strengthening and improving incident response capabilities across the EU through common tools. ENISA has contributed to preparedness, shared situational awareness and effective cooperation among operational actors in the EU in response to a massive cyber incident.

Throughout 2023, ENISA continued to invest in the support, maintenance and security of the services offered to the CSIRTs Network and EU-Cyclone. However, given the agency's role as a service provider, its responsibilities, the sensitivity of the services offered and the variety of tools and technologies managed, additional resources are necessary to maintain the current level of support and to invest in further security controls as required by NIS 2.

The 2025–2027 SPD points out that additional budget is required for activity 4 to host IT operations.

In 2023, ENISA not only supported and maintained the tools and services provided to its stakeholders but also developed additional functionalities. These included various technical requirements, governance schemes and architecture, as well as installation and proper maintenance of tools, a helpdesk and support for the EU CSIRTs. The CSIRTs services (excluding MeliCERTes) are operational. The services include chat messaging, video teleconferencing, team management and orchestration, and file sharing. The project supports the activities of the CSIRT Network secretariat and is used by all MSs.

Other activities involved the maintenance, further development and adoption of technical requirements for EU-Cyclone, OpenCTI, the Open Cyber Situational Awareness Machine and the ISACs Platform, which involved revising the design architecture, installation, development, operation and maintenance.

In carrying out its work, ENISA defined the basic security measures for all operational cooperation tools, following international standards and complying with ENISA's internal guidelines and IT strategy. This output provides the technical expertise for the tools required for the ENISA cybersecurity support action.

Under this activity, planning for decommissioning of underutilised IT tools was initiated, with the aim of facilitating the transition to more efficient cloud and software as a service solution. This move aims to enhance the operational management of IT resources. Additional resources would further accelerate the shift to a robust infrastructure moving away from legacy systems, thus drastically reducing risks.

Key performance indicator Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation	Unit (of measurement)	Frequency	Data source	2022 results	2023 results/ target
4.1. Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA					
CSIRTs Network (% increase year on year)					
Active users (% increase year on year)	%	Annual	Platform	19 %	114 %/110 %
Number of exchanges/interactions year on year	%	Annual	Platform	104 %	134 %/110 %
EU-Cyclone					
Active users (% increase year on year)	%	Annual	Platform	2 %	109 %/100 %
Number of exchanges/interactions (% increase year on year)	%	Annual	Platform	548 %	218 %/100 %
4.2. Uptake of platforms/tools/SOPs during massive cyber incidents		Ad hoc	Platform	NA	NA (15)
4.3. Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs provided by ENISA	%	Biennial	Survey	89 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	94 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	84 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	83 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	94 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	87 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	94 %	NA

Allocated FTEs as per SPD, based on full establishment at 2023 year end	16.55	**Number of FTEs actually used**	7.73
Planned budget (EUR) (16)	2 122 530	**Budget consumed (EUR) (17)**	2 046 122
		Of which carried forward to 2024 (EUR)	796 093

NA, not applicable.

(15) Although the networks were in escalated mode, this situation was not deemed a large-scale cybersecurity incident as defined by NIS 2 Article 6 (7).

(16) Direct costs only.

(17) Direct costs only.

ACTIVITY 5: Contribute to cooperative response at Union and Member States level

ENISA's work under activity 5 aims to contribute to cooperative response at the EU and MS levels primarily through three main activities:

- Common situational awareness in cooperation with ms and eu entities, primarily dg connect, cert- eu, europol and europol's european cybercrime centre (ec3), the eu intelligence and situation centre and eeas security and defence policy – cyber security.
- Delivery of preparedness and incident response support services through the cybersecurity support action,
- Establishing a framework for partnering with private-sector players to contribute to the agency's understanding of threats, incidents and vulnerabilities, in direct support of the output of this activity and the agency's activities at large.

In doing so, this activity contributes to the fulfilment of the strategic objective of effective cooperation among operational actors in the EU in the event of a massive cyber incident.

In 2023 ENISA built on work carried out in 2022 to strengthen its capacity to monitor, collect data on and analyse cyber threats, incidents and vulnerability as well as its ability to work with MSs and EU entities to consolidate situational awareness reports and launched new dedicated services and ensured timely reporting on critical cybersecurity issues. Situational awareness serves as the overarching framework for all other actions within this activity, as it is centred on comprehending the present landscape of threats and vulnerabilities in order to prepare and responding adeptly. One of the key achievements in 2023 was a significant improvement in ENISA's capacity to monitor, collect and analyse cybersecurity events observed in the public domain. As a result of a strategic redesign of its collection and analysis processes, the agency witnessed a remarkable increase (of over 500 %) in its output.

Demonstrating strong collaboration within the EU cybersecurity ecosystem, ENISA, in cooperation with CERT- EU and Europol, continued to release EU-JCARs (18) incorporating input from selected MSs and private-sector organisations with which the agency has formed partnerships. ENISA has also continued to deliver joint rapid reports, and in 2023 published a joint publication to warn business and organisations in the EU about sustained threat activities. This was done as part of the structured cooperation with CERT-EU. In 2023, ENISA signed an agreement to contribute to the Commission Cyber Situation Centre, starting in 2024.

Overall, ENISA's achievements under this activity in 2023 showcase its commitment to strengthening Europe's cybersecurity posture through common situational awareness. By enhancing its monitoring capabilities, establishing new services and ensuring timely reporting, ENISA contributed to the EU's cybersecurity situational awareness. The agency has received positive feedback on its contributions to the EU Integrated Political Crisis Response, in particular its integrated situational awareness and analysis (ISAA) reports.

In addition to its contribution to situational awareness, the agency continued to strengthen its operational capabilities. In 2023, ENISA provided operational support to MSs through the operationalisation of the ENISA cyber support action. Through this programme the agency delivered preparedness (*ex ante*) and incident response support (*ex post*) services to MS.

In delivering these services, the agency has helped to increase the resilience of critical entities in the EU and their ability to respond to cyber threats. In 2022, the cybersecurity support action received funding of EUR 15 million from the European Commission as a short-term response to the call from EU ministers in charge of telecommunications for the implementation of a new Emergency Response Fund for Cybersecurity. A long-term plan for this fund is currently being negotiated under the CSOA. Owing to the success of the ENISA cyber support action, in December 2023 ENISA signed a contribution agreement with DG Connect to continue to provide *ex ante* and *ex post* services to the value of approximatelyEUR 20 million. The programme will continue until 2026 and is financed through the 2023–2024 digital Europe programme.

With regards to the operationalisation of a framework to enable collaboration with partners from the private sector, the agency focused on piloting the ENISA cyber partnership programme with selected private

(18) CSA Article 7(6).

entities. This programme aims to increase the agency's visibility and understanding of threats, vulnerability incidents and cybersecurity events. In 2023, ENISA established and tested an MoU, information exchange templates, onboarding processes and pilot exit criteria. As part of the pilot, the agency onboarded six selected private-sector partners and held the first threat information exchange workshop. In 2025, this output will be moved to activity 4, which focuses on building and managing operational communities and networks.

As highlighted in the previous annual activity report, the resources required to mount a cooperative response have been growing as a result of the evolving and increasingly complex threat landscape. As in 2022, the majority of this activity's resources go towards generating and consolidating the situational awareness portfolio of services, more precisely 5.6 FTEs and EUR 829 000 in budget. In 2023, the agency was able maintain the quality of its services in this area, despite the high pressure of implementing the cybersecurity support action.

In 2023, ENISA operationalised the cybersecurity support action. This required a reassignment of several resources within the agency, resulting in a total allocation of 11 FTEs. The reassignments benefited the cybersecurity support action at the expense of some of the planned outcomes in activity 5, which had to be deprioritised. In particular, the build-up of the cyber partnership programme and work on the EU Regular Situational Awareness platform were implemented at a pace that was slower than planned.

Regarding human resources and talent, the agency acquired the resources, in terms of competencies, needed to provide situational awareness capabilities in a timely and effective manner. The focus in 2024 is on acquiring the right talent for the cybersecurity support action as well for tasks related to the CRA.

In 2023, the agency's operational capabilities made some important steps forward. In particular, the successful delivery of the first year of the cybersecurity support action and the stabilisation and continuous improvement of the situational awareness programme increased MSs' and EU entities' trust in the ability of the agency to provide operational capabilities to the EU.

In 2024, the cybersecurity support action will, owing to its size in terms of operations and output, be carried out under a separate activity (activity 5B), and will be largely resourced in terms of both budget and human resources (19) using external financing (a EUR 20 million contribution agreement). The services provided will, however, be similar those ones provided in 2023, with minor adjustments based on stakeholder feedback and lessons learned from the programme this year.

The outputs related to situational awareness and the establishment of the cyber partnership programme will instead remain within activity 5A. Both of these outputs will see a slight increase in resources owing to the release of resources that in 2023 were assigned to the cyber support action, and this will allow ENISA to continue the delivery of the output as planned. The agency will seek further synergies and optimisation to be able to continue to deliver on the outputs planned under this activity, in particular the Commission Cyber Situation Centre, as well as other activities.

The agency will further strive to provide services that all MSs can use. It will aim to further build a common EU situational picture, working with a subset of MSs on a voluntary basis, with a view to extending this service to all MSs in the future.

Objectives

- Enhanced preparedness and effective incident response and cooperation among MSs and EU institutions, including cooperation of technical, operational and political actors during incidents or crisis
- Common situational awareness before and during cyber incidents and crises across the Union
- Information exchange and cooperation, cross-layer and cross-border, between MSs and as well as with EU institutions

Results

- Member States and institutions cooperating effectively during large-scale cross-border incidents or crises
- Stakeholders and public aware of current cybersecurity development

Link to strategic objectives (ENISA strategy)

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

(19) In December 2023, the agency launched a call to build up a reserve list of contract agents in function group 4 to support the needs of the 2024–2026 cybersecurity support action.

Outputs	Outcome
5.1. Generate and consolidate information (including to the general public) on common cyber situational awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information at the strategic, operational and technical levels (20)	The work under this output underwent a comprehensive transformation of its reporting processes. The OSINT report was revamped, including its format and underlying processes, to deliver more efficient and insightful information including in a machine- readable format. In addition, the Flash Report template was upgraded and the service catalogue was streamlined to enhance clarity and accessibility. In line with the NIS 360 strategy, ENISA introduced new, dedicated, services to address specific cybersecurity needs. These included the ENISA threat research service, which focuses on in-depth analysis of emerging threats, and the ENISA sectorial report, which provides tailored insights into the cybersecurity challenges faced by different sectors. The agency's achievements in this area can be summarised as follows. • ENISA positioned itself as a **key situational awareness player in the EU ecosystem** in the eyes of its partners from the EUIBAs and MS. In particular, the agency increased its presence in the **HWPCI** and at other high-profile meetings, such as meetings of the **Security Union**. ENISA is also among the situational awareness actors involved in the **Cyber Diplomatic Toolbox.** • The agency increased the speed of tracking, reviewing and analysing events, as a result increasing its throughput by 500 % compared with 2022 **to over 4 600** by mid-November 2023. • ENISA's **capacity to monitor, collect and analyse security events** was increased by streamlining and executing the Union Response for Situational Awareness (**URSA) strategy, together with KIT.** • The agency **onboarded three threat analysts** and achieved **100 % budget commitment**, ensuring business continuity for Q1 2024 for essential situational awareness services. • A **daily situational awareness call and report** were established. In addition, duty officer services were extended to provide **24/7 on-call** incident-reporting support within the cyber support action. • The **weekly OSINT report**, including format and processes, was transformed, the Flash Report template was upgraded and the service catalogue streamlined. During the year, the agency delivered 24 **weekly OSINT** reports with the new process/template, with a cyber security assessment tool **score of 4.4** • The agency continued to **deliver established services** such as the **Flash Report (63 issues)** and issued **ISAA reports related to Ukraine and Russian** and Israel-Hamas conflicts **(46).** The EU report services were discontinued. • Two new services were piloted: **ENISA threat research**, which provides in-depth technical analysis for the CSIRTs Network and, in collaboration with colleagues from the policy development and implementation unit, the **ENISA sectorial report (**as part of the NIS 360 strategy). • Three new EU-JCARs were released. Reports are now released quarterly and the pilot phase is deemed to be complete. A mechanism enabling **MSs** and **private partnership programme** participants to make voluntary contributions was established. • The agency strengthened its **structural cooperation agreement with CERT- EU**, and operational cooperation with Europol (in particular **EC3**) and the EEAS (in particular intelligence and situation centre (**INTCEN**) was upgraded. • A **methodology and processes** to enable the agency to work with external partners such as **international partners** and partners within the **ENISA cyber partnership programme** was established**.** A **comprehensive partnership ecosystem** will help deliver more **accurate**, **timely** and **effective** situational awareness. Despite the progress made in 2023, resource limitations continue to hinder the output's ability to consistently deliver timely and high-quality services that fully meet stakeholders' expectations. This concern is particularly acute in scenarios involving multiple, large-scale, cross-border events occurring simultaneously or consecutively. ENISA witnessed this phenomenon with the activation of multiple integrated political crisis response processes, which led the EU Commission to request input for the ISAA (21) report. The majority of the budget allocated to this output was used to fund the agency's situational awareness activities and to contract CTI services and CTI platform development. The 2023 budget was almost unchanged from that allocated in 2022, despite a notable increase in costs due to inflation observed in 2022–2023. In 2024 some of the framework contracts used to provide CTI services will expire and the agency will need to issue new tenders to meet its needs.
5.2. Support technical (including through MeliCERTes) and operational cooperation, incident response coordination and EU-wide crisis communication during large-scale cross- border incidents or crises	This output includes services under the cybersecurity support action. In 2023, ENISA: • Engaged 26 of 27 mss in using at least one support service; • Updated its catalogue of ex ante and ex post services and ensured its ability to deliver these; • Established and maintained a community of points of contact in every ms; • Provided tools and procedures for service request and delivery; • Operationalised the governance structure of service provision, ensuring service delivery on time and within budget; • Organised opportunities to exchange information and lessons learned with mss and gathered feedback from mss via regular online meetings, physical events and a feedback survey; • Coordinated the implementation of national-level requirements, legal support and translation support for service provision. In total, in 2023 within the cybersecurity support action, ENISA fulfilled 342 service requests. These requests resulted in: • 185 pen tests, • 54 exercises, • 25 threat landscape reports, • incident response support in 16 MSs, • risk monitoring for 19 MSs, • training for 25 MSs. While the agency has shown agility in reprioritising work and assignments, in 2024, the delivery of the cybersecurity support action will be financed primarily through direct hiring using the funds available to run the programme. This will release the resources reassigned to the programme and enable the agency to run its work programme activities with the planned resources. ENISA aims to continue its provision of support services in 2024, building on lessons learned in 2023. Using practical experience, ENISA will work to further engage MSs (in particular those countries whose engagement has been limited until now). ENISA will also continue to review and tailor its service catalogue.

(20) Advisory group proposal for standby emergency incident analysis team provisioned within output 5.1.

(21) https://eur-lex.europa.eu/eli/reco/2017/1584/oj.

5.3. Maintain, develop and promote the trusted network of vendors/suppliers for information exchange and

With regard to the operationalisation of a framework to enable collaboration with partners from the private sector, the agency focused on piloting the programme with selected private entities.

Building on the work done in 2022, the agency initiated the onboarding process with selected private-sector companies and established operational procedure that will allow ENISA to work closely with these partners to increase the agency's understanding awareness of cyber incidents and threats. The programme, the

ENISA cyber partnership programme, targets companies from around the world, and situational awareness across the whole supply chain, that have visibility on the global cyber threat landscape.

In 2023, ENISA:

- Established a cyber partnership programme (with a plan for 10 partners, to be onboarded in two phases), onboarded six partners in the first phase and signed two mous;
- Established and tested MoU and information exchange templates, onboarding processes and pilot exit criteria;
- Created operational process for information exchange through interlock with situational awareness;
- Conducted one workshop to support the judgement and assessment of an eu-jcar.

The resources assigned to this output were primarily used to onboard new partners under the first pilot phase and to start developing an operational procedure for information sharing, including standard operating procedures and tools for information exchange. Despite reallocating resources to the higher-priority cybersecurity support action, the agency was still able to complete the first pilot phase in 2023.

Key performance indicator ENISA's ability to support the response to massive cyber incidents	Unit (of measure-ment)	Frequency	Data source	2022 results	2023 results/ target (22)
5.1. Number of relevant incident responses ENISA contributed to as per CSA Article 7 (23)	Number	Annual	Internal data source	NA	NA (see indicator 5.2)
5.2. Number of incidents analysed/curated	Number	Annual	Internal data source	775	4 858 (24)
5.3. Number of high- visibility incidents analysed	Number	Annual	Internal data source	38	63
5.4. Number of large-scale cross-border incidents with high impact analysed	Number	Annual	Internal data source	13	14
5.5. Number of incident responses to which ENISA contributed			Cyber Assistance Mechanism	1	An incident response retainer is in place in 16 MSs, and within the cybersecurity support action contributed to eight incidents
5.6. Timeliness and relevance of information shared and expertise provided by ENISA to mitigate the effects of cyber incidents		Biennial	Survey	Postponed (25)	NA
5.7. Take-up of ENISA support services	Number	Annual	Report	NA	26 (26)
5.8. Number of trusted vendors	Number	Annual	Report	NA	6
5.9. Stakeholder satisfaction with ENISA's ability to provide operational support	%	Biennial	Survey	84 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	82 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	73 %	NA

(22) Targets were to be established once baseline results were recorded, which occurred after the adoption of the 2023–2025 SPD.

(23) Indicator has been superseded by indicator 5.2.

(24) As of November 2022 for the year 2023.

(25) The survey was postponed because a reprioritisation exercise resulted in the reallocation of (24) resources to the cybersecurity support action.

(26) All but one MS (i.e. 26 MSs) used at least one of the services offered under the cybersecurity support action.

% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	86 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	82 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	82 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	100 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	82 %	NA
Allocated FTEs as per SPD, based on full establishment at 2023 year end	10	**Number of FTEs actually used**		9.55 (in addition 4.25 FTEs through external services)	
Planned budget (EUR) (27)	913 512	**Budget consumed (EUR) (28)**		902 958.12	
		Of which carried forward to 2024 (EUR)		122 903.48	

NA, not applicable.

(27) Direct costs only.
(28) Direct costs only

ACTIVITY 6:
Development and maintenance of EU cybersecurity certification framework

ENISA's work under activity 6 encompasses actions that seek to establish and support the EU cybersecurity certification framework by preparing and reviewing candidate cybersecurity certification schemes in accordance with Article 49 of the CSA, at the request of the Commission or on the basis of the EU's rolling work programme. Actions also include maintaining and evaluating adopted cybersecurity certification schemes and participating in peer reviews. In addition, under this activity, ENISA assists the Commission by providing the secretariat of the European Cybersecurity Certification Group (ECCG) and co-chairing and providing the secretariat of the Stakeholder Cybersecurity Certification Group (SCCG). In doing so, the activity contributes to the fulfilment of the strategic objective of promoting a high level of trust in secure digital solutions.

In 2023, on cybersecurity certification, ENISA continued to engage with its stakeholders, notably the Commission and the MSs, and developed further expert content concerning draft, candidate and emerging cybersecurity certification schemes. In this way, ENISA fully met stakeholders' expectations regarding its work to promote a voluntary cybersecurity certification framework in the EU.

ENISA successfully helped the Commission and the MSs to:

- Adopt the first cybersecurity certification scheme by means of a dedicated commission implementing regulation on eucc;
- Analyse all options available to meet digital sovereignty requirements in the draft european cybersecurity certification scheme for cloud services (eucs);
- Continue consolidating the requirements to be included in the draft candidate cybersecurity scheme on 5g;
- Study and analyse various aspects concerning the cybersecurity certification requirements concerning ai, managed security services, the eu digital identification wallet and vulnerabilities handling for certified products, services and processes.

ENISA also continued to engage with selected stakeholders, including the AHWGs on the EUCC, the EUCS and the EU certification scheme for 5G networks (EU5G) as well as thematic groups stemming therefrom, such as those on AI and vulnerabilities handling. In addition, when invited by public authorities, designated ENISA certification staff attended dedicated meetings to discuss aspects of the cybersecurity certification framework and associated requirements with a range of stakeholders seeking to contribute to the cybersecurity certification framework.

Importantly, in terms of governance, ENISA continued to support the Commission's ECCG by co-chairing, with the Commission, the SCCG.

In terms of lessons learned, ENISA dialled down the pace of development, notably on EU5G, which was commensurate with the progress in the other two, much more mature, draft candidate schemes (i.e. EUCC and EUCS). This way ENISA consumed its scarce resources efficiently and in line with the priorities of the Commission and the MS.

Objectives

- Trusted ICT products, services and processes
- Increased use and uptake of European cybersecurity certification
- Efficient and effective implementation of the European cybersecurity certification framework
- Improvement in the security posture management of certified products, services and processes by applying continuous compliance monitoring for high assurance level

Results

- Certified ICT products, services and processes are preferred by consumers and businesses

Link to strategic objectives (ENISA strategy)

- High level of trust in secure digital solutions

Outputs

6.1. Drafting and contributing to the preparation and establishment of candidate cybersecurity certification schemes

Outcome

ENISA supported the European Commission in the establishment of the EUCC scheme implementing regulation, which was adopted at the end of 2023 by committee procedure.

ENISA continued the development of the EUCS, which will be delivered in early 2024 for ECCG opinion, and which introduces sensitive requirements on the protection against unlawful access to data. ENISA also proposed technical specifications to compensate for the lack of standards for the scheme: security controls and the evaluation methodology developed for the EUCS were submitted to the European Committee for Standardisation (CEN) - CENELEC for adoption and further maintenance, and are currently under adoption.

ENISA further developed the EU5G, and it is intended that a public consultation will be launched at the end of Q1 2024. ENISA, based on the discussions of the AHWG on EU5G provided the Global System for Mobile Communication Association (GSMA) with proposed enhancements to its Network Equipment Security Assurance Scheme (NESAS) documents (FS.16, FS.47, FS.50, FS.51); GSMA is processing these proposals, as well as ENISA's request that the GSMA submits the relevant parts of its documents to the European Telecommunications Standards Institute (ETSI) so that they become standards that can be easily referred to in the EU5G; this is similar to the 3rd Generation Partnership Project's request that ETSI technical specification 33.117 include a vulnerability analysis.

ENISA complemented the initial CSA process of schemes development by launching a feasibility study on AI so as to better anticipate and respond to requests received from the Commission. The feasibility study on certification strategies of AI carried out in 2023 explored the possibility of ensuring confidence in high-risk AI systems through certification, as envisaged by the AI Act. ENISA, with the support of a dedicated thematic group, is now assessing whether future cybersecurity requirements on AI that need to be met could/may be supported by cybersecurity certification, serving as presumption of conformity. This feasibility study also reused the methodology for sectoral cybersecurity assessments, which was developed by ENISA to support the determination of certification requirements and was tested within phase 1 of the EU5G, and then submitted to CEN-CENELEC for optimisation, adoption and further maintenance.

In 2023, ENISA continued the thematic group dedicated to analysing the conditions for vulnerability handling and disclosure of certified solutions. As part of the activity, ENISA gathered information from the schemes' AHWGs, to enablebetter understanding of the specificities of the EUCC, the EUCS and the EU5G. A pilot involving MSs and the Commission could provide some recommendations for reducing the level of provisions within the EUCC implementing act and leave some scope for interpretation to support state-of-the-art documentation.

In 2023, ENISA started to develop accreditation requirements as a new horizontal activity for all schemes and shared the proposed state-of-the-art document to support the EUCC scheme with other schemes. The aim is to progressively analyse and consider specificities and to come up with the optimal overall approach.

ENISA liaised with MSs to determine their priorities for the development and implementation of certification schemes, as well on their expectations and possible red lines. MSs were involved in scheme development through the AHWGs as well as through bilateral workshops (ENISA staff visited Spain and Sweden in 2023).

ENISA provided proactive advice and support to the Commission on the use of cybersecurity certification schemes to demonstrate conformity with other regulations (such as the eIDAS/wallet, the AI Act and the CRA). Such schemes could already be in existence and, if necessary, adapted, or new schemes could be developed.

In 2023, ENISA proactively supported DG Connect by reviewing the essential requirements of the CRA, in conjunction with the provisions of the EUCC, and by reviewing the categories of CRA critical products in conjunction with the lists of products certified to date. ENISA also proposed notifying CRA assessment bodies of similar requirements that would apply to Conformity Assessment Bodies (CABs), allowing the community of CABs to better address the CRA and CSA 'worlds', and easing the future establishment of presumption of conformity to the CRA through CSA certificates. ENISA also expects that it will be necessary to harmonise the provisions of the CRA with non-EU assessments on consumer products, and for this reason participated in an EU–US dialogue on a possible common software bill of materials (SBOM).

Following a short study on certification of the European digital identity wallet in 2022, in 2023 ENISA was formally requested to lead the work on defining certification requirements; this activity is an essential aspect of citizen security, but is also an activity on which MS opinions are varied. The work resulted in a market study on the security mechanisms that will be available on mobiles in 5 years. The next important milestone is the delivery of EUDI wallet certification principles (due by end of Q1 2024), which will make possible the reuse of the EUCC, as well as an EU5G approach to certify embedded Universal Integrated Circuit Card (eUICCs) that can host wallet applets.

At the request of the Commission, and to support the negotiations on the amendment of the CSA related to the possibility of certifying managed security services, in 2023 ENISA provided the Commission with some key figures on the market and conducted a survey of MSs' existing activities and priorities. It also, in conjunction with awareness raising and education team, carried out a 360° review of MS skills in this area.

6.2. Implementing and maintaining established schemes, including evaluation of adopted schemes, participation in peer reviews, etc.

In 2023, ENISA developed state-of-the-art documents to support the implementation of the EUCC scheme.

- Nine existing SOG-IS documents were transformed by ENISA in 2023 into EUCC state-of-the-art documents supporting the EUCC scheme and were endorsed by the ECCG.
- ENISA, in coordination with the AHWGs, developed two new documents (accreditation of Information Technology Security Evaluation Facility and vulnerability handling) and invited the most mature MSs providing SOG-IS certificates to transform their national interpretations into four EUCC state-of-the-art documents (an on- going task). Based on the recent negotiation of the EUCC IA, a need for new state-of-the-art documents in the short term, concerning in particular the authorisation of CABs, been identified.
- ENISA developed, with the EUCC AHWG and the SOG-IS community – including MSs – a proposed organisation for the maintenance of the EUCC scheme. This approach should be further analysed under Commission governance once the EUCC has been formally adopted.

6.3. Supporting the statutory bodies in carrying out their duties with respect to governance roles and tasks

The ECCG, composed of representatives of national cybersecurity certification authorities and other related authorities of MSs, received regular updates on the main projects related to the market, certification and standardisation, and the schemes under development.

ENISA supported the Commission by preparing agendas and organising meetings (four in total) in 2023, analysing and processing the initial comments of the ECCG members on the draft of the EUCC implementing act. Together with a subgroup of the ECCG, ENISA drafted an initial proposal for a maintenance model for EUCC, which was subsequently discussed by the full ECCG. On the draft EUCS, ENISA supported the ECCG in the ongoing discussions and proposed several approaches and possible solutions for consideration by the ECCG. On the first steps of development of the EU5G draft candidate scheme, the outcome of a gap analysis was presented. It provided an overview with what is currently in place under the GSMA and what should the requested draft candidate scheme should cover resulting from the EU5G activities.

ENISA also presented its certification strategy and the feasibility studies proposal, both of which were endorsed by the ECCG. It also prepared the first initiatives of an ECCG cryptography subgroup, and the subgroup was established.

The SCCG, established in June 2020, is an advisory group and acts as sounding board for the Commission and ENISA when it comes to cybersecurity certification. It is composed of representatives from industry and consumer groups, small and medium-sized enterprises (SMEs), academia, cybersecurity certification interest groups and trade association groups. The group met three times in 2023. During these meetings Commission policy updates were presented and discussed. Scheme developments and related projects and reports were presented by ENISA and discussed. Topics for discussion put forward by SCCG members included the need for a security label, the need for harmonisation from industry perspective, the possibility of composition of certificates and reuse of evidence, the involvement of stakeholders in scheme development and the role of the SCCG was another topic of discussion (more specifically related to the cloud scheme discussions).

The SCCG welcomed the initiative to carry out feasibility studies on EU regulatory initiatives on cybersecurity certification and to involve of stakeholders, as the SCCG's role is limited. As in 2022, SCCG was invited to contribute to the programme of the ENISA cybersecurity certification conference in April 2023.

6.4. Developing and maintaining the necessary provisions and tools and services concerning the Union's cybersecurity certification framework (incl. certification website, support the Commission in relation to the core service platform of CEF

ENISA further developed and published the first version of its cybersecurity certification website, which is composed of two main parts. In the first main part, a dashboard displays schemes and supporting documentation, the catalogue of certificates and a directory of key certification stakeholders (NCCA and notified bodies).

A back-office function provides application programming interfaces to conformity assessment bodies issuing certificates. Associated processes were presented and discussed with the MSs, the ECCG and the SCCG.

ENISA supported the Commission in the development of the Connecting Europe Facility platform, which enables cybersecurity certification stakeholders to interact with each other. ENISA and the Commission have developed use cases concerning stakeholders' interactions. Examples are proposals for European Union Common Criteria, Protection Profile developments and looking for other stakeholders to create alliances for European funding calls.

In 2023, ENISA organised two hybrid editions of cybersecurity certification weeks, one in May (in Athens) and one in November (in Malaga), bringing together the various AHWGs and the thematic group on vulnerability handling. These weeks allowed interactions and synergies among the schemes' participants and gave ENISA the opportunity to update participants on new legislation that may affect the schemes or reuse their certificates (such as the CRA and the eIDAS regulation/wallet), as well as on the newly introduced AI feasibility study.

In the May session, the cybersecurity certification conference was organised as a hybrid event, gathering more than 800 participants online and 200 in person. The Commission, the MSs, ESOs, industry representatives, CABs, the European cooperation for Accreditation and ENISA were invited to provide updates on schemes and legislative developments and discussed possible associated impacts and opportunities. The November session comprised an ECCG meeting.

ENISA showcased certification at several external events, participating as exhibitors or speakers. Leveraging material (video, infographics) created in collaboration with the awareness-raising and education team, the goal was to increase understanding of and promote EU certification.

In coordination with stakeholders such as NCCAs, the Commission, etc., ENISA contributed to various EU cybersecurity conferences organised by parties such as the European Cyber Security Organisation, CEN-CENELEC, ETSI, International Conference on Common Criteria, Forum International de la Cybersécurité (FIC), IT Security Fair and Conference (IT-SA) and European Cyber Week (EUCW) as well as to the European 5G Conference and The One Conference.

Key performance indicators **Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions** Effective preparation of candidate certification schemes prepared by ENISA	**Unit (of measure-ment)**	**Frequency**	**Data source**	**2022 results**	**2023 results/ target**
Metrics					
6.1. Number of stakeholders (public authorities and/or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions	%	Annual	Survey	86 %	91 % / 50 %
Submetrics					
Percentage of respondents using (planning to use) the cybersecurity schemes to have solutions certified	%	Annual	Survey	29 %	16 % / NA
Percentage of respondents using (planning to use) the cybersecurity schemes to provide certified solutions	%	Annual	Survey	32 %	25 % / NA
Percentage of respondents using (planning to use) the cybersecurity schemes to certify solutions	%	Annual	Survey	44 %	44 % / NA
Percentage of respondents referring (planning to refer) to certifications within regulations	%	Annual	Survey	44 %	37.5 % / NA
Percentage of respondents planning to use the EUCC	%	Annual	Survey	57 %	78 % / NA
Percentage of respondents planning to use the EUCS	%	Annual	Survey	52 %	47 % / NA
Percentage of respondents planning to use the EU5G	%	Annual	Survey	NA	56.25 % / NA
Percentage of respondents that need ENISA's assistance to prepare for using the EU certification schemes	%	Annual	Survey	76 %	68.7 % / NA
6.2. Stakeholders' trust in digital solutions for certification schemes (citizens, public sector and businesses)	%	Biennial	Survey	74 %	NA
6.3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework	%	Biennial	Survey	73 %	NA

6.4. Number of candidate certification schemes prepared by ENISA	Number	Annual	Numerical	Three, in different stages of adoption	3/2.25 (Minimum 75 % of schemes formally requested to be under ongoing development)
6.5. Number of people/ organisations engaged in the preparation of certification schemes	Number	Annual	Numerical	Approximately 150	150 / minimum of 10 organisations and 10 individual experts; 50 % of MSs to join an AHWG; 30 % of organisations to be an SME; 5 % to be from a non-EU country
6.6. Satisfaction with ENISA's support for the preparation of candidate schemes	%	Biennial	Survey	82 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	75 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	88 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	75 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	75 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	83 %	NA
% of stakeholders satisfied with ENISA's community- building actions	%	Biennial	Survey	93 %	NA
Allocated FTEs as per SPD, based on full establishment at 2023 year end	9	**Number of FTEs actually used**			7.71
Planned budget (EUR) (29)	804 578	**Budget consumed (EUR) (30)**			798 665
		Of which carried forward to 2024 (EUR)			428 207.78

NA, not applicable.

(29) Direct costs only

(30) Direct costs only; resources related to the ongoing EU5G were not utilised, except in small part, in view of timing constraints and the absence of due delegation as long as meeting formal requirements remained work in progress in a multistakeholder environment.

ACTIVITY 7: Supporting the European cybersecurity market and industry

ENISA's work under activity 7 encompasses action to support stakeholders in terms of market analysis and standardisation, as well as good practices and vulnerabilities handling for certified products, services and processes. In doing so, the activity contributes to the fulfilment of the strategic objective of fostering a high level of trust in secure digital solutions.

In terms of achievements, standardisation has emerged as a staple and impactful activity. It has involved exploring relations with European standards organisations (ESOs) and carrying out gaps analyses of standards relating to important policy areas and to cybersecurity certification. Throughout 2023, ENISA's cooperation with selected ESOs came under scrutiny. Proposals for completely new European standards have recently emerged as a result of the growing prominence of the role of ENISA in cybersecurity certification. In recent years three such proposals have been submitted to and accepted by CEN-CENELEC, and in 2023 one such proposal reached the voting stage. Furthermore, ENISA continues supporting the cybersecurity standardisation community by means of a well-attended annual conference that is co-organised with CEN-CENELEC and the ETSI.

The area of cybersecurity market analysis is a recent addition to ENISA's remit, a result of the introduction of specific provisions in the CSA. Each year, ENISA, on the basis of an adopted methodology, analyses a market segment with a view to providing market insight in a way that cuts across technology and organisational requirements in that segment. In 2023, ENISA focused on the market for cryptographic products and produced a report that brought together data and analysis on all aspects of the agency's work, for example cybersecurity index, operations and research. In addition, an AHWG supported this activity and a thematic conference was organised to generate stakeholder interest in this emerging area.

In terms of good practices, ENISA launched a targeted analysis of open-source software testing in expectation of the coming into force of the CRA. As this is a primer for ENISA involvement in open source as a potential policy area, the outcomes have been evolving.

Finally, in the increasingly mature area of vulnerabilities handling for certified products, services and processes, ENISA continued to interact with a dedicated thematic group composed of experts appointed to the AHWGs on certification.

Budgetary constraints and changing policy requirements, particularly those stemming from the CRA, have necessitated a reprioritisation of ENISA's activities. However, the inclusion of market analysis in the CRA in a way that enables ENISA to support the market and standardisation is expected to be of benefit to both the Commission and MS' market surveillance authorities. Experience in data collection and market analysis will enable ENISA to make an invaluable contribution to other structured tasks under the CRA. It follows that vulnerabilities handling (output 7.4) can be merged into certification (activity 6) and that good practices (output 7.3) can be discontinued.

Objectives

- Improve conditions for the functioning of the internal market
- Foster a robust European cybersecurity industry and market

Results

- Contribution towards understanding market dynamics
- A more competitive European cybersecurity industry, SMEs and start-ups

Link to strategic objectives (ENISA strategy)

- High level of trust in secure digital solutions
- Empowered and engaged communities across the cybersecurity ecosystem

Outputs

7.1. Market analysis on the main trends in the cybersecurity market on both the demand and supply sides, and evaluation of certified products, services and processes

Outcome

In 2023, ENISA analysed aspects of the cybersecurity market by focusing on the market for cryptographic products and services. This thematic area was chosen because it is complementary to cybersecurity certification and is in line with the agency's previous work on the analysis of cryptographic products and services. This output also includes work on operational cooperation, the EU CSI and research and innovation (R & I).

In addition, the Cybersecurity Market Analysis Conference was, for the first time, arranged as a stand-alone, hybrid event.

ENISA was supported in these activities by the dedicated AHWG on EU cybersecurity market analysis.

More details on the abovementioned activities are provided below:

- **Cybersecurity Market Analysis for Cryptographic Products and Services.** This report provides data, a market overview and analysis, and it seeks to make observations on the actual state of the market of cryptographic products and services. The report was based on a combination of a desktop study, in-house ENISA and third-party expertise and data collected by means of a survey. The analysis provided an insight into the needs and requirements of stakeholders and of users of cryptographic products and services. It identified trends and potential problems that could result in European capacity being insufficient to meet demand. The approach followed in the cybersecurity market analysis was largely interdisciplinary, constrained as it was by limited internal resources in terms of data analysis tools and economics. ENISA addressed these limitations by engaging external experts and to some extent by tailoring goals to match the capacity available.
- **The 2nd ENISA Cybersecurity Market Analysis Conference.** This conference was organised as a hybrid event and brought together around 150 stakeholders, including suppliers and consumers of cybersecurity services, as well as some involved in market analysis; policymakers; regulators of cybersecurity products, services or processes; and research organisations (https://www.enisa.europa.eu/events/enisa-cybersecurity- market-analysis-conference-2023).
- **AHWG on EU cybersecurity market analysis.** This group provided knowledge and support, for instance by selecting the market segment to be analysed, scoping and analysing that segment, and developing the survey and validating the results. It also helped to draw up the programme for the Cybersecurity Market Analysis Conference and contributed to the development and validation of the report on the market for cryptographic products and services. The mandate of the AHWG formally expired on 16 November2023.

Finally, the small amount of resources required for this output was made available by redistributing resources from other outputs under this activity. The activity also contributed to the recasting of outputs to accommodate the advent of the CRA with its prominent disposition of competences for ENISA in the market area.

7.2. Monitoring developments in related areas of standardisation, analysis of standardisation gaps and establishment and take-up of European and international cybersecurity standards for risk management in relation to certification	In 2023, the output followed the directions for standardisation described below. • **Contacts with standards-developing organisations.** This involved maintaining contacts, participating in meetings of and liaising with multiple relevant technical committees (e.g. in the ETSI, CEN-CENELEC as well as private initiatives including GSMA, the 3rd Generation Partnership Project and Global Platform) and establishing cooperation with the O-RAN Alliance, notably in the area of 5G. ENISA remained in close contact with the ETSI and the Commission in an effort to better determine the future of the relationship between ENISA and ETSI, in line with the CSA and the evolving requirements of cybersecurity certification and standardisation. ENISA, along with CEN-CENELEC and ETSI, also co-organised the Cybersecurity Standardisation Conference, participated in other conferences and was involved in discussions with other ESOs. In addition, one internal report, *Methodology for Assessment of Standardisation activities*, was revised. • **Support for policy.** ICT products and services supply chain security. • **Support for certification.** Mapping of CRA requirements to standards. In this way, ENISA supported the Commission in relation to standardisation instruments that support policies regarding access of products of the digital single market, notably as set out in the CRA. ENISA also analysed existing standards relating to supply chains and identified gaps and made recommendations. This output helped to strengthen relations between ENISA and CEN, CENELEC and the ETSI and paved the way for a durable relationship with ESOs. There is a well- founded expectation that the ETSI is about to propose a deeper cooperation with ENISA and will support ENISA's participation in the 3rd Generation Partnership Project. Also in 2023, ENISA, with CEN-CENELEC and ETSI, organised the Cybersecurity Standardisation Conference, which has become one of the best-attended conferences in its field delivering information and opinion to thousands of registered attendees.
7.3. Guidelines and good practices on cybersecurity for ICT products, services and processes and recommendations to the EC and the ECCC	In 2023, a new definition for this output was conceived and approved, as the definition was no longer relevant. It was determined that an approach focused on the requirements of the CRA concerning the self-assessment of products with digital elements that contain open-source code would be appropriate. The purpose of the resulting report was to provide guidance to stakeholders that carry out testing of their products to meet the self-assessment level required under the CRA. It is likely that up to 90 % of products with digital elements will qualify for self-assessment. Furthermore, it is estimated that, as over 80 % of software is based on open-source components, the open-source community would be well served by suitable ENISA guidance. This deliverable brought ENISA into contact with a new stakeholder group. More broadly, it is expected that output 7.3 will eventually be discontinued owing to limited resources and the overall requirement to meet the expectations of the CRA. Under the market analysis output, a dedicated CRA preparation team will carry out Commission-related tasks while continuing to serve the needs of selected stakeholders. This requirement will be met over time in a way that is proportionate to the resources available.
7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services	The thematic group on vulnerability handling for certified solutions continued to support this analytical output, which provides input to activity 6 on cybersecurity certification. Certification of products, services and processes remains the centrepiece of the vulnerability-related work of this output. The group operated as a horizontal layer across certification schemes, notably EUCC, EUCS and EU5G. The resulting guidance for the vulnerability handling has been used by the EUCS and the EU5G (as the requirement for the EUCC has already been met). Output 7.4 will eventually be merged with activity 6 owing to limited resources and because the overall requirement for it as a horizontal activity has been met as a result of the sound work carried out in previous years.

Key performance indicator Effectiveness of ENISA's role in supporting participants in the European cybersecurity market	Unit (of measurement)	Frequency	Data source	2023 results	2024 results/ target
7.1. Number of market analyses, guidelines and good practices issued by ENISA	Number	Annual	Reports	2	6 /1
7.2. Uptake of lessons learned / recommendations from ENISA reports	%	Annual	Survey	49 %	61 % / 60 %
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work	%	Biennial	Survey	88 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	88 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	84 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	72 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	93 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	94 %	NA

Allocated FTEs as per SP, based on full establishment at 2023 year end	6	**Number of FTEs actually used**	6.1
Budget planned (EUR) (31)	356 027	**Budget consumed (EUR) (32)**	291 133.89
		Of which carried over to 2024 (EUR)	62 464.14

NA, not applicable.

(31) Direct costs only.
(32) Direct costs only

ACTIVITY 8:
Knowledge on emerging cybersecurity challenges and opportunities

ENISA's work under activity 8 provide 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 serves the purpose of providing topic-specific recommendations and general assessments on the impact of cybersecurity requirements and challenges. In doing so, the activity 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. Activity 8 met its objectives for 2023.

KPIs revealed that ENISA had a notable impact on identifying recommendations, analysis and challenges, and that it delivered the results expected. It is worth mentioning the high outreach of the outputs of activity 8, which showcases and points to an increased uptake of ENISA recommendations.

One of the major achievements of activity 8 is the EU CSI, which aims to assess the level of cybersecurity maturity across the EU using a series of qualitative and quantitative indicators, metrics for which are collected by MSs and using external sources. ENSIA's work on the EU CSI 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. All 27 MSs actively participated in the pilot that was run in 2023. The framework was also validated by the NIS Cooperation Group and the CSIRTs Network, as well as by the NLO (National Liaison Officers) Network.

The EU CSI exemplifies the vision of activity 8 by consolidating various pieces of information and analysing them in order to provide evidence for the assessment of the EU level of cybersecurity. The work that ENISA has carried out so far has been mostly of a preparatory nature. However, from 2024 onwards, and with the operationalisation of the EU CSI, as one of the main sources for the NIS 2 Article 18 report, further work by ENISA is expected to ensure that the EU CSI is useful to MS. In particular, ENISA's future work should focus on ensuring that MS can use the information included in the EU CSI to assess and improve their NCSSs, monitor policy effectiveness, strengthen the peer review process and boost their resilience. Accordingly, and in line with the overall vision for the EU CSI - as an effective instrument that will provide evidence to guide and support MSs' endeavours to improve their cybersecurity posture. ENISA will aim for this work to be more aligned with ENISA activities on NCSS, NIS investments and the policy observatory. It should also be pointed out that ENISA has developed a platform to support the collection of data for the EU CSI, which can also serve and empower MSs to conduct national-level exercises. In 2023, 24 of the 27 MSs utilised ENISA's platform. Finally, while effort has been made to reflect all dimensions of the cybersecurity ecosystem in the EU CSI, there is room for improvement when it comes to data on market and Research and Innovation (R & I). In this respect, further alignment with partners operating in these domains, such as the ECCC, should be pursued, to optimise synergies and ensure that the EU CSI is more coherent.

A further highlight of activity 8 involves ENISA's work on threat landscapes and foresight on emerging and future cybersecurity challenges. ENISA's outputs have significantly grown in terms of outreach, media mentions and references, thus highlighting the impact of this work. A notable achievement is the internal consolidation of knowledge management and information relevant to threat landscapes and situational awareness. The agency now has a single, consolidated platform for the collection, analysis and processing of relevant information. As a next step, alignment and coordination of the delivery of situational awareness and threat landscape products should be promoted to optimise internal resources, but also ensure the coherent delivery of relevant products to MSs and cybersecurity stakeholders. Moreover, strategic foresight has been institutionalised as a horizontal means to provide future guidance for ENISA's efforts, and threat landscapes have become a reference point both internally and externally to understand the current cybersecurity state.

When it comes to lessons learned, it is essential to note one of the main objectives of this activity, namely that of consolidating cybersecurity information and knowledge to support MSs and the ecosystem, as well as to promote internal synergies at ENISA through a comprehensive understanding of different cybersecurity dimensions. While the EU CSI and the work on threat landscapes are prime success cases, there is still room to grow as far as agency-wide information management is concerned. Additional pools of information from other ENISA activities, for example market analysis, situational awareness, R & I, can potentially be integrated with the information gathered under this activity to better satisfy the objective of providing a greater insight of the current state of cybersecurity across the EU. Such a move could result in this impact having an even bigger impact, by providing a more holistic set of enabling services to support MS' actions. In this respect, and in line with the aspiration to work more closely with MSs on consolidating information and knowledge, a future direction for this activity, and a measure of the agency's success, factor would be to foster greater cooperation with MS.

Objectives

- Identify and understand emerging and future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase MSs and Union's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities
- Greater insight of the current state of cybersecurity across the Union

Results

- Decisions about cybersecurity are futureproof and take account of trends, developments and knowledge across the ecosystem
- MSs have the tools for assessing and understanding their cybersecurity maturity

Link to strategic objectives (ENISA strategy)

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

Outputs	Outcome
8.1. Develop and maintain EU cybersecurity index	In 2023, ENISA continued its work on the development and maintenance of the EU CSI, which began in 2021. In collaboration with the ENISA NLO subgroup on the index (in which 21 MSs actively participate; all the outputs of the NLO subgroup are also shared with the entire ENISA NLO Network) and under the strategic guidance of the ENISA management board (which held dedicated held in March 2023), ENISA revised the index framework, statistical model and methodology, redesigned the indicators based on stakeholders' feedback and introduced a weighting scheme for the indicators and the different areas and subareas of the index to reflect their importance in the overall calculation algorithm (weights were defined based on specific criteria and based on the input of the MSs were assigned specific values). Moreover, ENISA continued with the maintenance and further development of the index platform, a collaboration platform for the collection, management and analysis of the data for different MSs, allowing MSs to review and analyse their own data, and allowing ENISA to process the results concerning the EU CSI. To test the feasibility of the index framework and the platform, in anticipation of the operationalisation of the index in 2024, ENISA successfully conducted a second pilot exercise (the first one was conducted in 2022), in which all 27 MSs actively took part. The results were processed and validated by the NLO subgroup on the index and lessons were learned on the use of the platform, the validation of the data and the presentation of the results. Each country received a revised report comparing its performance with the EU average, as well as the EU average report. The lessons learned from the second pilot exercise and the additional feedback received by NLOs feed directly into the 2024 SPD, which sees the EU CSI becoming operational. The added value provided by the EU CSI is an assessment of the level of cybersecurity across the EU and the MSs, and as a result the ability to identify progress made in various directions. As stated in the agency's 2022 annual activity report and the 2023 SPD, the index may in certain cases be helpful in assessing the success of ENISA's attempts to raise the level of cybersecurity across the EU and, to this end, the KPIs for ENISA activities included in 2023 SPD already take into account the results of the EU CSI. In line with Article 18 of NIS 2 on the state of cybersecurity in the EU, in 2023 ENISA worked to map the relevant indicators to the provisions of Article 18(1) and (3) and validated the methodology with the designated stakeholder communities, namely the Commission, the NIS Cooperation Group and the CSIRTs Network (April 2023), with all feedback received addressed and incorporated in the second pilot exercise, which ran from July to October 2023. Serving as, among other things, a consolidated information and knowledge management framework for EU cybersecurity, output 8.1 directly contributes to strategic objective 7 and all the relevant objectives defined under activity 8. When it comes to resource utilisation, as the EU CSI matures and its uptake on defining policy recommendations (as per Article 18 of NIS 2) is expected, ENISA will focus its efforts on better interpreting the results, as well as identifying use cases for the effective utilisation of the results of the index by the MSs and the EU. Accordingly, extensive discussions with MSs and the Commission are expected in 2024 with the aim of streamlining this work as it moves from the pilot phase to the production phase. Given the scope of the work and the link with the NID 2 Article 18 report, which will make policy recommendations based on the assessment of the state of cybersecurity in the EU, further alignment of this work with activity 1 and policy development should be considered.
8.2. Collect and analyse information to report on the cyber threat landscapes	Throughout 2023, ENISA continued to collect and analyse information to enable it to report on the cyber threat landscape. The latest annual report, *ENISA Threat Landscape 2023*, was published in October 2023. Dedicated threat landscapes on transport (February 2023), healthcare (June 2023) and denial of service (December 2023) were also created. This approach of providing dedicated sectorial and thematic threat landscapes to complement the horizontal picture of the ENISA threat landscape has been welcomed by the cybersecurity communities and in particular complements ENISA's work to support and empower the NIS sectorial communities. ENISA also continued its collaboration with the EEAS on mapping the threat landscape of foreign information manipulation and interference (work included as a dedicated chapter in the *ENISA Threat Landscape 2023*), while additionally conducting a deep-dive analysis of vulnerabilities in 2023 and their impact on the threat landscape (also included in the *ENISA Threat Landscape 2023*). The importance of the CTI community and of information and analysis sharing for the effective mapping of the threat landscape led to a series of community engagements. A dedicated conference on CTI was held in September 2023, with around 120 participants. ENISA is supported in its work in this area by a dedicated AHWG on cyber threat landscapes. Together with the NLO Network, this AHWG validates relevant outputs. The output is well defined and directly serves ENISA's statutory task of carrying out long-term strategic analyses of cyber threats and incidents (Article 9(2) of the CSA) and fulfils ENISA's strategic objective 7 on efficient and effective cybersecurity information and knowledge management for Europe. This is evidenced by internal coordination activities and synergies identified with the work on situational awareness (activity 5) as well as incident reporting (output 8.3). Accordingly, ENISA has continued to work towards the development of an integrated approach and platform for managing information and knowledge on threats and incidents with the aim of delivering information threat landscapes in a timely, accessible and service-oriented manner. The work is expected to be completed in 2024, aligning all aforementioned ENISA work and optimising resources in addition to establishing agency-wide common methodologies for situational information processes. The widespread uptake and dissemination of the work produced in this output (as evidenced by the media monitoring findings, KPIs and numerous engagements in international conferences and fora) is undeniable evidence of the added value of the output in ensuring that information and knowledge is shared and expanded within the EU cybersecurity ecosystem. There is widespread recognition of ENISA's threat landscapes, and they have been well received by the cybersecurity community. Currently, ENISA's KPIs mostly reflect the outreach of the work carried out under output 8.2. However, in 2023 significant effort went into revising the KPIs to put emphasis on assessing the performance of the output, and particularly its uptake, considering also metrics from the EU CSI. Given the strong links between output 8.2 and the agency's work on incident reporting (output 8.3) and situational awareness (activity 5), consideration should be given to consolidating these three streams of work to better reflect and strengthen the already existing links, and also to optimise resource utilisation.

8.3. Analyse and report on incidents as required by Article 5(6) of the CSA as well as other sectorial legislation (e.g. DORA, Article 10 of the eIDAS regulation)	In 2023, ENISA fulfilled the statutory tasks under Article 5(6) of the CSA by delivering annual summary analyses of incident reporting and reports concerning the eIDAS regulation (Article 19) and the European Electronic Communications Code (Article 40). Moreover, ENISA supported the NIS Cooperation Group, and in particular the workstream on incident reporting, by analysing and reporting incidents reported under Article 10(3) of the NIS2. To this end, in 2023 ENISA assumed the role of secretariat for the aforementioned workstream. In addition, 2023 saw the inclusion of one additional incident-reporting stream in ENISA's line of work, namely that of eIDAS Article 10, at the request of the eID Cooperation Network. Relevant onboarding activities for the new entities and development of a targeted SOP were delivered. ENISA also continued its efforts to integrate and consolidate the information collected and analysed under incident reporting with that of threat landscapes in order to provide a comprehensive overview of the state of cybersecurity, by cross-correlating relevant trends and patterns. Accordingly, ENISA provides MS with an online incident-reporting and analysis system to facilitate the summary reporting process under Article 5(6) of the CSA, thus allowing rapid processing and extraction of trends and patterns across several dimensions (e.g. root cause, affected assets, impact on availability). During 2023, the platform was redesigned to address the needs of NIS 2 by rehauling the online system to cater for changes in incident-reporting requirements and the inclusion of additional sectorial entities. In 2023, ENISA made a series of contributions to policy implementation, and in particular to NIS 2 and DORA. As secretariat of the NIS Cooperation Group workstream on incident reporting, ENISA supported the Commission and MSs in providing input to the implementing act envisaged under Article 23(11) of NIS 2 and, more generally, the definition of criteria for notification of significant incidents. In addition, ENISA began the preparation of technical guidelines for Article 23(9) of the NIS 2, which are to be reviewed and finalised by the workstream during 2024. In the case of DORA, ENISA was actively engaged in all discussions for the preparation of the incident-reporting regulatory technical standards and supported the European supervisory authorities by providing subject matter expertise and year-long experience in the realm of incident reporting. Furthermore, in the context of the EU–US dialogue, ENISA, together with the Commission, worked with their US counterparts to map the different incident reporting frameworks in an effort to promote better understanding. ENISA's work on incident reporting not only is a statutory task but, more importantly, is integral to efficient and effective information management in Europe. Reporting incidents and the subsequent analysis by ENISA allow those involved to share lessons learned, identify emerging trends and extract multiannual patterns, with the aim of being better prepared in the future. Accordingly, the output is integral to ENISA's work and strategic priorities, and to the successful implementation of NIS 2. NIS 2 envisages the consolidation of all three incident-reporting streams (NIS 2, eIDAS and the European Electronic Communications Code), more frequent reporting of incidents to ENISA (every trimester instead of annually) and an increased number of applicable sectors. Supporting the incident reporting required by DORA, by means of consultations with the European supervisory authorities and technical expertise, will undoubtedly increase in the course of 2024, as will the needs of NIS 2, since the deadline for national transposition is set for October 2024. Accordingly, it is expected that output 8.3 will require additional resources, including an expansion of the capacity of current IT systems. This work is included in the 2024 SPD and has already commenced; however, it is expected to increase in the course of 2024 because of the inclusion of additional incident- reporting streams in upcoming regulations such as the CRA. Continuing the work of 2023 on improving the KPIs for the uptake of relevant ENISA recommendations, in 2024 more refined and targeted KPIs have already been introduced, and ENISA will assess their effectiveness. It should be noted that the output was delivered with the same number of FTEs as in 2022, despite the increasing workload for ENISA staff introduced by the numerous activities mentioned above (e.g. DORA support, transition to NIS 2 while maintaining the NIS 1 regime, providing the secretariat for the workstream on incident reporting and creating preparatory documents). Given that the additional tasks will move to operational support as of 2024, the need for additional resources to deliver this output is evident. Aligning with output 8.2 on threat landscapes, as well as the work of activity 5 on situational awareness, promotes better internal knowledge management at ENISA, a dimension that was explored further in 2023.
8.4. Develop and maintain a portal (information hub) and identify appropriate tools that will act as a one-stop shop to organise and make available to the public information on cybersecurity, and establish a procedural framework to support knowledge management activities, maximising synergies with the European Cybersecurity Atlas	In 2023, ENISA continued its multiannual work on delivery of the information hub (infohub) by developing the framework defined in the initial phase of the project. The agency consolidated and addressed the feedback received from stakeholders (namely the NLO Network) during the first iteration of the infohub in 2022, and proceeded with the development of the second iteration, which was completed at the end of 2023. In addition, ENISA developed a concrete and detailed benchmarking approach for the infohub, to enable it to assess its impact, usefulness and usability. The process was supported with guidance from a testing group comprising experts nominated by NLOs from 11 MSs. Based on management board strategic guidance, it was decided that output 8.4 should be deprioritised and should not be continued in 2024. Relevant resources will be redirected towards other activities in the 2024 SPD, namely capacity building. Given this structural change, the infohub did not become operational with extended (i.e. public) access at the end of 2023 as planned, and hence the relevant KPI, KPI 8.1, cannot be assessed. Building on the outcomes of this work, and to foster cross-fertilisation and synergies, as well as optimise resource utilisation, the work conducted during 2021–2023 will be utilised to enable other ongoing or upcoming projects within ENISA to benefit from possible transfer of knowledge and insights (e.g. the ENISA website and awareness-raising activities).
8.5. Foresight on emerging and future cybersecurity challenges and recommendations	In 2023, ENISA worked, in line with Article 9 1 of the CSA, to deliver foresight on emerging and future cybersecurity challenges and to make recommendations on how to address the challenges identified. With regards to foresight, with the participation of the ENISA advisory group, the ENISA AHWG on foresight and members of operational communities such as the CSIRTs Network and EU-Cyclone, the agency conducted three cybersecurity foresight exercises. The first involved an update of scenarios for cybersecurity threats in 2030, the second the development of scenarios for large-scale incident and crisis escalation and the third focused on the future of operational cooperation tools in the EU. These works, and in particular the first, identified topic-specific trends and assessed 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 was published in March 2023. Moreover, in September 2023, the flagship conference Threathunt 2030 took place, 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 6 on foresight regarding emerging and future cybersecurity challenges.

	Building on the results of foresight work carried out in 2022, in 2023 ENISA carried out targeted analyses on three identified challenges and made recommendations to address these. Two dedicated reports on Artificial Intelligence (AI)use cases, one for energy and one for medical imaging, were published, as was a mapping of the threat landscape for space using the ENISA threat landscape methodology (the report on space threat landscape is expected to be published in 2024 subject to validation by relevant stakeholders). Moreover, a study on ongoing work on the standardisation of elliptic curve cryptography, focusing on implementation guidance, was conducted, and the results are expected to be published in 2024. The work on AI cybersecurity was completed with the support of the ENISA AHWG on AI. Given the significance and prevalence of the challenges related to AI and cybersecurity, a dedicated conference was held in Brussels in June 2023 to bring together the community and exchange insights on the way forward.				
8.6. Building and exchanging knowledge on ransomware threats (including through capacity building, awareness raising and education)	In accordance with the 2023 SPD, output 8.6 did not form part of the 2023 work programme owing to insufficient resources.				

Key performance indicator	**Unit (of measurement)**	**Frequency**	**Data source**	**2022 results**	**2023 result/ target**
ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including into research and innovation agenda					
8.1. Number of users and frequency of use of a dedicated portal (observatory) (33)					
8.2. Total number of recommendations, analyses and challenges identified and analysed	Number	Annual	ENISA reports and studies	357	389 Target 300
8.3. The influence of foresight on the development of ENISA's work programme	Number	Annual	SPD	NA	3 (AI, supply chain, space infrastructure)
8.4. Uptake of reports generated in activity 8	Number	Annual	Media monitoring report	NA	102 media mentions 74 761 downloads
8.5. Uptake of the cybersecurity index	Number	Annual	Index platform	NA	24/27 MSs actively using the index platform
8.6. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research	%	Biennial	Survey	91.5 %	NA
% of stakeholders rating the outcome/ results of ENISA's work as providing high or some added value	%	Biennial	Survey	94 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	90 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	86 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	94 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	94 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	91 %	NA

Allocated FTEs as per SPD, based on full establishment at 2023 year end	8.5	**Number of FTEs actually used**	6.84
Planned budget (EUR) (34)	811 881	**Budget consumed (EUR) (35)**	781 364.76
		Of which carried forward to 2024 (EUR)	92 897.51

NA, not applicable.

(33) The infohub has yet to be implemented.

(34) Direct costs only.
(35) Direct costs onl

ACTIVITY 9: Outreach and education

Activity 9 endeavours to deliver against the strategic objective of creating engaged and empowered communities and cutting-edge competences across the EU. It does this by implementing projects around raising awareness and promoting 'good' cybersecurity behaviour, with the goal of eventually creating a cultural shift. The tasks carried out under this activity include awareness-raising activities, the creation of tailor-made promotional material and the use of innovative methods for staff education to achieve a mindset shift. At the same time, increasing the number of professionals to meet demand is regarded as one of the key priorities under this activity. A wide spectrum of projects are covered by this activity, from promoting cybersecurity in education (primary, secondary and higher levels of education) to the development of the ECSF to support the specialisation, upskilling or reskilling of professionals in cybersecurity.

One of the main achievements of activity 9 carried out in 2023 was the development the ECSF, which has become the reference framework for the Cyber Skills Academy and European policy proposals. It has been recognised for its role in bridging the cybersecurity talent gap and improving EU competitiveness, growth and resilience. Surveys have revealed a level of high awareness of the ECSF among professionals (over 60 %), with an even higher proportion (over 80 %) considering it relevant to their profession. In addition, the Cybersecurity Higher Education Database (Cyberhead) is now the largest hub for students seeking cybersecurity university programmes, listing 146 programmes by the end of 2023. It provides valuable insights into trends for graduates and gender balance, as well as mapping to the ECSF, thus facilitating informed learning choices and career planning for students, bridging the gap between education and professional requirements. Cyberhead feeds into the EU CSI. Finally, in relation to implementation of the international strategy, ENISA concluded working arrangements (with the United States and Ukraine) and a similar process with the NATO Communications and Information Agency is at an advanced stage. ENISA's work to develop international cooperation is finally bearing fruit in the form of valuable collaboration and exchange of knowledge and information.

In 2023, ENISA was charged with some additional tasks stemming from the Cybersecurity Skills Academy Communication. These had to be actioned immediately, necessitating the reallocation of resources (human and financial).

When it comes to lessons learned it is essential to consider the impact of actions undertaken under the activity and how to refocus them in order to shape the activity and achieve greater impact going forward. As an example, ENISA has deprioritised the organisation of European cybersecurity month (ECSM) from 2024. In addition, in 2023, the Commission lowered the priority of the ECSM. As MSs have indicated that they have the capacity to run individual national campaigns, this is not expected to impact awareness raising across the EU. From now on, ENISA will focus on maintaining the cybersecurity national coordinator group and will expect the ECCC and the NCCs to play a more decisive role in in the future.

In terms of specific awareness-raising topics, namely support for SMEs, the impact that ENISA can achieve is minimal, for a number of reasons, one being the prohibitive cost of translating promotional materials into other languages. For this reason, ENISA proposes to discontinue output 9.2, related to topical awareness-raising actions. ECCC and NCCs are better placed to adapt their awareness-raising activities to the SME community. However, ENISA will be able to support, offer advice to and collaborate with the NCCs in this endeavour.

Finally, the outputs of activity 9 are closely interlinked with the capacity-building outputs of activity 3 and complement each other, forming a circle in terms of skills and developing capacity. For this reason it is proposed that, from 2025 onwards, these activities be merged in order to achieve greater synergy and efficiency by taking into account skills development and developing all the other outputs such as educational activities, exercises and training by making use of the ECSF. Finally, the activities around awareness could become part of the services list in the ENISA cybersecurity support action, namely the concept of augmented reality (AR)-in-a-box, which is currently attracting a great deal of attention and demand from stakeholders.

The current indicators measure the promotion and uptake of awareness-raising materials and messages; however, they cannot measure cultural change or secure behaviour online. That said, quantitative data (e.g. requests for AR-in-a-box sessions, ECSF adoption and endorsement rates, policy development with regards to skills, etc.) do showcase the success of ENISA and its role in cybersecurity awareness and workforce development. The indicators will be reviewed in the light of the proposed merging of activities 3 and 9 from 2025 onwards.

Objectives

- Advance cyber secure behaviour by essential service providers in critical sectors
- Elevate the understanding of cybersecurity risks and practices across the EU and globally
- Foster EU cybersecurity values and priorities
- Increase the supply of skilled professionals to meet market demand, and promote cybersecurity education

Results

- Greater understanding of cybersecurity risks and practices
- Stronger European cybersecurity through higher global resilience

Link to strategic objectives (ENISA strategy)

- Empowered and engaged communities across the cybersecurity ecosystem

Outputs

9.1. Develop activities to enhance behavioural change by essential service providers in critical sectors (as defined by the NIS Directive)

Outcome

ENISA conducted targeted cybersecurity awareness campaigns aimed at bolstering awareness of emerging cybersecurity threats within critical sectors, including healthcare, energy (electricity and gas) and the railway industry. These initiatives were designed to equip stakeholders with the knowledge and skills necessary to mitigate cybersecurity risks effectively.

The healthcare campaign, held from 15 to 19 May 2023, emphasised phishing, ransomware and cyber hygiene, utilising materials from the previous year. Similarly, the cybersecurity awareness campaign for distribution system operators, known as Cyber Energy Week, took place from 18 to 22 September 2023. It featured updated content, including a video addressing ransomware attack phases and corresponding mitigation strategies. The campaign targeting gas operators, titled #FuelforCyber, focused on social engineering, phishing, and ransomware, and took place from 16 to 20 October 2023.

ENISA also developed a campaign for the railway sector, #CyberOnTrack, highlighting the intersection of physical security and cybersecurity, alongside phishing, vishing and cyber hygiene, which ran from 6 to 10 November 2023.

Furthermore, ENISA enhanced its AR-in-a-box package by updating the Cyber Crisis Communication Guide. Moreover, the organisation conducted over 20 physical and online/hybrid 'train-the-trainer sessions' to present guidelines for developing awareness-raising programmes, responding to stakeholder requests. These sessions aimed to empower organisations and private companies to cultivate cybersecurity cultures efficiently and affordably.

Overall, the constantly increasing number of requests to ENISA indicates that the community requires more support.

9.2. Promote cybersecurity topics, education and good practices in the basis of the ENISA stakeholders' strategy	ENISA actively raised awareness among SMEs by promoting its work on maturity assessments, guidelines and the AR-in-a-box initiative. This work included engagement with the current SME working group to validate information and disseminate ENISA's work effectively. Furthermore, ENISA developed a comprehensive SME strategy with long-term objectives, considering the evolving regulatory and threat landscapes. The organisation expanded its outreach to stakeholder communities through participation in various conferences, workshops and similar events. ENISA also took steps to challenge stereotypes surrounding cybersecurity professionals by creating promotional material based on the profile of certain roles related to the ECSF. The organisation actively supported and promoted the CyberALL campaign through various activities and events. ENISA also organised a CTF event aimed at empowering young people and adult women interested in pursuing careers in cybersecurity. These events featured training sessions, CTF challenges and world café discussions on inclusivity issues within the cybersecurity field. Furthermore, ENISA participated in a panel discussion at Security Bsides Athens, engaging with over 200 international participants to foster discussions and inspire action on inclusivity in cybersecurity. Finally, the organisation developed a video series, complemented by guidance leaflets, to support the release of the EU cybersecurity certification framework implementing act, providing valuable support and guidance to stakeholders.
9.3. Implement ENISA's international strategy and outreach	ENISA pursued international activities under three approaches (limited/assisting/outreach) as defined by ENISA's international strategy, which was approved in November 2021. Under this output, ENISA achieved the following in 2023. • It concluded working arrangements with the United States and Ukraine. A similar arrangement with the NATO Communications and Information Agency is at an advanced stage. • Coordinated the agency activities within the context of the EU–US dialogue workstreams, in cooperation with the units and teams involved. • Agency staff participated in three cyber dialogues (EU–US, EU–UK EU– Japan), the EU–NATO High-Level Staff Talks on Cyber Security and Defence and the Western Balkan Digital Summit. • It established a regional strategy to scale international cooperation services for the Western Balkans. • It nurtured relationships with key EU stakeholders such as the EEAS, DG Connect and the Directorate-General for Neighbourhood and Enlargement Negotiations. 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. • Specifically, the ENISA International Cooperation handled 141 requests: 11 for outreach engagements, 20 for assisting engagements and 110 for limited engagements. • Of 110 limited engagements which have been approved, 37 were undertaken in the context and support of an outreach activity, showing that the agency is prioritising high-value engagements. • The agency experienced significant growth in requests for assisting engagements (which accounted for 14.2 % of all requests, compared with 2.9 % in 2022). This can be attributed primarily to ENISA's support for Western Balkan and EU–US dialogue. Outreach engagement requests also increased (accounting for 7.8 % of the total, compared with 4.9 % in 2022), driven primarily by the cyber partnership programme. The proportion of limited engagement requests decreased accordingly (to 78 % of the total, down from 92.2 % in 2022), although the total number of engagement requests increased to 141 (up from 102 in 2022). • A total of 26 requests (18.4 % of all requests) were declined, compared with only eight (7.8 % of all requests) in 2022. Most requests were declined because they were not in alignment with the priorities set in the strategy, showing the agency's commitment to adherence to its international strategy.
9.4. Organise the ECSM and related activities	In addition to the October campaign, mini-campaigns were introduced for the first time, running monthly and centred on international observance days (e.g. World Password Day). These mini-campaigns received widespread acclaim and were endorsed by all MSs as well as the European Commission. All materials disseminated throughout the year were provided in various editable formats, enabling MSs to customise them according to their needs. This approach significantly expanded the reach of the campaigns and was highly appreciated by MSs, which received and utilised ECSM materials on a monthly basis. An original song was produced to promote the ECSM, and was widely used by MSs, with one country even incorporating it into a youth dance contest and producing an accompanying video. The song also featured in the ECSM launch event at the European Parliament. For the second consecutive year, there was enthusiastic participation in the ECSM awards, and a video of the online awards ceremony was broadcast during the ECSM launch event in Brussels. MSs showed a keen interest in the competition. Quantitative data show that the popularity of the ECSM on social media declined in 2023. This can be attributed to the absence of paid advertising campaign (as a result of budget constraints).

9.5. Report on cybersecurity skills needs and gaps and support skills development, maintenance and implementation (including producing a digital education action plan and a report on higher education programmes)

ENISA formed a new AHWG to assist in the governance, implementation and future evolution of the European Cybersecurity Skills Framework (ECSF). The group has been instrumental in the promotion of the ECSF across a wider community and in its further evolution.

ENISA designed a new communication strategy and branding to promote the ECSF. As part of this strategy, three webinars under the #ECSFtalks tagline were organised during the year, attracting over 5 000 viewers. These webinars aimed to raise awareness of the ECSF and its significance in addressing the cybersecurity skills gap.

Under the Spanish Presidency of the Council, ENISA organised the second annual conference of the Cyber Skills Academy in Segovia, Spain. The conference brought together more than 120 participants for a 2-day event focused on sharing progress and discussing the impact and prospects of the ECSF. During this event the discussions centred on the ECSF adoption rate and the new communication processes of the Cybersecurity Skills Academy.

In April 2023, the Cybersecurity Skills Academy communication (36) assigned new tasks to the agency. As no additional resources were available, ENISA, to deliver these new tasks, reassessed the priorities of the output. Among the numerous activities implemented by ENISA in response to the communication, the agency spearheaded the institutionalisation of the ECSF, and in September 2023 it launched its review to ensure the framework's ongoing relevance and effectiveness. ENISA also led efforts to define cybersecurity indicators, validated by the European Commission, Cooperation Group working group 9 and NCC working group 5, on skills (37), providing insights into the demand and supply dynamics of cybersecurity skills.

Furthermore, ENISA developed a concept paper giving an overview of MS current status as regards the creation of repositories of training programmes and certifications from the public and private sectors with the aim of providing a single point of access to the resources available for professional skills development. This initiative, shared with the National Competence Centres (NCCs) working group 5 for validation, seeks to facilitate access to pertinent training materials. Finally, ENISA conducted a feasibility study, through a concept paper, to assess the viability of a European-level attestation scheme for cybersecurity skills. This involved surveys and interviews with national representatives of MSs to enable ENISA to understand different governance, assessment and validity approaches to cybersecurity skills assessment. The study concluded that three different viable options are available and that MSs should choose the most appropriate for their needs.

In parallel with these activities, ENISA invested heavily in community building, disseminating information and educating relevant actors on the ECSF, to ensure its adoption and/or endorsement. For example, building strong links between ECSF profiles and the higher education institutions programmes, with training and certification organisations, with operators of critical entities and numerous EU bodies, all of them contributing implementing and utilising the ECSF.

(36) Communication on the Cybersecurity Skills Academy –Shaping Europe's digital future.

(37) NCC working group 5, on skills, was created by the NCC network to deal with numerous tasks relating to the Cybersecurity Skills Academy to be led by the NCCs and the ECCC.

9.6. Implement the cybersecurity in education roadmap (38)

In 2023, ENISA conducted a comprehensive study to evaluate the maturity level of cybersecurity in primary and secondary education systems across MSs, collecting pertinent data from 15 of them . The findings enabled ENISA to create a model and assessment framework for MSs and to provide useful recommendations to MSs.

ENISA also embarked on a strategic endeavour by initiating the development of a web platform intended to centralise all cybersecurity education initiatives in the EU, providing stakeholders with easy access to valuable resources and fostering collaboration in this critical area.

ENISA remains committed to fostering collaboration with key stakeholders, including the European Commission, the European Cyber Security Organisation (through the YouthforCyber initiative), national cybersecurity coordinators and MSs. To this end, in 2023, the agency actively participated the Cybercitizen Initiative's annual meeting with Aalto University, Finland, and the Bucharest Annual Conference, at which it contributed to panel discussions on cybersecurity education. Furthermore, it presented its ongoing activities at pivotal meetings, ensuring transparency and alignment with the objectives of the agency's partners.

Key performance indicators Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU	**Unit (of measure ment)**	**Frequency**	**Data source**	**2022 results**	**2023 results/ target**
Level of outreach					
9.1. Number of cybersecurity incidents reported having human error as a root cause	Number	Annual	ENISA tool	153	147/NA
9.2. Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics					
Total social media impressions	Number	Annual	ENISA analytics	27 278 491	946 100/ 20 000 000
Total social media engagement	Number	Annual	ENISA analytics	19 301	57 000/ 150 000
Total video views	Number	Annual	ENISA analytics	6 602 355	0/3 000 000
Total website visits	Number	Annual	ENISA analytics	300 530	603 459/150 000
Total participation at events	Number	Annual	ENISA analytics	40	40/10
CyberAll (formerly Women4Cyber campaign)					
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter))	82 900	115 800
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter))	1 286	2 300
Video views	Number	Annual	YouTube	2 285	NA

(38) Roadmap developed by ENISA during the course of 2022.

Cybersecurity for SMEs campaign					
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter)	35 900	63 900
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter))	1 200	1 800
Video views	Number	Annual	YouTube	6 113	NA
Website	Number	Annual	ENISA website	55 082	115 313 page views
References	Number	Annual	Media monitoring	NA	214
Participation in events	Number	Annual	Website announcements	6	10
Campaign on health					
Social media impressions	Number	Annual	ENISA analytics	58 200	96 900
Social media engagement	Number	Annual	ENISA analytics	1 100	1 800
Video views	Number	Annual	ENISA analytics	197	NA
Website	Number	Annual	ENISA analytics	1 008	51 104 page views
Campaign on gas					
Social media impressions	Number	Annual	ENISA analytics	NA	80 800
Social media engagement	Number	Annual	ENISA analytics	NA	1 100
Video views	Number	Annual	ENISA analytics	NA	NA
Website	Number	Annual	ENISA analytics	NA	5 031 page views
Campaign on energy					
Social media impressions	Number	Annual	ENISA analytics	56 900	53 300
Social media engagement	Number	Annual	ENISA analytics	703	1 800
Video views	Number	Annual	ENISA analytics	224	NA
Website	Number	Annual	ENISA analytics	586	51 307 page views
Campaign on rail					
Social media impressions	Number	Annual	ENISA analytics	NA	128 400
Social media engagement	Number	Annual	ENISA analytics	NA	2 200
Video views	Number	annual	ENISA analytics	NA	NA
Website	Number	annual	ENISA analytics	NA	4 755 page views
ECSM campaign					
Social media impressions	Number	Annual	ENISA analytics	26 823 591	202 600
Social media engagement	Number	Annual	ENISA analytics	9 000	34 300
Video views	Number	Annual	ENISA analytics	6 589 457	NA
Website	Number	Annual	ENISA analytics	179 571	132 368 page views
Certification campaign					
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter))	200 000	204 400
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter))	5 900	11 700
Video views	Number	Annual	YouTube	45 00	NA
Website	Number	Annual	ENISA website	N A	148.435 page views
AR-in-a-box metrics					
Downloads	Number	Annual	ENISA analytics	31 000	43 245/> 30 000
Requests for collaborations	Number	Annual	ENISA analytics	20	20/20
'Train-the-trainer' sessions	Number	Annual	ENISA analytics	15	20/15
Presentations in events	Number	Annual	ENISA analytics	15	20/20
Cyberhead metrics					
Social media impressions	Number	Annual	social media	21 000	NA
Social media engagement	Number	Annual	social media	112	NA
Website	Number	Annual	ENISA website	64 283	95 146 page views
9.3. Number of cybersecurity programmes (courses) and participation rates					
Total number of students enrolled in the first year of the academic programmes	Number	Annual	Report (39)	6 000	6 612/6 000
Number of male students	%	Annual	Report	70 %	80 %/70 %
Number of female students	%	Annual	Report	30 %	20 %/30 %
Total number of cybersecurity programmes	Number	Annual	Report (CyberHead)	130	141/130
Number of graduate programmes	%	Annual	Report (CyberHead)	5 %	6 %/5 %
Number of master's programmes	%	Annual	Report (CyberHead)	80 %	76 %/80 %
9.4. Geographical and community coverage of outreach in the EU	Number	Annual	ENISA analytics	All 27 MSs and EFTA countries	All 27 MSs and EFTA countries

(39) https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education.

9.5. Level of awareness of cybersecurity across the EU / general public (e.g. EU Barometer and other) (40)		Biennial		NA	NA
9.6. Stakeholder satisfaction with awareness-raising and education activities	%	Biennial	Survey	91 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	100 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	80 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	84 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	95 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	86 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	98 %	NA
Allocated FTEs as per SPD, based on full establishment at 2023 year end	7.5	**Number of FTEs actually used**			7.93
Planned budget (EUR) (41)	489 209	**Budget consumed (EUR) (42)**			479 257
		Of which carried forward to 2024 (EUR)			54 719.61

NA, not applicable.

40) KPI proposed to be updated to reflect the requirements of NIS 2 Article 18(1) in the draft 2024–2026 SPD

(41) Direct costs only.

(42) Direct costs only.

ACTIVITY 10: Advice on research and innovation needs and priorities

Through 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. Firstly, the agency takes account of past and ongoing research, activities in development and technology assessment. Secondly, 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 contribute to the EU's strategic R & I agenda, by means of the alignment and collaboration with the ECCC and the network of NCCs, as well as with the R & I community via targeted round tables.

In line with the strategic objective on foresight regarding emerging and future cybersecurity challenges (strategic objective 6), this activity requires regular consultation with the ECCC, NCCs, NLOs, relevant user groups, projects (including EU-funded projects), researchers, universities, institutes, industries, start-ups and digital innovation hubs. The aim of such consultation is to consolidate information and identify gaps, challenges and opportunities in R & I from the different parts of the cybersecurity community. In this way, the agency delivers on its mandate as per Article 11 of the CSA.

One of the main achievements of activity 10 is ENISA's advice to the European Cybersecurity Competence Centre (ECCC) and the National Competence Centres (NCCs) and its contributions to the ECCC's 2025–2026 strategic action plan, which followed the adoption, in March 2023, of the ECCC strategic agenda. The latter reflects ENISA's input, placing emphasis on cross-fertilisation between the activities of ENISA and the ECCC. While it remains a challenge to ensure operational alignment, ENISA and ECCC have agreed an MoU to better coordinate their actions, and in 2024 and beyond ENISA will continue to pursue closer cooperation with the NCCs and the ECCC. To this end, a potential concrete contribution would be for ENISA to be more actively engaged in supporting the ECCC with the review and assessment of calls for proposals, in addition to providing input to their content to ensure that they accurately reflect ENISA's knowledge of the EU cybersecurity ecosystem, obtained through its projects and from stakeholder communities. Accordingly, ENISA has been co- chairing two ECCC governing board working groups, one on the strategic action plan and one on cybersecurity skills, emphasising the importance that the agency places on its collaboration with the ECCC.

ENISA set the grounds for a multiannual strategy on R & I by introducing the dedicated and focused activity 10 in its annual work programme. The three outputs under this activity were designed to work coherently with one another. Output 10.1 defines the biennial R & I roadmap by taking stock of existing strategies, technological roadmaps, ENISA activities and R & I activities in the EU. The topics and themes identified in the R & I roadmap serve as input to outputs 10.2 and 10.3.

In the future, this action will be undertaken by not only including NCCs and the ECCC in relevant discussions, but also collecting and analysing information and knowledge from the entire cybersecurity ecosystem and ENISA activities (threat landscapes, situational awareness, sectorial assessments, etc.). Consideration will be given to revising the approach taken by ENISA. The aim would be to empower and enable communities at the national level to identify their research and priorities needs for cybersecurity, with ENISA acting a trusted facilitator, consolidating and analysing relevant findings and produce concise, targeted and focused EU-wide recommendations.

An additional lesson learned involves the use of strategic foresight, one of ENISA's core strategic objectives, as a means to fulfil the agency's mandate and mission when it comes to R & I. It should be highlighted that, although the agency carried out a dedicated foresight exercise on research and innovation in 2023, foresight remains a horizontal objective for the entire agency, cutting across all of its activities. In the future, strategic foresight should take a broader view, with consequent steps to contextualise the results to the particular field.

Activity 10 met its objectives for 2023, despite limited resources and a vast R & I ecosystem whose needs had to be prioritised. If ENISA is to continue to meet its objectives and fulfil its mission, a different approach should be considered. In particular, ENISA should consider acting as an enabler of relevant communities at the national level, notably the NCCs, and empower them to identify their needs and priorities.

An important part of activity 10 involves measuring the uptake of ENISA's advice and in general taking stock of, and assessing, EU's R & I ecosystem. This would provide valuable insight of ongoing activities at the national and EU levels and could greatly contribute to ascertaining whether any gaps, threats, opportunities and challenges vis-à-vis R & I exist.

Objectives

- Advance the response to current and emerging cyber risks and threats with the use of effective risk prevention technologies.
- Ensure that the EU strategic research and innovation agenda in cybersecurity is aligned with the needs and priorities of the community.
- Reduce dependence on cybersecurity products and services from outside the Union and to reinforce supply chains within the Union

Results

- Research and development of cybersecurity technology reflecting the needs and priorities of the Union.
- Funding the development of cybersecurity technologies that meet the Union's ambition to become more resilient, autonomous and competitive.

Link to strategic objectives (ENISA strategy)

- Foresight on emerging and future cybersecurity challenges

Outputs

10.1. Consolidated cybersecurity research and innovation roadmap across the EU

Outcome

Output 10.1 focused on the consolidation of ENISA's R & I work, as well as the results of all other operational activities, to develop an R & I roadmap across the EU. In doing so, ENISA collected existing mature cybersecurity R & I agendas, including those from the four pilot projects, to which more than 100 research groups and academics had contributed. The next step involved the analysis of the aforementioned agendas in conjunction with emerging technologies' R & I agendas, such as roadmaps produced by major industrial associations, following which targeted bilateral discussions were held with innovation stakeholders from the cybersecurity industry. The consolidation of all relevant input was conducted by ENISA on the basis of the Joint Research Centre (JRC) cybersecurity taxonomy, which led to the mapping of priority areas across a series of research domains. The report on the ENISA's R & I roadmap will serve as an internal ENISA reference document to support discussions with the ECCC, NCCs and other stakeholders vis-à-vis R & I priorities.

Overall, more than 60 research domains and themes were identified and included in the R & I roadmap, and the scope and the findings of the work conducted under output 10.1 were validated by experts, members of the R & I community, the JRC, the NCCs, the European Commission, members of the ENISA advisory group and those involved in the four pilot projects.

The inherently long-term nature of this work does not justify frequent updates. Accordingly, a biennial review of the R & I roadmap is envisaged. This is in line with the strategic guidance of the ENISA management board, which has led to this output being deprioritised in the 2024–2026 SPD. As a result, it is envisaged that this work will not be continued in 2024, and resources will be reallocated to higher- priority outputs (outputs 10.2 and 10.3).

10.2. Collect and analyse information on new and emerging information and communications technologies in order to identify gaps, trends, opportunities and threats (R & I observatory)

Output 10.2 aimed to decouple the identification of emerging and future trends in technology R & I from the process of producing relevant, informed, timely and well- supported advice on R & I and deployment needs and priorities. The R & I observatory that was introduced in output 10.2 lays the foundation for ENISA's advice to stakeholders (ECCC, NCCs, the Commission) as per Article 11 of the CSA.

In 2023, ENISA developed the concept of the R & I observatory. Drawing on relevant information and knowledge derived from previous ENISA work (notably output 10.1, the R & I roadmap) and strategic foresight (in particular a foresight exercise dedicated to identifying technologies likely to be disruptive by 2035), specific priority areas were identified and served as input to ECCC and NCC network activities to address pragmatic cybersecurity needs. ENISA conducted a foresight exercise focusing on disruptive technologies with a 10-year horizon to collect and analyse information on new and emerging ICT (information and communication technologies), and identified over 20 trends and new drivers of change likely to have a significant impact in the future. With the support of the relevant validation bodies (the ENISA AHWG on foresight and the ENISA advisory group), these drivers of change were mapped to cybersecurity trends, opportunities and threats and will serve as a baseline for future discussions on R & I priorities.

Building on work carried out in 2022, ENISA also selected three important themes to be the subject of deep-dive analyses, with the aim of determining their implications and identifying gaps, trends, opportunities and threats. The themes chosen were cybersecurity for AI, cyber biosecurity and the interlink between law and cybersecurity and the aim was to pinpoint relevant R & I trends. Accordingly, ENISA organised two round tables (one on cyber biosecurity and one on the law and cybersecurity) with the participation of relevant stakeholders (from academia, EUIBAs, industry and the NCCs). The aim was to answer fundamental questions on what needs to be researched and how to create an environment conducive to cybersecurity innovation. In addition, the ENISA AI Conference in June 2023 included a panel discussion on relevant R & I trends, the results of were subsequently published in a dedicated report. The agency examined existing research, identified gaps and analysed emerging and future trends in technological innovation focusing on cyber insurance in a report that will be published in Q2 2024.

The scope and the findings of the work conducted under output 10.2 were validated by experts, members of the R & I community and industry representatives during round-table discussions.

Although the importance of the work carried out under output 10.2 in helping ENISA to fulfil the relevant activity objectives and its mandate under Article 11 of the CSA cannot be understated, it needs to be noted that the approach is not scalable.

ENISA has limited resources to deliver this work, and considerable time is needed to conduct strategic foresight exercises (approximately 1 year) and engage with the multitude of interested stakeholders. Therefore, a prudent course of action would be for the agency to consider acting as a facilitator in the future, empowering communities at the national level to conduct relevant exercises. This would free up ENISA to identify cybersecurity R & I gaps, trends, opportunities and threats by consolidating and analysing the information collected. Moreover, given their strong ties, the 2025 SPD will explore opportunities to align the work of this output with other ENISA work on research, industry innovation and cybersecurity market.

10.3. Provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment

In 2023, ENISA carried out multiple activities in conjunction with the ECCC and the network of NCCs. To better define and plan these activities, ENISA prepared an MoU. The MoU, which was signed in September 2023, sets out a framework for cooperation and the development of synergies with the ECCC. ENISA also followed up on the SLA that has been set up with the ECCC concerning offering of support on accounting and Data protection officer (DPO) services. ENISA acted as co-chair of ECCC governing board working group 4 on the development of the strategic action plan, following on from the 2023 publication of the ECCC strategic agenda. In doing so, ENISA utilised work carried out under outputs 10.1 (R & I roadmap) and 10.2 (foresight via the R & I observatory).

ENISA continued, as it has done since 2022, to co-chair the ECCC governing board working group on skills and also, as a member of governing board working group 3, contributed to the follow-up and implementation of the community guidelines. The agency also organised several bilateral meetings with the NCCs to discuss the ECCC Single Programming Document (SPD) and agenda, hosted the Network of NCCs Day in ENISA headquarters and held webinars for ECCC staff, to familiarise them with ENISA's work and promote alignment

This is a new output, introduced in response to management board guidance and the 2022 annual activity report, and aims to better align the output with Article 11 of the CSA, which states that ENISA should advise stakeholders, including the ECCC and NCCs, on R & I and deployment needs and priorities. In 2023, considerable effort was expended on this output, and on increasing support for the ECCC and the NCCs, with a particular focus on cross-fertilisation with outputs 10.1 and 10.2. Given the role of ECCC and NCCs in the EU's strategic R & I agenda, it is essential to further strengthen this work, as this, in turn, will lead to greater uptake of ENISA's advice to the EU agenda on cybersecurity research, innovation and deployment.

Key performance indicator ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including into research and innovation agenda	Unit (of measurement)	Frequency	Data source	2022 results	2023 results/ target
10.1. Number of requests from the EU-IBAs (including the ECCC) and MS to contribute, provide advice or participate in activities.	Number	Annual	Report	NA	3
10.2. Number of references to ENISA advice and recommendations in the EU Strategic R & I Agenda including Annual and Multiannual Work programmes.	Number	Annual	Report	NA	1
10.3. Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's advice on cybersecurity research needs and funding priorities	%	Biennial	Survey	NA	NA

Allocated FTEs as per SPD, based on full establishment at 2023 year end	4	**Number of FTEs actually used**	3.34
Planned budget (EUR) (43)	195.371	**Budget consumed (EUR) (44)**	181 603
		Of which carried forward to 2024 (EUR)	96 735.56

NA, not applicable

(43) Direct costs only.
(44) Direct costs only

ACTIVITY 11: Performance and risk management

Activity 11 encompasses the objectives of performance and risk management, with both external and internal dimensions. 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. Internally, single administration, risk and compliance management via updated processes and tools are key focus areas of this activity.

In 2023, ENISA achieved the following in the area of performance and risk management.

- An assessment of the implementation of ENISA's 2020–2024 strategy was initiated, with a view to redefining priorities and setting out a path to a new strategy, extending beyond 2024.
- It surveyed its stakeholders to determine their level of satisfaction with ENISA's work, in particular their perception of the outcome/results of its work and how the work was carried out and their level of trust in ENISA's abilities. There were 163 responses to the survey from across the cybersecurity community, including from statutory bodies.
- It piloted a virtual CISO project to share experience and develop common practices in implementation of the new cybersecurity regulation (Regulation (EU) 2023/2841) with six EU agencies and in close cooperation with Commission services and CERT-EU.
- It developed and applied a thorough enterprise and IT security risk management framework, and subsequently carried out an on-site IT security assessment for a key service provider.
- It launched its new document management system as a cornerstone of the agency's approach to single administration.

These highlights of the year reflect ENISA's culture, which is one focused on performance management through practicable steps, with the goal of protecting the agency's assets and reputation while reducing risks. In particular, the agency, acting on lessons learned, aims to further enhance data collection and analysis of stakeholders' opinions, to enable automation of processes and to ensure continuity and functional-based approaches to single administration. In addition, on the basis of the virtual ISO pilot, the agency will explore the possibility of sharing services with other EU agencies, to achieve synergies, over the next 3 years.

The activity also supported the agency's overall internal controls framework and strengthened its own cybersecurity posture. The agency also responded, through its liaison function, to the increased demand from the co-legislators of the EU for technical advice on the proposals for the CRA and the CSOA, as well as the amendment of the CSA. The annual communications strategy was also part of this activity, and its impact needs to be further assessed based on the lessons learned.

Increased demand for a presence at physical events and the geopolitical context had a direct impact on the activity's budget. Objectives and KPIs were met, and additional activities not planned initially were carried out with the budgetary support of internal transfers. Additional activities, however, resulted in an increased workload for staff.

In addition, the end of the year budget process allowed surplus funds to be channelled to postponed actions, such as a website revamp and stocking up on outreach materials to support ENISA's 20-year anniversary activities in 2024. This explains the higher than usual budget amounts carried forward to 2024.

Moreover, this activity supported the cybersecurity support action under activity 5 by providing visual materials, translation coordination and legal advice amounting to 0.5 FTEs in total.

In the coming years, taking into consideration the diversity of topics to be addressed, the need for technical support and resource constraints, external contractors and services will used to achieve some of the goals of the activity.

Activity 11 met its objectives for 2023. The KPIs show that the expected compliance levels were met. The adoption of the corporate strategy necessitated internal adjustment, in terms of processes and better management of the activity, to ensure that both the external and internal dimensions of this activity are adequately addressed. Concrete steps taken in this direction in 2023 included splitting this activity into two distinct parts, with relevant KPIs introduced in the 2024 SPD. It is expected that this recalibration of work, combined with an increase in the number of FTEs allocated as a result of enlisting external support, will rebalance the workload within the unit, with a significant improvement in staff's work–life balance.

The way forward is to leverage the use of analytical tools to make the data easier to reuse within the activity and with other ENISA activities. As ENISA's work increasingly focuses on the processing of data to support evidence-based outreach and risk assessments, there is a need to increase the executive director's office data collection and analysis skillset.

Objectives

- Increased effectiveness and efficiency in achieving Agency objectives
- Fully compliant with legal and financial frameworks in our performance (build a culture of compliance)
- Protect the Agencies assets and reputation, while reducing risks
- Achieve full climate neutrality of all operations by 2030

Results

- Maximise value for money provided to stakeholders and citizens
- Build lasting credibility and trust

Link to corporate objective

- Sound resource and risk management

Outputs	Outcome
11.1. Maintain performance management framework including through single administrative practices across the agency	In September 2023, the agency migrated to the centralised records management system (used by the Commission and other EU institutions). This task required the establishment of a general register for ENISA official files using the Advanced Records System as the official documents management system for registering, filing and accessing documents and for workflow management. The HAN / Advanced Records System environment enables centralised management of the filing plan and provides an official repository for official documents. Establishment of the document management framework is intended to ensure sound document management through single administrative practices across the agency. During 2023, 49 management team meetings took place, and draft minutes were distributed to all ENISA staff within 1 day of each meeting, in line with the agency's commitment to transparency in decision-making. As part of standard compliance tasks, internal risk assessment, internal control assessment and audit follow-ups were conducted. In addition, a new project management tool was piloted to support staff throughout the life cycle of initiating, executing and finalising work programme implementation actions. Although the tool in its current form is static, meaning that it is merely a repository of information about work programme activities, outputs and projects, it has the potential to streamline and enhance internal processes via the automation of workflows and linkage with other tools, for example for budget monitoring. In 2023, an ENISA stakeholder survey was also conducted to measure stakeholder satisfaction with ENISA's work, specifically their perception of the outcome/results of ENISA's work and how the work was carried out and their trust in ENISA's abilities. A total of 163 responses were received from across the cybersecurity community, including from statutory bodies, expert groups and other external stakeholders. The results of the survey became available in early 2023 and have already been discussed in the 2022 annual activity report. This was the first time that such a large stakeholder satisfaction survey had been conducted. A lesson learned from this exercise is that, in the future, rather than administering a single generic survey, the questions should be tailored to individual activities. For this reason the survey should be incorporated into the foresight and knowledge management activities of the agency.
11.2. Develop and implement annual communications strategy	By transitioning ENISA's corporate websites and portals to the cloud and by implementing strong security measures, such as DDoS protection, the agency further fortified its online presence in 2023. To implement the communications strategy, a total of 25 individual communication plans were completed jointly with operational units and teams. The communications sector supported the publication of 34 reports, 20 press releases and 14 news items during 2023. The communication activities resulted in 839 media mentions of ENISA in 2023, down from 1 150 in 2022. This decrease should be seen in the context of a qualitative assessment of such mentions. Element of 'newsworthiness' was used in 2023, for example focusing on news that can have an impact and uptake by the media outlets. During 2023, ENISA's website received 2.3 million visitors, up from 2.03 million in 2022. Social media impressions also increased in 2023, to 4.4 million (compared with 3.6 million in 2022). This increase can be attributed to the proactive approach to its website that the agency adopted in 2023, which led to a restructuring of its thematic topics, coupled with the agency's strategic promotion across various platforms, social media channels and events. ENISA organised a total of 126 events in 2023. These included meetings and workshops, as well as 27 meetings of statutory bodies. ENISA updated its events policy to support this. For example, if the number of participants is 40 or more, attendees are asked to complete an event satisfaction survey. In 2023, 16 events fell into this category, and 664 responses were received. Of the 664 respondents, 320 (48.14 %) were overall 'very satisfied' with the organisation of the event and 280 (42.16 %) were 'satisfied'. The responses were further processed to define metrics and KPIs for 'lessons learned'. The background of participants at ENISA events in 2023 was as follows: industry, 37 %, MSs, 33 %; EU public organisations, 7.5 %; academia, 6.5 %; and international organisations, 6 %. The internal communications strategy, as part of the overall communications strategy, also contributed to building trust in the agency. The internal communications function during 2023 held 16 question and answer sessions and six ENISA academies and informed headquarters staff about upcoming events by displaying a list of such events on dedicated TV screens. In addition, communications staff issued weekly management team updates in the form of short debrief videos and, jointly with colleagues from the Corporate Support Services (CSS) Unit, made a total 171 of internal announcements in an effort to keep staff informed and engaged. In addition, the ENISA code of conduct was updated and adopted by means of an executive director's decision; dedicated information sessions were arranged, and handouts were made available for all staff. In total, 11 management board decisions, 88 executive director decisions and 11 administrative notices were adopted.
11.3. Develop and implement risk management plans, including an IT systems cybersecurity risk assessment, with a focus on the quality management framework and business processes as well as relevant policies	An enterprise risk assessment and an IT security risk assessment were conducted in 2023. The findings were reported to the management board and followed up with detailed action plans. ENISA also participated in relevant activities of the EU agencies network on risk management, including the peer-review risk assessment exercise for decentralised agencies in Q4 2023. In addition, as part of its risk management framework, in 2023 ENISA initiated supplier security assessments and the first on-site visit to a key external service provider took place. Another development in 2023 was the adoption of ENISA's code of conduct. This sets out ENISA's expectations regarding staff members' behaviour and conduct towards their colleagues, supervisors and the organisation as a whole, as well as towards citizens and stakeholders. The code of conduct is built on the principles of independence, impartiality, objectivity, loyalty, circumspection, transparency and accountability, mutual respect, integrity and lawfulness. It applies to all staff members regardless of employment agreement or rank and respect of its provisions forms the basis of the annual employee appraisal exercise.

11.4. Maintain and monitor the implementation of agency-wide IT management processes and develop budgetary management processes

The budget management committee

In 2023, three interim budgetary reports and a final budgetary report at year end were produced. Key conclusions from 2023 regarding the budget execution, payments rates and transfers are reported in relevant sections of the annual activity report.

The IT management committee

The IT management committee continued its work, started in 2022, on drafting, quality assurance and approving pending IT policies. It also examined and sanctioned the IT budget for 2023, overseeing the implementation of the budget in alignment with the global IT plan and the overall process for submitting requests for new or modified system. Furthermore, the committee handled 27 requests comprising statutory actions, requests for new systems and information points.

Importantly, the committee prepared a comprehensive proposal for revamping IT governance, with a shift towards centralisation of services and creation of an operational IT capability, as per the objective and goals set in the corporate strategy. The new IT governance at ENISA was adopted by Executive Director's Decision No EDD/05/2024.

11.5. Manage and provide secretariat for statutory bodies (executive board, management board, national liaison officers, advisory group)

Both the management board and the executive board saw a changing of the guard in 2023. In June, a new chair and deputy chair were elected to the management board, and in October and November four members/alternates were elected to the executive board. The executive board elections were held online. Two ordinary management board meetings were held. The management board adopted the necessary decisions in line with its mandate. A number of written procedures also led to the adoption of several decisions during the year. An informal meeting in March focused on strategic discussions. The management board, considering resource constraints, provided recommendations for the prioritisation of ENISA outputs and work programmes beyond 2024. Four online executive board meetings were held in 2023 (in January, May, July and October).

On 9 February 2023, following a public call for expressions of interest and a subsequent selection procedure, the management board adopted Decision No MB/2023/02 on setting up an advisory group for 2023–2025. The decision states that the advisory group will comprise 33 *ad personam* selected experts and eight nominated organisations, in line with Article 21 of the CSA, and that its term of office will be 2.5 years, from 1 February 2023 to 31 July 2025. The group will place particular thematic emphasis on recommendations for ENISA's work programme regarding the implementation of NIS 2, as this will be a key element of the agency's work during the lifetime of the advisory group. The newly composed advisory group held two formal meetings in 2023, complemented by an onboarding seminar, and five written validation requests for items to be included in the 2023 work programme were addressed.

The group's 2023 summer survey (which attracted 36 responses) provided further guidance's on the prioritisation of ENISA's future of outputs. A framework for self- initiative opinion papers was agreed by the advisory group (via terms of reference). Several topics for such opinion papers, falling into distinct clusters, were proposed.

- **Cluster 1.** Disruptive emerging trends and threats/cyberattacks, for example information distortion, threat projections and cognitive threat.
- **Cluster 2.** Digital sovereignty and innovation, for example AI, cryptography, post-quantum, skills/talent retention.
- **Cluster 3.** NIS implementation, critical infrastructures, NIS sectors, for example sector-specific papers, establishing trust, NIS 2 implementation.
- **Cluster 4** Infrastructure, services and supply chains, for example supply chain security, European Parliament elections, digital identity.
- **Cluster 5.** The general advisory group strategy and specific advisory group outlook on ENISA and the EU cybersecurity framework, for example the EU in the age of digital transition, advisory group guiding principles.

The NLO Network held three meetings in 2023. In addition, three NLO subgroups undertook additional work and held meetings, namely the NLO subgroup on the EU CSI (output 8.1), the NLO subgroup on NCSSs (output 3.1) and the NLO subgroup of cyber Europe planners (output 3.2).

Eight new NLOs and two new NLO alternates were appointed in 2023. In addition to individual onboarding and an onboarding webinar for all new NLOs was organised by the NLO secretariat.

The NLO Network was consulted via a written procedure on nine dedicated validation requests for 2023 work programme outputs.

11.6. Obtain and maintain the EU Eco- Management and Audit Scheme (EMAS) certificate through continuous overview of the CO_2 impact of all operations of the agency, in line with applicable legal framework, and publish an environmental statement	In 2023, ENISA carried out a technical study to calculate the agency's carbon footprint in 2022. Since 2022 several actions to reduce greenhouse gas (GHG) emissions have been implemented, such as recycling of office waste, the establishment of a watering system and the incorporation of specific provisions for GHG emissions in procurement procedures/tenders. The areas with the highest carbon footprint are business travel, energy consumption and consumption of fuel and resources. The next steps, planned for 2024, are the development of an environmental statement, external verification and the implementation and registration of an environmental management system (in accordance with the EMAS regulation).

Key performance indicators Organisational performance culture Trust in the ENISA brand	**Unit (of measurement)**	**Frequency**	**Data source**	**2022 results**	**2023 results/ target**
11.1. Proportion of KPIs reaching targets	Number	Annual	Annual activity report	Targets established as of 2023; however, compared with the base year (2021), 13 metrics were unchanged, 21 underperformed and 58 overperformed	69 % / 65 %
11.2. Individual staff contribution to achieving the objectives of the agency via clear link to KPIs in staff career development report (all units aggregated)	%	Annual	Staff survey	64 %	86 % (45) / 85 %
11.3. Exceptions in the risk register	Number	Annual	Internal control	27	23/11
Deviation from financial regulations	Number	Annual	Internal control	26	23/10
Deviation from staff regulations	Number	Annual	Internal control	1	0/1
11.4. Number of complaints filed against ENISA including the number of enquiries/complaint s to the EU Ombudsman	Number	Annual		3	2/12
To European Ombudsman	Number	Annual	ENISA functional mailbox	0 (46)	1
As Article 90	Number	Annual	Internal control files	3	1
To the European Data Protection Supervisor (EDPS)	Number	Annual	Internal control files	0	0
11.5. Number of complaints addressed on time and in accordance with the relevant procedures	Number	Annual	Internal files	3 (Article 90(2) and complaints to the EU Ombudsma n successfully closed on time and in accordance with the relevant procedures	2/NA
11.6. Number of high risks identified in annual risk assessment exercise	Number	Annual	Internal control files		4/NA
11.7. Implementation of risk treatment plans	Number	Annual	Internal control files		In progress
11.8. Number and types of activities at each engagement level (47)	Number	Annual	Report		Total activities: 149 Partner level: 36 % Consult level: 19 % Engage level: 22 % Inform level: 23 %
11.9. Observations from external audit bodies (e.g. the European Court of Auditors (ECA)) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed)	Number	Annual	Report	2	1/2
11.10. Level of trust in ENISA (48) (survey)	%	Biennial	Survey	95 %	NA
Allocated FTEs as per SPD, based on full establishment at 2023 year end	18	**Number of FTEs actually used**			16.74 (in addition 2 FTEs external contract services)
Planned budget (EUR) (49)	849 000	**Budget consumed (EUR) (50)**			976 458
		Of which carried forward to 2024 (EUR)			374 263

NA, not applicable.

(45) Based on responses to a question in the 2023 staff satisfaction survey asking staff if they 'understand how their job contributes to ENISA's strategic priorities and goals'.

(46) Complaints submitted in late 2021 were closed in Q3 2022.

(47) Stakeholder management at the agency is decentralised and handled at activity level. Each activity in the SPD focuses on the needs of a specific group of stakeholders in the cybersecurity ecosystem. The relevant stakeholders are identified, and the desired level of engagement is determined. At the closure of a project, stakeholder management is implemented and stakeholder feedback is elicited. Subsequently, KPIs are reported at the activity and output levels.

(48) Based on the proportion of respondents to the stakeholder satisfaction survey who said that they 'agree' or 'somewhat agree' with the statement 'I am confident in ENISA's ability to achieve its mandate'.

(49) Direct costs only: consultancy and missions linked to activity 11.

(50) Direct costs only: consultancy and missions linked to activity 11.

ACTIVITY 12:
Staff development and working environment

This activity supported ENISA's activities under Article 3(4) of CSA, which obliges the agency to 'develop its resources, including [...] human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation'. Actions under this activity focused on attracting, retaining and developing talent and building ENISA's reputation as an employer of choice and an agile and knowledge-based organisation where staff can evolve personally and professionally, feel engaged and motivated and experience a sense of belonging. The activity continued building an attractive workspace by establishing and maintaining excellent working conditions (premises, layout of office space), developing user-centric (tele)working and conferencing tools (including IT systems and platforms) and supporting ENISA's business owners and stakeholders in line with the agency's objectives.

In 2023, the Corporate Support Services (CSS Unit) was able to maintain day-to-day business and to continue to support critical services. However, its resources were overextended, making necessary the use of overtime and surplus hours. The unit's daily workload also included activities arising from the additional resource of EUR 15 million stemming from the cybersecurity support action. This further stretched the resources of the CSS Unit, primarily affecting the Budget, Finance and Procurement Team. At the same time, the unit centralised financial transactions to maximise compliance and control in the processing of operations.

In 2023, management of the corporate IT budget was improved the and zero-cost principle was applied, which resulted in significant improvements in ENISA's operations. Several IT-related projects aimed at improving the IT security infrastructure and the agency's digital transformation were initiated and completed, or are nearing completion. The CSS Unit prepared and implemented the Mission Processing System and the Public Procurement Management Tool (PPMT), digitalised recruitment by means of an e-platform and transitioned to a new IT service delivery corporate ticketing tool. Microsoft Teams was introduced as a corporate communication tool, and audiovisual leasing services were introduced to provide interactive and soundproof meeting facilities. ENISA successfully outsourced facility management services, a cost-effective solution that reduced administrative burden and financial risk. Improvements were made in ergonomic office design and building maintenance. The CSS Unit created a comprehensive library of SOPs and procedures for IT governance and increased cybersecurity defences by implementing ISO recommendations and findings.

ENISA is continually working to enhance its cybersecurity posture and has put considerable effort into complying with 'Protection of European Union classified information' requirements, such as developing a robust security governance framework and creating detailed SOPs and procedures. The organisation aims to achieve 'Protection of European Union classified information' accreditation for its Brussels office in 2024.

In 2023, the CSS Unit was unable to achieve certain human resources (HR)-related and financial goals identified in the corporate strategy owing to limited resources. A first draft of the revision of the current learning and development and performance system was implemented. However, talent development and growth, innovation and simplifications of SOPs on financial transactions were deprioritised to meet other agency-wide priorities. The use of external contractors for tasks such as missions was not executed, and further improvements in budget planning and monitoring could not be implemented because these are manual and time-consuming processes. The unit requires an integrated budget planning tool with automated dashboards to reduce financial management risks. This would also significantly increase the service provision and financial maturity.

In 2023, ENISA's 2023–2026 corporate strategy, which includes its HR strategy, was endorsed by the management board, which set the key areas for development in CSS for the future. The overall shortcomings in the areas of HR and finance adversely affected service delivery and the implementation of key results areas of the corporate and HR strategy. All of the main key HR processes, with the exception of payroll, were delayed, and none of the key strategic priorities on talent management and innovation, growth and competency development could be achieved. The absence of key framework contracts implementing HR development services, such as 360° evaluation, competency development, and learning and development, contributed to delays in planning learning and development activities. The overall service of implementing the newly drafted strategic workforce planning decision was seriously impacted. In addition, HR activities aimed at staff engagement and employer branding were deprioritised or could not be followed up. The continues lack of sufficient legal knowledge and expertise proved to be detrimental to the progress of different files, and the unit had to engage with different SLAs in handling legal requests.

Despite good progress, the agency's overall (and consequently organisational) performance was badly affected, and business continuity has proven to be a challenge. Overall, the unit needs to use the annual workforce review exercise in 2024 to review posts and functions, as well as their allocated grades, with a view to ensuring that these are appropriate to meet the agency's short-, medium- and long-term business needs, to address work programme priorities and to implement the corporate and HR strategies. As some functions are critical for strategic decisions and corporate results, a review of the business operating model, redesigning the strategic, tactical and operational work modalities, is required. To this end, the CSS Unit should carry out an internal review of its structure and, for each post, assess whether the grade is appropriate for the responsibilities performed. This should be followed by an assessment of its workforce needs and a reorganisation of functions to ensure that the unit is able to address business priorities and meet corporate objectives.

CSS continues its transformation path in terms of people development, processes and policies, and its services are at the core of all ENISA operations and instrumental to the execution of work programme outputs.However, the resources allocated to the unit are not sufficient to handle the breadth of work, outputs and deliverables entrusted to it. The unit will continue to use external service providers to perform essential functions, with the associated risk and cost to be borne by ENISA, and proceed to restructure functions and services in order to meet the demand and address the competency gap.

In terms of the KPIs, the majority of metrics, notably learning and development, exceeded their targets. However, staff satisfaction was below the target value, driven mainly by time management and stress levels, which will be addressed in the new corporate strategy.

Objectives

- Engaged staff, who are committed and motivated to deliver, and empowered to use fully their talent, skills and competences
- Consistent and regular review of the agency's resources, to ensure that these match the organisation's needs, while seeking internal and external efficiency gains across the organisation
- A digitally enabled workplace environment (including home work-space) that promotes good performance and considers social and environmental responsibility
- Enable operations at the highest level of security
- Build a culture of continuous improvement and agility, one that is customer centred and with a can-do attitude

Results

- ENISA as an employer of choice, and one enabling growth and excellence in a secure environment

Link to corporate objective:

- Build an agile organisation focused on people

Outputs	Outcome
12.1. Manage and provide high-quality recurrent support services in the area of resources, security (51) and infrastructure for ENISA staff, employees, corporate partners and visitors	The CSS Unit continued to deliver recurrent regular services in the area of HR, finance, procurement, budget planning, IT, facilities and security as a baseline service. While improvements were made in some key areas, in particular the area of security, resources were stretched and service delivery was adversely affected. An example of cross-unit collaboration is the CSS Unit's partnership with the operational cooperation unit (OCU) to implement the cybersecurity support fund, the first example of a 'business partnering' model at ENISA. The overstretched resources in the budget and finance teams delayed the modernisation of financial services and timely revision of the ENISA budget structure. In 2023, despite overstretched resources, the CSS Unit implemented the establishment plan with a 98 % execution rate and maximised the use of the EPSO cast lists and other reserve lists to recruit subject matter experts. The first internal mobility call (to encourage staff mobility and provide a means of career development) was implemented and resulted in a number of staff transfers. The CSS Unit continued to implement comprehensive facilities management procedures to optimise productivity and well-being in all buildings and spaces. This involved regular assessments and adjustments to meet the needs of both ENISA staff and stakeholders. ENISA spearheaded initiatives to ensure that all ENISA buildings and spaces promote productivity and well-being; this involved making ergonomic adjustments, optimising natural light, enhancing common spaces and ensuring compliance with health and safety standards. The unit also prioritised the maintenance of and strategic upgrades to critical IT systems, networks and communications infrastructure, to maximise uptime, resilience and adaptability to support current operations and evolve with emerging technology trends. In addition, IT infrastructure was maintained or upgraded to ensure continuous operations and facilitate seamless collaboration; this included physical infrastructure upgrades and implementing collaborative tools and platforms to enhance teamwork across different locations and functions. In terms of the overall budget management and execution of Title I and Title II, significant improvements were seen in 2023. In the case of Title I, the payment rate was 96.3 % (compared with 95.3 % in 2022 and 93.3 % in 2021) while carry-forward in Title I was 3.7 % (compared with 4.7 % in 2022 and 6.7 % in 2021). In the case of Title II, the financial indicators also demonstrate similar improvements: a payment rate of 63.8 % (compared with 59,1 in 2022 and 40.2 % in 2021) and a reduced carry-forward of 36.2 % (compared with 40.9 % in 2022 and 58.8 % in 2021). Thus, despite resource constraints in all areas of the activity, the aim of increasing financial maturity produced fruitful results; however, there is still room for improvement.
12.2 Develop and implement the agency's corporate strategy (including its HR strategy) with an emphasis on talent development and growth, innovation and inclusiveness	ENISA's 2023–2026 corporate strategy was endorsed by the management Board in June 2023. The strategy will not only act as a baseline but will constitute a long-term vision and plan to be used by the agency to manage its resources, define service standards and create a revised business operating model. Given overstretched resources in HR and the current maturity and knowledge level, this output's deliverables have been rescheduled to start in 2024 and continue over the subsequent years. In 2023, the CSS Unit introduced automated tools to improve recruitment selection processes and is finalising a new online tool for maximising staff engagement. In doing so, ENISA's five key competencies were introduced in all appraisal and recruitment processes. A revised selection methodology, purely competency driven, was introduced with the aim of **focusing on the transferable skills and competencies of staff and new applicants**. The results of the existing processes and feedback from staff received were taken into consideration when revising the HR and talent development policies, strategies and processes.
12.3. Enhance operational excellence and digitalisation through modern, secure and streamlined ways of working and self-service functionalities	In 2023, the CSS Unit introduced a new mission management system (MiPS+) and an online recruitment platform and achieved significant milestones in connecting its accruals-based accounting (ABAC) system with a contract module and the PPMT. It also decommissioned all legacy systems, reducing the risk of vulnerabilities, and moved ahead with further IT improvements and the digitalisation of services. The unit also introduced an IT service ticketing tool and in 2024 will continue its expansion in facility management, security and, later, HR modules. CSS continued to improve the availability of the EU HR management system (Sysper) to staff members and to provide continuous support. In 2023, CSS successfully implemented seven new modules of the HR management information system, which involved a systematic approach that focused on meeting the agency's needs while ensuring smooth integration and user adoption. A great achievement was the deployment of a reporting module for retrieving reliable HR-related data, but more work is needed to align HR and financial data for workforce planning purposes. In 2023, CSS introduced several new IT tools to enhance collaboration between ENISA colleagues and external partners. These tools include the latest operating systems and productivity tools, a virtual private network infrastructure to improve teleworking effectiveness, a new recruitment platform and an advanced IT digital transformation and service management platform. Moreover, to further improve security and offer innovative human-centric services, ENISA has adopted a zero-trust approach to IT systems and implemented a mobile device management solution to enhance the security of mobile devices. CSS made Microsoft Teams its primary collaboration platform and installed new conference systems to improve communication and collaboration.
12.4. Provide a secure, safe, modern and welcoming place to work (and telework) and promote staff welfare	In 2023, ENISA continued to ensure that staff have a modern and welcoming place to work and telework and promoted staff welfare through measures such as financial support for the education of staff members' children, the provision of medical advisor services, other welfare measures. CSS also ensured that all ENISA employees can access ergonomic and modern work equipment, for example by providing electrically adjustable desks, ergonomic office chairs, multiple high-resolution screens and peripheral equipment. ENISA's premises are protected by high-level physical security 24/7 and are compliant with the maximum safety standards required by the staff regulations.

(51) Including achieving full 'Protection of European Union classified information' accreditation by the end of 2023, which has been confirmed by Directorate-General for Human Resources and Security.

12.5. Set up service provisions standards and service optimisation processes	In May 2023, Executive Director's Decision No EDD/24/2023, on specifying the roles and responsibilities of ENISA's structural entities and on putting in place other organisational measures to ensure efficient performance of the agency's tasks and functions, was adopted, further to which the financial initiating agent (FIA) function was centralised under CSS. In addition, in July 2023, Executive Director's Decision No EDD/37/2023, on a framework of the financial delegation of the authorising officer, was adopted. This provides further details on financial circuits and financial delegations, as well as on the roles and responsibilities of financial actors (FIA, financial verification agent, authorising officer by delegation) and KPIs for financial management. In 2023, CSS IT revised and updated the IT governance framework. The aim was to improve the service levels and ensure seamless service delivery by adhering to best practices and ITIL standards. As a result of this update, the ENISA's IT helpdesk has now obtained full ITIL certification. A first attempt to define a costing model for non-essential services was introduced; however, the results, as well as the service delivery standards for CSS, have yet to be disseminated as limited resources and additional activities and scope have forced the unit to reprioritise its tasks.

Key performance indicator **Staff commitment, motivation and satisfaction**	**Unit (of measurement)**	**Frequency**	**Data source**	**2022 results**	**2023 results/ target**
12.1. Staff satisfaction survey (including the attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools)	%	Annual	Staff satisfaction survey		64 %/75 %
Percentage of staff who would recommend ENISA as an employer	%	Annual	Staff satisfaction survey	NA	74 %
Percentage of staff who have enough authority to do their job	%	Annual	Staff satisfaction survey	NA	68 %
Percentage of staff who have opportunities to have their ideas adopted and put into use	%	Annual	Staff satisfaction survey	NA	64 %
Percentage of staff who feel encouraged to come up with new or better ways of doing things	%	Annual	Staff satisfaction survey	NA	61 %
Percentage of staff who are asked for their opinion on decisions that affect their daily work and tasks at ENISA	%	Annual	Staff satisfaction survey	NA	56 %
Percentage of staff who are satisfied with their work	%	Annual	Staff satisfaction survey	76 %	76 %
Percentage of staff indicating that their line manager provides sufficient feedback on their performance	%	Annual	Staff satisfaction survey	60 %	64 %
Percentage of staff who feel well informed by ENISA's leadership regarding important matters	%	Annual	Staff satisfaction survey	36 %	46 %
12.2. Quality of ENISA training and career development activities organised for staff	%	Annual	Staff satisfaction survey	48 %	58 %/55 %
Percentage of staff indicating that courses match their training and development needs	%	Annual	Staff satisfaction survey	43 %	47 %
Percentage of staff reporting that their line manager dedicates enough time during the career development report dialogue for mapping training and development needs	%	Annual	Staff satisfaction survey	36 %	61 %
Percentage of staff who agree that the learning and development opportunities at ENISA help them to maintain and develop their transferable competencies	%	Annual	Staff satisfaction survey	36 %	44 %
Percentage of staff who know which key competencies they are required to maintain or develop	%	Annual	Staff satisfaction survey	71 %	76 %
Percentage of staff who agree that their learning and development objectives are consistent with the competencies they need for their career	%	Annual	Staff satisfaction survey	55 %	63 %
12.3. Reasons for staff departure (exit interviews) (52)	Scale 1–10	As required	HR files	7.9	7.9/7.5
12.4. Turnover rates	%	Annual	HR files	4 %	4.9 %/3 %
12.5. Establishment plan posts filled	%	Annual	HR files	89 %	98 %/95 %
12.6. Resilience and quality of ENISA's IT systems and services	%	Annual	IT reports and staff satisfaction survey	73 %	96.66 %/80 %
Critical systems downtime	%	Annual	Uptime report for Fortimail / SolarWinds	100 %	99.97 %
Percentage of central IT infrastructure assessments with few (< 5) critical findings	%	According to needs	Intranet repository	100 %	NA (53)
Percentage of central infrastructure patched to the last formal versioning of 1 year	%	Annual	Yearly IT maintenance plan in PDF format	97.33 %	99.90 %
Percentage of major IT helpdesk requests resolved in a satisfactory way within 2 business days	%	Annual	IT ticket repository	79.28 %	90.00 %
12.7. Percentage of procurement procedures launched via e-tool (PPMT)	%	Annual	IT ticket repository	79.28 %	90.00 %
12.7. Percentage of procurement procedures launched via e-tool (PPMT)	%	Annual	Procurement files	NA	100 %/ > 90 %

(52) Exit interviews are an opportunity for ENISA to seek feedback about staff members' experience. Staff are asked a set of 10 standard questions, each scored on a scale of 1 to 10. The higher the number, the better their experience.

(53) Assessments are conducted in accordance with the needs of the agency; no changes occurred in 2023.

12.8. Percentage of payments made within 30 days	%	Annual	Finance files		NA	90 %/ > 90 %
12.9. Late payments	%	Annual	Finance files		NA	9 %/ < 10 %

Planned budget (EUR) (54)	4 417 000 (55)	**Budget consumed (EUR) (56)**	4 619 097
		Of which carried forward to 2023 (EUR)	1 490 324
Allocated FTEs. as per SPD based	17	**Number of FTEs actually used**	14.31 (in addition 16.25 FTEs external contract services)
On full establishment at 2023 year end			

NA, not applicable.

(54) Direct costs only: staff learning and development, staff welfare, external temporary staffing, building and corporate ICT costs, other administrative costs, consultancy and travel expenditure linked to activity 12.

(55) Indicated budget excludes staff (temporary agents, contract agents, seconded national experts) salaries and allowances.

(56) Direct costs only: staff learning and development, staff welfare, external temporary staffing, building and corporate ICT costs, other administrative costs, consultancy and travel expenditure linked to activity 12.

PART II (A) MANAGEMENT

2.1 Management board

The management board of ENISA is composed of representatives from each MS and from the European Commission. The term of office of the members of the management board and their alternates is 4 years. That term is renewable.

The main role of the board is to approve the agency's work programme, but it also establishes the budget of the agency and verifies its execution. Other essential roles of the board are to appoint the executive director and to adopt appropriate financial rules. The management board thus ensures that the agency sets the conditions necessary for its tasks to be delivered as provided for in the CSA.

In 2023, three ordinary meetings and one extraordinary meeting of the management board were held. The extraordinary meeting was convened to facilitate the online voting to fill three positions on the ENISA executive board.

The management board strategy meeting opened with a discussion of topics covered in a previous meeting, namely the status of the ENISA cybersecurity support action, international relations and the adoption of ENISA's corporate strategy.

Strategic discussions were held to gather guidance for ENISA'S future work programme priorities based on the lessons learned from the 2022 annual activity report.

In total, the management board made 12 decisions during the year, including a decision on setting up an ENISA advisory group for 2023 to 2025. In accordance with the CSA and the management board rules of procedure, the management board decisions were prepared by the executive board and adopted by the management board. The 2022 annual activity report was adopted. The management board also expressed its opinion on the final annual accounts for the 2022 financial year and adopted the 2024–2026 ENISA SPD, including the 2024 budget and establishment plan.

Finally, the management board and the executive board saw a changing of the guard with the election of a new management board chair and deputy chair in June 2023 and the election of four members/alternates of the executive board in October and November.

2.2 Major developments

In the light of Russia's war of aggression against Ukraine, on 9 March 2022, EU telecommunications ministers unanimously urged the Commission to establish of a new Emergency Response Fund for Cybersecurity. To facilitate short-term support, the Commission allocated additional resources to ENISA, aiming to enhance its assistance to MSs, as per ENISA's CSA mandate. Consequently, in 2022, the Commission increased ENISA's budget by EUR 15 million, some of which remained to be disbursed in 2023, reinforcing ENISA's capacity to support MSs promptly.

Within the framework of cybersecurity support actions, ENISA provided MSs with various services, including penetration tests, cybersecurity drills, incident response, risk monitoring and training sessions. Ultimately, the agency successfully spent 100 % of the committed budget of EUR 15 million.

New advisory group. In 2023, ENISA concluded the selection process for new members of the advisory group. The advisory group's role is to provide counsel to ENISA on its tasks, excluding the cybersecurity certification framework. This group is tasked with ensuring communication with relevant stakeholders concerning ENISA's annual work programme and advising the executive director on formulating the agency's annual work programme. A total of 33 candidates were selected, based on their specific expertise and merits, to form ENISA's new advisory Group, each serving a term of 2.5 years. The group comprises leading experts representing various stakeholder groups such as the NIS industry, academia, research, non-governmental organisations, citizens and nominated organisations including BEREC, CEN, CENELEC, CERT-EU, the EDPS, the ETSI, eu-LISA, Europol (EC3) and the European Border and Cost Guard Agency.

The mandate of the newly established advisory group spans from 1 February 2023, to 31 July 2025.

Management Board. In 2023, ENISA's management board elected a new chair and Deputy. Fabienne Tegeler (Germany) replaced the outgoing chair, Jean-Baptiste Demaison (France), while Stefan Lee (Finland) succeeded the outgoing vice-chair, Krzysztof Silicki (Poland). The board's main functions include approving the agency's work programme, establishing its budget, ensuring its execution, appointing the executive director and adopting suitable financial regulations, thereby ensuring that ENISA operates in line with the CSA.

International cooperation. ENISA formalised a working arrangement with its Ukrainian counterparts in 2023, focusing on capacity building, best practices exchange and enhancing situational awareness. The agreement involves ENISA, the National Cybersecurity Coordination Centre of Ukraine and the Administration of the State Service of Special Communications and Information Protection of Ukraine. This arrangement encompasses short-term structured cooperation actions while also facilitating the alignment of cybersecurity policies and implementation approaches in the long term.

Also in 2023, ENISA signed a working arrangement with the Cybersecurity and Infrastructure Security Agency (CISA) of the United States, centred on capacity building, best practices exchange and bolstering situational awareness. ENISA's international strategy emphasises selective engagement with international partners, focusing on areas and activities that offer high and measurable added value in achieving strategic objectives. The working arrangement with CISA strengthens ongoing cooperation and opens avenues for new collaborations, covering both short-term structured cooperation actions and long-term alignment of cybersecurity policies and implementation approaches.

New 2023–2026 corporate strategy. ENISA's new corporate strategy, endorsed by the management board in 2023, aims to evolve into a dynamic, service-oriented organisation and an appealing workplace. The strategy focuses on establishing a long-term vision for resource planning and management aligned with baseline requirements and priorities set by the ENISA management board and EU law.

2.3 Budgetary and financial management

Financial management

During 2023, ENISA had an operating budget of EUR 25.2 million. For comparison, the 2022 budget amounted to EUR 39.2 million because ENISA was granted additional budget of EUR 15 million for the pilot implementation of a cybersecurity support action, activities on which continued throughout 2023. This cybersecurity support action was aimed at reinforcing ENISA's response capabilities in supporting MSs in accordance with its mandate, in particular under Articles 6 and 7 of the CSA, to improve the prevention, detection and analysis of cyber threats and incidents, and the EU's ability to respond to these, by providing MSs with knowledge and expertise. A further EUR 20 million was granted to ENISA in late December 2023 under a contribution agreement for the implementation of cyber support and situational centre actions during 2024–2026.

In 2023, in addition to the 113 very low-value contracts with direct award (less than EUR 15 000), ENISA concluded 24 public procurement procedures: six using the open procedure (25.0 %), 17 through reopening of competitions under framework contracts (70.8 %) and one was through a negotiated procedure for medium- and low-value contracts (4.2 %). No restricted procedures were launched (0 %). In 2023, the agency paid a total of EUR 1 060.11 in interest on late payments to EUIBAs.

The table below shows ENISA's budget implementation targets and achievements in 2023, which improved compared with 2022.

Area	Objective	2022 level of completion	2023 target	2023 level of completion
Budget implementation including support action (appropriations committed through the year)	Efficiency and sound financial management	99.93 %	95 %	NA
Budget implementation without support action (appropriations committed through the year)	Efficiency and sound financial management	99.91 %	95 %	100.00 %
Payments against appropriations of the year including support action (C1 funds)	Efficiency and sound financial management	52.02 %	80 %	NA
Payments against appropriations of the year without support action (C1 funds)	Efficiency and sound financial management	84.11 %	80 %	83.86 %
Payments against appropriations carried over from previous year (C8 funds)	Efficiency and sound financial management	95.07 %	95 %	96.14 %
Payments against appropriations carried over from previous year including support action (C8 funds)	Efficiency and sound financial management	NA	95 %	99.20 %

Budget execution of EU subsidy (C1 funds of current year 2023)

From 1 January to 31 December 2023, ENISA executed EUR 25 182 935 in commitment appropriations, representing 100.00 % of the total budget for the year, and EUR 21 118 393 in payment appropriations, amounting to 83.86 % of the total budget.

Compared with 2022, there was a slight increase in commitment execution – 100.00 % in 2023, compared with 99.93 % in 2022 (99.51 % in 2021). Overall payment execution decreased very slightly, to 83.86 % (compared with 84.11 % in 2022), excluding cybersecurity support action funds.

The target of 95 % for the commitment rate set by the Commission (Directorate-General for Budget) was reached. The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not paid at the end of 2023 were carried forward to 2024.

The tables below summarise the execution of the budget in 2023.

2023 budget implementation (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	12 693 659	12 693 482	100.00%	12 229 033	96.34%	464 449
Title II	3 700 001	3 700 001	100.00%	2 361 982	63.84%	1 338 019
Title III	8 789 835	8 789 453	100.00%	6 527 378	74.26%	2 262 075
TOTAL	**25 183 495**	**25 182 935**	**100.00%**	**21 118 393**	**83.86%**	**4 064 543**

Amending budget / budgetary transfers

According to Article 26 of the financial rules, the executive director may transfer appropriations:

- 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;
- From one chapter to another and within each chapter without limit.

Beyond the limit referred here above, the executive director may propose transfers of appropriations from one title to another to the management board. The management board has 2 weeks to oppose the proposed transfers. After that time limit, the proposed transfers will be deemed to be adopted.

During 2023, the agency made two transfers based on the executive director's decision on the adopted budget (compared with one transfer on the initial budget and three transfers on the amended budget in 2022).

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

The table below summarises changes to the budget 2023:

2023 Budget (C1) (EUR)	Initial budget	Amending Budget	Transfers approved by the Executive Director	Final budget
Title 1	12 719 412	-	-25 753	12 693 659
Title 2	3 519 470	-	180 531	3 700 001
Title 3	8 944 613	-	-154 778	8 789 835
TOTAL	**25 183 495**	**-**	**-**	**25 183 495**

Implementation of appropriations carried forward

The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not fully paid at the end of 2022 were carried forward to 2023 (C8 appropriations).

In 2023, overall payment execution for C8 funds (including the implementation of the Assistance Fund) reached 99.20 %, with a payment rate of 94.51 % for Title I, 98.69 % for Title II and 99.46 % for Title III.

Compared with 2022, there was an increase in payment execution for implementation of ENISA's 'normal' budget (i.e. excluding the implementation of the Assistance Fund) – 96.14 % in 2023, compared with 95.07 % in 2022.

Payment execution for the Assistance Fund reached only 99.99 %.

The total amount cancelled, including both the 'normal' budget and the Assistance Fund, was EUR 149 739, which represents 0.80 % of the total amount carried forward and 0.38 % of the full 2022 budget.

A large part of the amount cancelled had been provisionally committed to missions and events that had to be modified as a result of unforeseen circumstances, or to various training, coaching and staff development expenses, which are difficult to estimate, as well as to building-related expenditure (utilities, security, cleaning), which was lower than anticipated.

Implementation of C8 including Assistance Fund				
2023 Budget (C8) (EUR)	Appropriations carried forward from 2022 to 2023 (EUR)	Payment amount (EUR)	Percentage paid	Amount cancelled (EUR)
Title 1	675 605,75	638 526,48	94.51%	37 079,27
Title 2	1 883 887,30	1 859 234,41	98.69%	24 652,89
Title 3	16 223 132,65	16 135 125,33	99.46%	88 007,32
TOTAL	**18 782 625,70**	**18 632 886,22**	**99.20%**	**149 739,48**

Implementation of C8 without Assistance Fund				
2023 Budget (C8) (EUR)	Appropriations carried forward from 2022 to 2023 (EUR)	Payment amount (EUR)	Percentage paid	Amount cancelled (EUR)
Title 1	560 686,75	525 662,41	93.75%	35 024,34
Title 2	1 389 387,30	1 364 734,41	98.23%	24 652,89
Title 3	1 873 132,65	1 785 284,18	95.31%	87 848,47
TOTAL	**3 823 206,70**	**3 675 681,00**	**96.14%**	**147 525,70**

Implementation of C8 - Assistance Fund only				
2023 Budget (C8) (EUR)	Appropriations carried forward from 2022 to 2023 (EUR)	Payment amount (EUR)	Percentage paid	Amount cancelled (EUR)
Title 1	114 919,00	112 864,07	98.21%	2.054,93
Title 2	494 500,00	494 500,00	100.00%	-
Title 3	14 350 000,00	14 349 841,15	100.00%	158,85
TOTAL	**14 959 419,00**	**14 957 205,22**	**99.99%**	**2.213,78**

2.4 Delegation and subdelegation

As per Articles 39 and 41 of ENISA's applicable financial rules (57), '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 increased 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, head of units 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. No subdelegation was granted in 2023.

All the delegations and subdelegations are time limited. In the event of a change of the person of the executive director, all delegations (and subdelegations) 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 (Directorate-General for Budget).

2.5 Human resources management

In 2023, ENISA continued with the new organisational structure established by the management board in 2020. Guidelines for the proportional allocation of resources between the operational units and those that support the administrative and corporate functions were followed and the results reported indicated that the allocation of resources was appropriate.

The HR team continued to support the operational and administrative goals of the agency in terms of staff acquisition and development. In 2023, ENISA welcomed 19 new staff members (14 temporary agents and five contract agents).

In 2023, ENISA adopted, by analogy, the Commission decision on hybrid ways of working, with the new rules coming into force on 1 January 2023, and further applicable teleworking rules were explained in Executive Decision No EDD/2023/01 of 3 January 2023 implementing Commission Decision C(2022) 1788 on working time and hybrid working.

In terms of digitalisation, the agency undertook a series of initiatives and continued its transition from paper-based to self-service functionalities by preparing further HR modules in Sysper. In 2023, seven modules were implemented, relating in particular to time management and payroll.

Compliance remained a priority for the HR Unit, both in terms of meeting audit and internal control recommendations and in terms of meeting statutory requirements, for example in the area of personal data protection.

In 2022, the ENISA code of conduct was developed, and it was adopted in January 2023. The code of conduct outlines ENISA's expectations regarding staff members' behaviour and conduct towards their colleagues, their supervisors and the organisation as a whole, as well as their behaviour and conduct towards citizens and stakeholders.

The following table presents the performance of the HR team in 2023

Area	Objective	2022 performance	2023 performance	2023 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	≤ 5 months	≤ 5 months
Turnover of staff	Reduced turnover rate of statutory staff (temporary agents and contract agents)	4 %	4.9 %	< 15 %
Staff performance management	Implementation and monitoring of the appraisal and reclassification exercises (launching and completion of the exercises)	100 %	100 %	100 %

Implementing rules adopted in 2023

In 2023, ENISA adopted, by analogy, the Commission decision on hybrid ways of working, with the new rules coming into force from 1 January 2023, and further applicable teleworking rules were explained in Executive Director's Decision No EDD/2023/01 of 3 January 2023 implementing Commission Decision C(2022) 1788 on working time and hybrid working.

Brief description of the results of the screening/benchmarking exercise

In 2023, ENISA continued to apply the benchmarking exercise following the methodology of the European 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' increased slightly, to 26 %. A slight decrease can be observed in posts under the 'operational' area, estimated to account for 67 % of posts. The management board established a transitional period for the agency in the 2022–2024 SPD with regard to meeting the requirements outlined in Article 3(3) of Management Board Decision No MB/2020/9, which directs the executive director to take steps to ensure that the average number of staff members assigned to the Executive Director's Office and the CSS Unit does not exceed the average number of staff members assigned to operational units. The remaining 8 % of the posts were defined as 'neutral' posts.

(57) https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-2019_8-financial-rules

2.6 Strategy for efficiency gains

The agency has demonstrated significant productivity gains over the past years, having managed to absorb the growing workload stemming from the implementation of cybersecurity support action and policy changes.

In 2023, ENISA continued to work towards delivering efficiency gains across its operational and corporate administrative tasks.

The first step in this endeavour was the roll-out of the ENISA corporate strategy (approved by the management board in June 2023), which aims to improve ENISA's organisational efficiency and flexibility to meet operational needs and encompasses its HR strategy, greening, ENISA's digital strategy and service modelling.

In order to achieve the goals set out in the corporate strategy, the following benchmarks were taken into consideration when drawing up the agency's budgetary and HR plan from 2024 onwards:

- The agency's investment in talent development will increase from 2.1 % Of staff salaries in 2023 to 3.5 % In 2024;
- The agency's expenditure on movable property and costs related to retaining a modern workplace will remain below 1 % of the planned expenditure on the salaries of staff in active employment;
- The agency will dedicate over 40 % of its total investments to core, corporate and operational it systems in order to ensure the cybersecurity of these systems;
- The agency, starting from 2024, will offset 100 % of its carbon dioxide (CO_2), methane and nitrous oxide emissions (approximately 150 tonnes).

These will be generated across all its activities and as a result of its operations in the relevant budgetary period.

The HR strategy is part of the corporate strategy and is based on the multiannual plan for HR needs, which aims to achieve efficiency gains through the introduction of new tools, business process reviews and better organisation of the workload. In 2023, new Sysper modules for HR management, for missions and for document approvals and registry were introduced. Over the course of 2023, ENISA implemented the Advanced Records System, the Missions Integrated Processing System, the PPMT, ServiceNow (a key ticketing and service management tool) and an online recruitment platform, Allegro. In addition, work on implementing Sysper modules continued, as did work to expand the use of ABAC functionalities following the switch to a web-based ABAC platform.

The agency also began to explore the possibility of introducing new modules on contract management and of redesigning financial workflows to make use of the PPMT / Advanced Records System.

The agency continued to support the EU Agencies Network (EUAN) in relation to the implementation of cybersecurity requirements proposed in the draft regulation on common binding rules on cybersecurity for EUIBAs, namely through a concept of shared services on cybersecurity risk management, such as the concept of a virtual chief information security officer. This concept was developed in close cooperation with CERT-EU and another six EU agencies that volunteered to join the initiative.

In the area of facilities management and security, in 2023 ENISA completed the review of facility and security service and introduced an additional module named ServiceNow to integrate facility management and security requests.

The agency conducted an independent analysis of its financial procedures and processes which resulted in options for further simplification in the execution of its budget implementation and more flexible application of the budget expenditure in full compliance with the legal and financial framework.

Capitalising on shared services

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 shares accounting and data protection functions with the ECCC.

2.7 Assessment of audits and *ex post* evaluation results during the reporting year

Internal Audit Service

In 2023, the Internal Audit Service (IAS) conducted an audit on procurement and contract management in ENISA. The audit report will be finalised and shared with ENISA in 2024.

European Court of Auditors

In 2023, the ECA issued its report on the 2022 annual accounts of the agency (58). In the ECA's opinion, the accounts of the agency for the year ended 31 December 2022 present fairly, in all material respects, the financial position of the agency at 31 December 2022, the results of its operations, its cash flows and the changes in net assets for the year then ended, in accordance with its financial regulation and with the accounting rules adopted by the Commission's accounting officer. Moreover, the revenue and payments underlying the accounts for the year ended 31 December 2022 are legal and regular in all material respects.

Although not calling into question the ECA's opinion, in 2023 the ECA issued three observations on procurement- related processes. These three observations are currently being addressed by the agency.

However, the ECA qualifies its opinion on the legality and regularity of payments underlying the accounts because the operational payments made in the context of the "enhanced cybersecurity support from ENISA in the wake of Russia's invasion of Ukraine" are assessed as irregular. To implement this exceptional "cybersecurity support" which was adopted in August 2022 by ENISA's Management Board, the agency had, in accordance with the appliable EU financial rules, less than a five months period to sign legal commitments for a total amount of EUR 15 million (whereas ENISA's standard annual operational budget oscillates between EUR 8 and 9 million). In this short time period, ENISA successfully absorbed this unplanned additional workload by fully executing such complex action. Despite ENISA's best efforts to mitigate the inherent legal risks, the ECA deemed that the specific contracts signed in 2022 do not provide sufficient details (quantities, date of deliveries) of the services acquired (total value: EUR 13,2 million) as per ECA's interpretation of the EU financial rules. It is thus worth noting that the ECA is objecting on the legal form of the contracts but not on the end-result: altogether, the same contractors would have provided the same services to the same beneficiaries if the detailed specific contracts would have been signed in 2023.

ENISA shall provide its comments to the ECA preliminary audit observations in June 2024, with the objective to come to an agreement on the text to be adopted for the final ECA's audit report (including ENISA's reply to the audit observations).

Ex post control evaluation result

In 2023, ENISA contracted a leading international audit firm to perform an ex post control of financial transactions made during the 2022 financial year as per Article 45(8) and (9) of the ENISA financial regulation.

A total of 129 financial transactions were scrutinised, representing 4.99 % of the agency's financial transactions and 12.75 % 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. These two weaknesses led to two recommendations: (1) improve the monitoring of time to payment to ensure that all payments are made within their legal time limit and (2) improve the documentation supporting payments to ensure a proper audit trail.

2.8 Follow-up of recommendations and action plans for audits

Internal Audit Service

The IAS's final audit report on HR management and ethics was issued in September 2019. Three very important and four important recommendations were issued as a result of this audit. Although six recommendations were closed by the IAS following its review of the corrective actions implemented by ENISA, one sub-recommendation remained open at the end of 2022.

ENISA's HR strategy, which is aligned with the programming documents and aims to enable effective and efficient planning and allocation of HR to achieve the agency's objectives, was endorsed in 2023 by the

(58) https://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-2022-annual-accounts-eca-report.pdf.

management board, and all recommendations arising from the audit on HR management and ethics in ENISA have now been formally closed by the IAS.

In 2021, the IAS conducted an audit on strategic planning programming and performance management in ENISA, and it issued its final audit report in April 2022, with three important recommendations for ENISA.

In early 2023, the IAS performed a follow-up audit of these open recommendations to assess the progress made in implementing them. Based on the results of the follow-up audit, all recommendations arising from the audit on strategic planning, programming and performance management in ENISA have now been formally closed by the IAS.

European Court of Auditors

The ECA has deemed all previous years' observations (i.e. up to 2021) closed, except for the observation on the absence of evaluation reports and award decisions for low-value contracts. This weakness has been addressed by the agency and the ECA will review the corrective actions implemented by ENISA before closing this audit's observation.

2.9a 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.

2.9b Follow-up of observations from the discharge authority

In April 2024, the European 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 2022" and approved "the closure of the accounts of ENISA (European Union Agency for Cybersecurity) for the financial year 2022."(59)

The European Parliament also made some observations for ENISA to take into account in the coming years (60). The agency welcomed the feedback received from the European Parliament as part of the discharge process, which provides essential input into the agency's organisation and performance.

In reply to observations and comments made by the European Parliament in its discharge, the agency provided further information on actions taken to address previously identified areas for improvement and highlighted some actions taken that might be of interest to the European Parliament.

In particular: the agency took the steps necessary to mitigate the weaknesses identified by the auditors by strengthening its internal controls and updating its internal processes for procurement procedures; to better tackle concerns about gender and nationality balance, ENISA is continuously fine-tuning its HR policy.

2.10 Environmental management

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

ENISA further strengthened its environmental management by introducing a new output in 2022, namely an overarching audit on the CO_2 impact of all the operations of the agency in 2023.

To this end, ENISA, in 2023, carried out the following greening activities:

- With the assistance of an external contractor, it carried out a technical study to calculate the agency's carbon footprint in 2022.
- A final report was prepared, presenting the GHG emissions arising from ENISA's operations during 2022 (reporting period 1 January to 31 December 2022) at its three installations: its Athens headquarters in Greece, its Heraklion local office in Greece and its Brussels local office in Belgium.
- To achieve its goal of reducing GHG emissions, ENISA has, since 2022, developed different pathways of actions with different ambition levels. The main areas covered by the actions are business travel, energy consumption and consumption of fuel and resources.
- During 2023 several actions to reduce GHG emissions were implemented. These included recycling of office waste, the establishment of a watering system and the incorporation of specific provisions for GHG emissions in the agency's public procurement procedures / tenders.

The next stage, for 2024 onwards, is to implement an environmental management system and to work towards EMAS accreditation.

2.11 Assessment by management

The agency's operational and corporate activities were implemented in accordance with the 2023 work programme, with the necessary guidance and support of the management board. 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.

The agency regularly monitors the implementation of the action plans based on ECA and IAS audit recommendations. In 2023, 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 the staff of the agency 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.

(59) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0252_EN.html
(60) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023BP1905

PART II (B)
EXTERNAL EVALUATIONS

The last evaluation was finalised by ENISA in April 2023 and covered the 2021 and 2022 work programmes. 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 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 and The last evaluation was finalised by ENISA in April 2023 and covered the 2021 and 2022 work programmes. 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 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 and how feedback from external stakeholders is taken into account.

On aggregate, the results demonstrate that ENISA's deliverables provide high added value, with 93 % of stakeholders considering that the outcome/results of ENISA's work provide significant added value. Only 7 % of stakeholders surveyed considered the added value to be limited and none thought that ENISA provides no added value. In terms of take-up, 85 % of stakeholders also rated the likelihood of their taking up the results of ENISA work in support of their tasks in the immediate to medium term. ENIAA's operational cooperation activities, activities 4 and 5, were those that achieving the highest score in terms of immediate take-up (50 %), which, given the nature of these activities, is a good result.

The mandate of the agency requires that the tasks that it carries out do not duplicate MS activities. Therefore, the fact that 83.7 % 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. The agency will undertake analogous evaluations in 2025 for the 2023 and 2024 work programmes.

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 European 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 2023, this assessment was based on the indicators of the framework, and also on additional information from specific (risk) assessment reports, audit findings and other relevant sources. The assessment also followed the related guidance and templates developed through the EU Agencies' Performance Development Network.

Assessment of 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 partially present and functioning mainly due to deficiencies in the area of mandatory trainings on ethics and integrity for staff (where participation is very low).

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. Moreover, ENISA's code of conduct, including the code of good administrative behaviour, was adopted by Executive Director Decision No EDD/2023/02 in January 2023.

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

The assessment concluded that this principle is present and functioning well, and only minor improvements are needed.

In 2023, ENISA implemented, as a management supervision tool, a single monitoring table to monitor all major identified risks. The aim is to ensure effective follow-up of recommendations and the implementation of relevant mitigating measures.

ENISA regularly reports to its supervisory stakeholders (the management board, the discharge authority, the Commission, etc.) on the agency's operational and financial performance. The declaration of assurance of the executive director is included in this report (Part V). All authorising officers by delegation have signed their own declarations of assurance covering their areas.

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. Only 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 2023 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 mid-term reviews are planned, significant effort is expended on the ex ante evaluation and continuous monitoring of projects through the weekly 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 is 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.

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.

On the basis of ENISA's strategy, adopted in 2020, Executive Director Decision No EDD/35/2020 on the internal structures was adopted, setting out in detail the mission statements of all units and teams (it was reviewed and updated by newly adopted Executive Director Decisions Nos EDD/3/2022 and EDD/24/2023 to reflect the latest organisation structure and consequent changes to mission statements). In addition, 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 management board. Throughout the year, the agency's outputs are planned, reviewed and finalised in close consultation with stakeholders, including ENISA's management board, the advisory group and the NLO Network. ENISA uses its objectives as a basis for allocating resources to achieve policy, operational and financial performance goals.

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

The assessment concluded that this principle is present and functioning well, but improvement is needed in the implementation of mitigating measures against high risks within the target deadline.

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 European 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.

Nevertheless, the top risks for the agency identified in 2023 were as follows:

- Dependence on external providers (systems, services, people),
- Lack of resources and talent / insufficient hr management,
- Lack of a comprehensive it strategy implementation across the agency (risk level reduced from 2022 because a new it governance scheme was adopted at the end of 2023).

The results of 2023 the risk assessment were presented to and endorsed by the ENISA management team in early 2024 and form the basis of a comprehensive action plan to mitigate all identified main high risks.

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 and that the only improvement needed is to increase the rate of participation in anti-fraud training.

The agency's anti-fraud strategy was updated in 2021 and formally adopted by Management Board Decision No B/2021/5. A dedicated web page was created on ENISA's intranet. Here all staff can access all relevant regulations, documents and training material and a toolbox. 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 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.

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, although further development of the agency's business continuity plan is needed.

Since the implementation, in 2023, of a single monitoring table to monitor identified weaknesses, the assessment of the functioning of the internal control principles has been used as an activity supervision tool.

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

The assessment concluded that this principle is partially present and functioning; however, during 2023, concrete steps were taken to improve the efficiency of IT management and the agency's IT governance approach. While a number of identified high risks were addressed, further work is needed to fully address weaknesses in this area until the new IT governance framework, scheduled for 2025, is implemented.

That being said, the performance of the corporate IT systems during 2023 was assessed as high (99 %) on the basis of specific indicators adopted by the IT Management Committee.

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. For example, recurrent weaknesses identified by internal control tools (such as the registry of exceptions) in recent years have not yet been effectively addressed and ENISA's internal policies and procedures are not always adequately documented or communicated to staff.

However, out of 24 non-compliant events (i.e. exceptions) identified and registered in 2023, none was assessed as high risk (17 were assessed as low risk and seven as medium risk) and 13 exceptions were deemed too be of material relevance.

The majority of exceptions (18) concerned a posteriori transactions (i.e. the budgetary or legal commitments were not compliant to proceed forward with the transaction). Three exceptions were associated with the contracting of an expert at a cost above the limit of EUR 15 000. It is important to note that third-party experts in niche areas in high demand come at a cost that may exceed the thresholds set by ENISA. This threshold will therefore be reassessed in 2024 to ensure that the operational need for external expertise is adequately addressed.

It is also worth mentioning that ENISA's management board decided in July 2023 to temporarily derogate from the applicable financial rules to provide greater flexibility in the disbursement of ENISA's additional budgetary resources of EUR 15 million, granted in 2022 to enable ENISA to meet the request from MSs to scale up its support for ex post and ex ante services in the context of the emergency situation due to possible spillover effects resulting from the Russian war of aggression against Ukraine.

This derogation exceptionally allowed the agency to change the recipient of an individual commitment for the provision of ex post and ex ante cybersecurity services and was intended to better address the needs of individual MSs. Of EUR 15 million committed in 2022, EUR 1.82 million was reallocated to a different recipient in 2023 using this derogation.

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, but some improvements are needed. For example, internal information sharing and the mapping of information could be improved and the need-to-know principle (to access internal information) needs further monitoring.

Principle 14 – ENISA communicates internally information, 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 2023. Mid-term 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 presentations 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. 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.

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 and risks identified in ex ante and ex post controls and other financial evaluation.

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 in the coming years, as the single monitoring table of weaknesses identified was implemented only in Q3 2023.

3.2 Conclusions of assessment of internal control systems

The overall assessment shows that the internal controls at ENISA provide reasonable assurance that the agency's policies, processes, tasks and behaviours, 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, there is room for improvements in some areas, in order to increase effectiveness and ensure proper implementation of the internal controls in the future. Progress in making these improvements will be assessed as part of the agency's next mid-term review.

3.3 Statement of the internal control coordinator in charge of risk management and internal control

I, the undersigned,

Alexandre-Kim Hugé

in my capacity as Internal Control Coordinator, in charge of risk management and internal control, declare that, in accordance with the 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, 28th June 2024

Alexandre-Kim Hugé
Internal Control Coordinator

IV

PART IV
MANAGEMENT ASSURANCE

4.1 Review of the elements supporting assurance

4.2 Reservations

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 (the eca, complemented by a private audit firm), internal auditors (the 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.

Considering the results of the 2023 annual audits performed by the ECA and the IAS, the 2023 results of the internal controls (ex post controls, review of the register of exceptions, the internal controls framework assessment) and the 2023 results of the key financial and operational indicators, the authorising officer can conclude that ENISA operated in 2023 in such a way as to manage appropriately 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.

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 (61) 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,

Qualified electronic signature by:
JUHAN LEPASSAAR
Date: 2024-06-28 18:14:06 +02:00

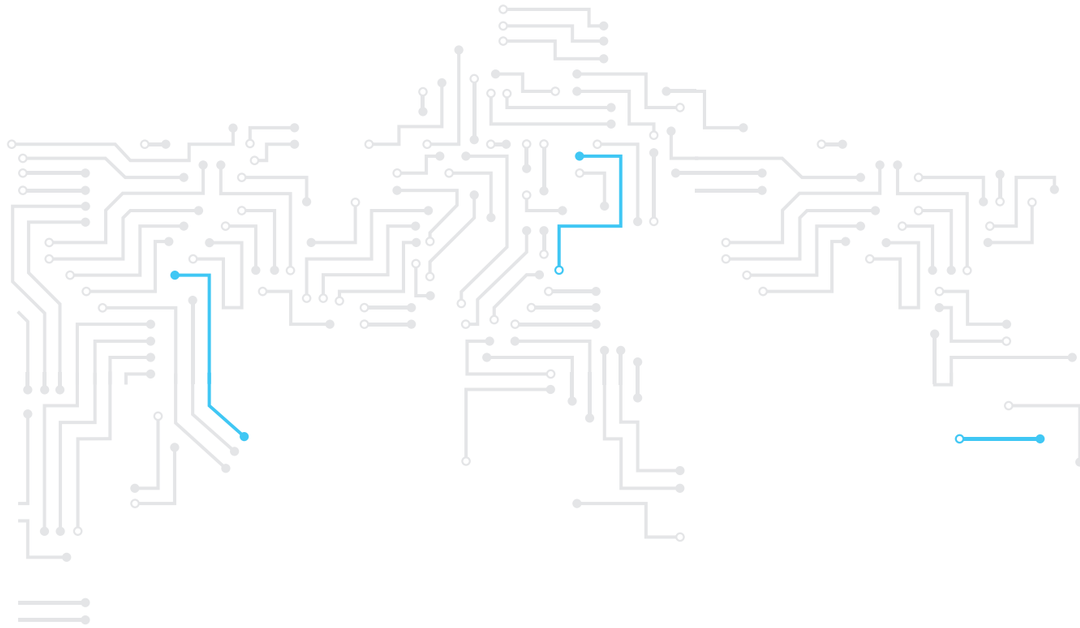
Juhan LEPASSAAR
Executive Director

(61) True and fair in this context means reliable, complete and accurate.

A

ANNEX

CORE BUSINESS STATISTICS



Activity 1:
Providing assistance on policy development

Key performance indicator ENISA's added value to EU institutions, bodies and MSs in providing support for policymaking (*ex ante*)	Unit (of measure-ment)	Frequency	Data source	2022 results	2023 results/ target
1.4. Number of relevant contributions to EU and national policies and legislative initiatives (62)	Number	Annual	Manual collection from staff members	314	172/215
Contributions to task forces and bodies	%	Annual	Manual collection from staff members	9 % of 314 total contri-butions	17 % of 172 total contri-butions
Contributions to workshops and conferences	%	Annual	Manual collection from staff members	87 % of 314 total contri-butions	77 % of 172 total contri-butions
Support actions/contributions to Commission and MS for policies and legal initiatives following relevant requests	%	Annual	Manual collection from staff members	4 % of 314 total contri-butions	6 % of 172 total contri-butions
1.5. Number of references to ENISA reports, analysis and/or studies in EU policy documents		Biennial		New value: 16 (up from 10)	13/NA
1.6. Satisfaction with ENISA added value of contributions	%	Biennial	Survey	93 %	NA
% of stakeholders rating the outcome/ results of ENISA's work as providing high or some added value	%	Biennial	Survey	92 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	92 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	90 %	NA
% of stakeholders satisfied with the way ENISA organises and managed processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	95 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	91 %	NA
1.4. Number of EU policy files under development and supported by ENISA	Number	Annual	Report	NA	6

(62) This KPI should be viewed as a reflection of performance over a number of years and not just in 2021

Activity 2:
Supporting implementation of EU policy and law

Key performance indicator Contribution to policy implementation and implementation monitoring at the EU and national levels (*ex post*)	Unit (of measure-ment)	Frequen-cy	Data source	2022 results	2023 results/ target
2.4. Number of EU policies and regulations implemented at the national level supported by ENISA	Number	Annual	Manual collection from staff members	5	6/5
2.5. Number of ENISA reports, analyses and/ or studies referred to at the EU and national levels		Biennial	Survey	65	NA
2.6. Satisfaction with ENISA added value of support	%	Biennial	Survey	94 %	NA
% of stakeholders rating the outcome/ results of ENISA's work as providing high or some added value	%	Biennial	Survey	93 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	87 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	90 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	97 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	93 %	NA
2.4. Number of critical sectors with a high level of cybersecurity maturity (NIS sector 360)	Number	Annual	Internal analysis (NIS sector 360)	NA	6/NA

Activity 3:
Building capacity

Key performance indicator Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	Unit (of measurement)	Frequency	Data source	2022 results	2023 results/ target
3.1. Increase/decrease in maturity indicators (63)					
Maturity of national cybersecurity strategies					
MSs' rating of the overall maturity of their cybersecurity strategy					
High maturity	Number	Annual	Survey	6	7/5
Medium maturity	Number	Annual	Survey	5	3/5
Low maturity	Number	Annual	Survey	0	4/0
Number of MSs planning to use the ENISA framework to measure the maturity of their national cybersecurity capabilities					
Already using	Number	Annual	Survey	2	1/3
Not using but planning to use	Number	Annual	Survey	9	7/7
Don't know or will not use in the foreseeable future	Number	Annual	Survey	2	3/4
Number of MSs that have set KPIs to measure the progress and effectiveness of the implementation of their strategic objectives when drafting their NCSSs					
Already using	Number	Annual	Survey	9	7/5
Not set but planning to use	Number	Annual	Survey	5	3/5
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	0	0/3
Frequency with which MSs update their strategy to adapt to technological advancements and new threats.					
Every 2–3 years	Number	Annual	Survey	1	1/3
Every 4–5 years	Number	Annual	Survey	12	7/8
More than 6 years or don't know	Number	Annual	Survey	1	3/2
Sectorial ISACs coverage					
Percentage of NIS 2 sectors having an EU ISAC	%	Annual	Report	60 %	60 %
3.2. Outreach, uptake and application of lessons learned from capability-building activities					
Cysopex (number of improvements proposed by participants)	Number	Per exercise		5	5/3
3.3. The number of exercises executed annually					
Number of exercises executed annually	Number	Annual	Report	5	7/5
3.4. Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity building activities					
% of stakeholders rating the outcome/ results of ENISA's work as providing high or some added value	%	Biennial	Survey	97 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	77 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	80 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	96 %	NA
% of stakeholders satisfied with ENISA's community- building actions	%	Biennial	Survey	97 %	NA
SOPEX series (Cybersopex, Cysopex, Blue OLEX)					
Usefulness low	%	Per exercise	Survey	6 %	0 %
Usefulness medium	%	Per exercise	Survey	54 %	25.56 %
Usefulness high	%	Per exercise	Survey	40 %	74.44 %
Relevance low	%	Per exercise	Survey	7 %	5.93 %
Relevance medium	%	Per exercise	Survey	53 %	31.11 %
Relevance high	%	Per exercise	Survey	40 %	62.96 %
Cyber Europe exercise series (biannual)					
Usefulness low	%	Per exercise	Survey	6 %	NA
Usefulness medium	%	Per exercise	Survey	54 %	NA
Usefulness high	%	Per exercise	Survey	40 %	NA
Relevance low	%	Per exercise	Survey	7 %	NA
Relevance medium	%	Per exercise	Survey	53 %	NA
Relevance high	%	Per exercise	Survey	40 %	NA
Jasper series					
Data to be made available as from 2023	%	Per exercise	Survey	NA	NA (64)
Usefulness low	%	Per exercise	Survey	NA	0 %
Usefulness medium	%	Per exercise	Survey	NA	41.5 %
Usefulness high	%	Per exercise	Survey	NA	58.95 %
Relevance low	%	Per exercise	Survey	NA	0 %
Relevance medium	%	Per exercise	Survey	NA	30.77 %
Relevance high	%	Per exercise	Survey	NA	69.23 %
3.5. SACs maturity					
Number of exercises organised by EU ISACs	% (65)	Report		NA	
Number of training events organised by EU ISACs	%	Report		NA	2

(63) This KPI should be viewed as a reflection of performance over a number of years and not just in 2021. The 2021 KPI establishes the 'baseline' that allows us to gauge the evolution of the maturity indicator over the next years.

(64) Pilot implementation; indicators not relevant for tracking.
(65) The percentage out of a total of 10 EU ISACs (as per NIS and NIS 2).

Activity 4:
Enabling operational cooperation

Key performance indicator Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation	Unit (of measurement)	Frequency	Data source	2022 results	2023 results/ target
4.1. Number of users, both new and recurring, and usage per platform/tool/SOP provided by ENISA					
CSIRTs Network (% increase year on year)					
Active users (% increase year on year)	%	Annual	Platform	19 %	114 %/110 %
Number of exchanges/interactions year on year	%	Annual	Platform	104 %	134 %/110 %
EU-Cyclone					
Active users (% increase year on year)	%	Annual	Platform	2 %	109 %/100 %
Number of exchanges/interactions (% increase year on year)	%	Annual	Platform	548 %	218 %/100 %
4.2. Uptake of platforms/tools/SOPs during massive cyber incidents		Ad hoc	Platform	NA	NA (66)
4.3. Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs provided by ENISA	%	Biennial	Survey	89 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	94 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	84 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	83 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	94 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	87 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	94 %	NA

(66) Although the networks were in escalated mode. this situation was not deemed a large-scale cybersecurity incident as defined by the NIS 2 Article 6(7).

Activity 5:
Contribute to cooperative response at the EU and MS levels

Key performance indicator ENISA's ability to support the response to massive cyber incidents	Unit (of measurement)	Frequency	Data source	2022 results	2023 results/ target (67)
5.1. Number of relevant incident responses to which ENISA contributed, as per CSA Article 7 (68)	Number	Annual	Internal data source	NA	NA (see indicator 5.2)
5.2. Number of incidents analysed/curated	Number	Annual	Internal data source	775	4 858 (69)
5.3. Number of high-visibility incidents analysed	Number	Annual	Internal data source	38	63
5.4. Number of large-scale cross- border incident with high impact analysed	Number	Annual	Internal data source	13	14
5.5. Number of incident responses to which ENISA contributed			Cyber Assistance Mechanism	1	Incident response retainer in place in 16 MSs, Within Support Action contributed to eight incidents
5.6. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents and which contributes to mitigation work		Biennial	Survey	Post-poned (70)	NA
5.7. Take-up of ENISA support services	Number	Annual	Report	NA	26 (71)
5.8. Number of trusted vendors	Number	Annual	Report	NA	6
5.9. Stakeholder satisfaction with ENISA's ability to provide operational support	%	Biennial	Survey	84 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	82 %	NA

(67) Targets were to be established once baseline results were recorded, which occurred after adopting the 2023-–2025 SPD.
(68) Indicator has been superseded by indicator 5.2.
(69) As of November 2022 for the year 2023.
(70) The survey was postponed because resources were reallocated to the Cybersecurity Support Action
(71) All but one MS used at least one of the services offered under the Cybersecurity Support Action

% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	73 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	86 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	82 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	82 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	100 %	NA
% of stakeholders rating the outcome/results of ENISA's work as high or some added value	%	Biennial	Survey	82 %	NA

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

Key performance indicators Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions Effective preparation of candidate certification schemes prepared by ENISA	**Unit (of measurement)**	**Frequency**	**Data source**	**2022 results**	**2023 results/ target**
Metrics					
6.1. Number of stakeholders (public authorities and/or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions	%	Annual	Survey	86 %	91 %/50 %
Submetrics					
Percentage of respondents using (planning to use) the cybersecurity schemes to have solutions certified	%	Annual	Survey	29 %	16 %/NA
Percentage of respondents using (planning to use) the cybersecurity schemes to use certified solutions	%	Annual	Survey	32 %	25 %/NA
Percentage of respondents using (planning to use) the cybersecurity schemes to certify solutions	%	Annual	Survey	44 %	44 %/NA
Percentage of respondents referring (planning to refer) to certifications within regulations	%	Annual	Survey	44 %	37.5 %/NA
Percentage of respondents planning to use the EUCC	%	Annual	Survey	57 %	78 %/NA
Percentage of respondents planning to use the EUCS	%	Annual	Survey	52 %	47 %/NA
Percentage of respondents planning to use the EU5G	%	Annual	Survey	NA	56.25 %/NA
Percentage of respondents that need ENISA's assistance to prepare for using the EU certification schemes	%	Annual	Survey	76 %	68.7 %/NA
6.2. Stakeholders' trust in digital solutions for certification schemes (citizens, public sector and businesses	%	Biennial	Survey	74 %	NA
6.3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework	%	Biennial	Survey	73 %	NA
6.4. Number of candidate certification schemes prepared by ENISA	Number	Annual	Numerical	3 in different stages of adoption	3/2.25 (Minimum 75 % of schemes formally requested to be under ongoing development)
6.5. Number of people/organisations engaged in the preparation of certification schemes	Number	Annual	Numerical	Approximately 150	150 / minimum of 10 organisations and 10 individual experts; 50 % of MSs to join an AHWG; 30 % of organisations to be an SME; 5 % to be from a non-EU country
6.6. Satisfaction with ENISA's support for the preparation of candidate schemes	%	Biennial	Survey	82 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	75 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	88 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	75 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	75 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	83 %	NA
% of stakeholders satisfied with ENISA's community- building actions	%	Biennial	Survey	93 %	NA

Activity 7:
Supporting the European cybersecurity market and industry

Key performance indicator Effectiveness of ENISA's supporting role for participants in the European cybersecurity market	Unit (of measure-ment)	Frequency	Data source	2023 results	2024 results/ target
7.1. Number of market analyses, guidelines and good practices issued by ENISA	Number	Annual	Reports	2	6 (72)/1
7.2. Uptake of lessons learned / recommendations from ENISA reports	%	Annual	Survey	49 %	61 %/60 %
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work	%	Biennial	Survey	88 %	NA
% of stakeholders rating the outcome/ results of ENISA's work as providing high or some added value	%	Biennial	Survey	88 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	84 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	72 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	100 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	93 %	NA
% of stakeholders satisfied with ENISA's community- building actions	%	Biennial	Survey	94 %	NA

(72) One internal guideline on vulnerability handling; one internal report on OSS; one report on mapping of standards to CRA requirements (publication depending on COM); one report on supply chain security standards (pending finalisation ; publication expected Q1 2024); one internal report on the methodology for the assessment of standardisation activities; and one report planned and delivered on market analysis on cryptography products and services in progress (finalisation in progress' publication expected Q1 2024).

Activity 8:
Knowledge on emerging cybersecurity challenges and opportunities

Key performance indicator ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge including into research and innovation agenda	Unit (of measure-ment)	Frequency	Data source	2022 results	2023 results/ target
8.1. Number of users and frequency of use of a dedicated portal (observatory) (73)					
8.2. Total number of recommendations, analyses and challenges identified and analysed	Number	Annual	ENISA reports and studies	357	389/300
8.3. The influence of foresight on the development of ENISA's work programme	Number	Annual	SPD	NA	3 (AI, sup-ply chain, space infra-structure)
8.4. Uptake of reports generated in activity 8	Number	Annual	Media monitoring report	NA	102 media mentions 74 761 downloads
8.5. Uptake of the EU CSI	Number	Annual	Index platform	NA	24/27 MSs actively using the index platform
8.6. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research	%	Biennial	Survey	91.5 %	NA
% of stakeholders rating the outcome/ results of ENISA's work as providing high or some added value	%	Biennial	Survey	94 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	90 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	86 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	94 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	94 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	91 %	NA

(73) The infohub has not been implemented.

Activity 9:
Outreach and education

Key performance indicators Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU	Unit (of measure-ment)	Fre-quency	Data source	2022 results	2023 results/ target
Level of outreach					
9.1. Number of cybersecurity incidents reported having human error as a root cause	Number	Annual	CIRAS tool	153	147/NA
9.2. Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics					
Total social media impressions	Number	Annual	ENISA analytics	27 278 49 1	946 100/20 000 000
Total social media engagement	Number	Annual	ENISA analytics	19 301	57 000/150 000
Total video views	Number	Annual	ENISA analytics	6 602 355	0/3 000 000
Total website visits	Number	Annual	ENISA analytics	300 530	603 459/150 00 0
Total participation at events	Number	Annual	ENISA analytics	40	40/10
CyberAll (formerly Women4Cyber campaign)					
Social media impressions	Number	Annual	Social media (Face-book, LinkedIn, X (former-ly Twitter))	82 900	115 800
Social media engagement	Number	Annual	Social media (Face-book, LinkedIn, X (former-ly Twitter))	1 286	2 300
Video views	Number	Annual	YouTube	2 285	NA
Cybersecurity for SMEs campaign					
Social media impressions	Number	Annual	Social media (Face-book, LinkedIn, X (former-ly Twitter))	35 900	63 900
Social media engagement	Number	Annual	Social media (Face-book, LinkedIn, X (former-ly Twitter))	1 200	1 800
Video views	Number	Annual	YouTube	6 113	NA
website	Number	Annual	ENISA website	55 082	115 313 page views
References	Number	Annual	Media monitor-ing	NA	214
Participation in events	Number	Annual	Website announ-ceme nts	6	10
Campaign on health					
Social media impressions	Number	Annual	ENISA analytics	58 200	96 900
Social media engagement	Number	Annual	ENISA analytics	1 100	1 800
Video views	Number	Annual	ENISA analytics	197	NA
Website	Number	Annual	ENISA analytics	1 008	51 104 page views
Campaign on gas					
Social media impressions	Number	Annual	ENISA analytics	NA	80 800
Social media engagement	Number	Annual	ENISA analytics	NA	1 100
Video views	Number	Annual	ENISA analytics	NA	NA
Website	Number	Annual	ENISA analytics	NA	5 031 page views
Campaign on energy					
Social media impressions	Number	Annual	ENISA analytics	56 900	53 300
Social media engagement	Number	annual	ENISA analytics	703	1 800
Video views	Number	Annual	ENISA analytics	224	NA
Website	Number	Annual	ENISA analytics	586	51 307 page views
Campaign on rail					
Social media impressions	Number	Annual	ENISA analytics	NA	128 400
Social media engagement	Number	Annual	ENISA analytics	NA	2 200
Video views	Number	Annual	ENISA analytics	NA	NA
Website	Number	Annual	ENISA analytics	NA	4 755 page views
ECSM campaign					
Social media impressions	Number	Annual	ENISA analytics	26 823 59 1	202 600
Social media engagement	Number	Annual	ENISA analytics	9 000	34 300
Video views	Number	Annual	ENISA analytics	6 589 457	NA
Website	Number	Annual	ENISA analytics	179 571	132 368 page views

Certification campaign					
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter))	200 000	204 400
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, X (formerly Twitter))	5 900	11 700
Video views	Number	Annual	YouTube	4 500	NA
Website	Number	Annual	ENISA website	NA	148 435 page views
AR-in-a-box metrics					
Downloads	Number	Annual	ENISA analytics	31 000	43 245/> 30 000
Requests for collaborations	Number	Annual	ENISA analytics	20	20/20
'Train-the-trainer' sessions	Number	Annual	ENISA analytics	15	20/15
Presentations in events	Number	Annual	ENISA analytics	15	20/20
Cyberhead metrics					
Social media impressions	Number	Annual	Social media	21 000	NA
Social media engagement	Number	Annual	Social media	112	NA
Website	Number	Annual	ENISA website	64 283	95 146 page views
9.3. Number of cybersecurity programmes (courses) and participation rates					
Total number of students enrolled in the first year of the academic programmes	Number	Annual	Report (74)	6 000	6 612/6 000
Number of male students	%	Annual	Report	70 %	80 %/70 %
Number of female students	%	Annual	Report	30 %	20 %/30 %
Total number of cybersecurity programmes	Number	Annual	Report	130	141/130
Number of postgraduate programmes	%	Annual	Report	5 %	6 %/5 %
Number of master's programmes	%	Annual	Report	80 %	76 %/80 %
9.4. Geographical and community coverage of outreach in the EU	Number	Annual	ENISA analytics	All 27 MSs and EFTA countries	All 27 MSs and EFTA countries
9.5. Level of awareness of cybersecurity across the EU / general public (e.g. EU Barometer and other) (75)		Biennial		NA	NA
9.6. Stakeholder satisfaction with awareness-raising and education activities	%	Biennial	Survey	91 %	NA
% of stakeholders rating the outcome/results of ENISA's work as providing high or some added value	%	Biennial	Survey	100 %	NA
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates MSs' activities	%	Biennial	Survey	80 %	NA
% of stakeholders likely to take up immediately, or in the medium term, the results of ENISA's work	%	Biennial	Survey	84 %	NA
% of stakeholders satisfied with the way ENISA organises and manages processes for planning and implementing work	%	Biennial	Survey	95 %	NA
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	86 %	NA
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	98 %	NA

(74) https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

(75) It has been proposed that this KPI be updated to reflect the requirements of NIS 2 Article 18(1) in the draft 2024–2026 SPD.

Activity 11:
Performance and risk management

Key performance indicators Organisational performance culture Trust in ENISA brand	Unit (of measurement)	Fre-quency	Data source	2022 results	2023 results/ target
11.1. Proportion of KPIs reaching targets	Number	Annual	Annual activity report	Targets established as of 2023; however, compared with the base year (2021), 13 metrics were unchanged, 21 underperform ed and 58 overperforme d	69 %/65 %
11.2. Individual staff contribution to achieving the objectives of the agency via clear link to KPIs in staff career development report (all units aggregated)	%	Annual	Staff survey	64 %	86 % (76)/85 %
11.3. Exceptions in the risk register	Number	Annual	Internal control	27	23/11
Deviation from financial regulations	Number	Annual	Internal control	26	23/10
Deviation from staff regulations	Number	Annual	Internal control	1	0/1
11.4. Number of complaints filed against ENISA, including number of enquiries/ complaints to the EU Ombudsman	Number	Annual		3	2/12
To European Ombudsman	Number	Annual	ENISA functional mailbox	0 (77)	1
As Article 90	Number	Annual	Internal control files	3	1
As Article 24	Number	Annual	Internal control files	0	0
To the EDPS	Number	Annual	Internal control files	0	0
11.5. Number of complaints addressed on time and in accordance with the relevant procedures	Number	Annual	Internal files	3 (Article 90(2) and complaints to the EU Ombudsman successfully closed on time and in accordance with the relevant procedures	2/NA
11.6. Number of high risks identified in annual risk assessment exercise	Number	Annual	Internal control files		4/NA
11.7. Implementation of risk treatment plans	Number	Annual	Internal control files		In progress
11.8. Number and types of activities at each engagement level (78)	Number	Annual	Report		Total activities: 149 Partner level: 36 % Consult level: 19 % Engage level: 22 % Inform level: 23 %
11.9. Observations from external audit bodies (e.g. the ECA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings and number of observations successfully completed and closed)	Number	Annual	Report	2	1/2
10.8. Level of trust in ENISA (79)	%	Biennial	Survey	95 %	NA

(76) Based on responses to a question in the 2023 staff satisfaction survey question asking staff if they 'understand how their job contributes to ENISA's strategic priorities and goals'.

(77) Complaints submitted in late 2021 were closed in Q3 2022.

(78) Stakeholder management at the agency is decentralised and handled at activity level. Each activity in the SPD focuses on the needs of a specific group of stakeholders in the cybersecurity ecosystem. The relevant stakeholders are identified, and the desired level of engagement is determined. At the closure of a project, stakeholder management is implemented and stakeholder feedback is elicited. Subsequently, KPIs are reported at the activity and output levels.

(79) Based on the proportion of respondents to the stakeholder satisfaction survey who said that they 'agree' or somewhat agree' with the statement 'I am confident in ENISA's ability to achieve its mandate'

Activity 12:
Staff development and working environment

Key performance indicator Staff commitment, motivation and satisfaction	Unit (of measure-ment)	Frequency	Data source	2022 results	2023 results/ target
12.1. Staff satisfaction survey (including the attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools)	%	Annual	Staff satisfaction survey		64 %/75 %
Percentage of staff who would recommend ENISA as an employer	%	Annual	Staff satisfaction survey	NA	74 %
Percentage of staff who have enough authority to do their job	%	Annual	Staff satisfaction survey	NA	68 %
Percentage of staff have opportunities to have their ideas adopted and put into use	%	Annual	Staff satisfaction survey	NA	64 %
Percentage of staff who feel encouraged to come up with new or better ways of doing things	%	Annual	Staff satisfaction survey	NA	61 %
Percentage of staff who are asked for their opinion on decisions that affect their daily work and tasks at ENISA	%	Annual	Staff satisfaction survey	NA	56 %
Percentage of staff who are satisfied with their work	%	Annual	Staff satisfaction survey	76 %	76 %
Percentage of staff indicating that their line manager provides sufficient feedback on their performance	%	Annual	Staff satisfaction survey	60 %	64 %
Percentage of staff who feel well informed by ENISA's leadership regarding important matters	%	Annual	Staff satisfaction survey	36 %	46 %
12.2. Quality of ENISA training and career development activities organised for staff	%	Annual	Staff satisfaction survey	48 %	58 %/55 %
Percentage of staff indicating that courses match their training and development needs	%	Annual	Staff satisfaction survey	43 %	47 %
Percentage of staff reporting that their line manager dedicates enough time during the career development report dialogue for mapping training and development needs	%	Annual	Staff satisfaction survey	36 %	61 %
Percentage of staff who agree that the learning and development opportunities at ENISA help them to maintain and develop their transferable competencies	%	Annual	Staff satisfaction survey	36 %	44 %
Percentage of staff who know which key competencies they are required to maintain or develop	%	Annual	Staff satisfaction survey	71 %	76 %
Percentage of staff who agree that their learning and development objectives are consistent with the competencies they need for their career	%	Annual	Staff satisfaction survey	55 %	63 %
12.3. Reasons for staff departure (exit interviews) (80)	Scale 1–10	As required	HR files	7.9	7.9/7.5
12.4. Turnover rates	%	Annual	HR files	4 %	4.9 %/3 %
12.5. Establishment plan posts filled	%	Annual	HR files	89 %	98 %/95 %
12.6. Resilience and quality of ENISA's IT systems and services	%	Annual	IT reports and staff satisfaction survey	73 %	96.66 %/80 %
Critical systems downtime	%	Annual	Uptime report for Fortimail / SolarWinds (2023)	100 %	99.97 %
Percentage of central IT infrastructure assessments with few (<5) critical findings	%	According to needs	Intranet repository	100 %	NA (81)
Percentage of central infrastructure patched to the last formal versioning of 1 year	%	Annual	Yearly IT maintenance plan in PDF format	97.33 %	99.90 %
Percentage of major IT helpdesk requests resolved in a satisfactory way within 2 business days	%	Annual	IT ticket repository	79.28 %	90.00 %
12.7. Percentage of procurement procedures launched via e- tool (PPMT)	%	Annual	Procurement files	NA	100 %/> 90 %
12.8. Percentage of payments made within 30 days	%	Annual	Finance files	NA	90 %/> 90 %
12.9. Late payments	%	Annual	Finance files	NA	9 %/< 10 %

(80) Standardised set of 10 questions, with answers on a scale of 1 to 10, that provide an opportunity for ENISA to seek feedback about a staff member's experience. The greater the number, the better the experience.

(81) Assessments are conducting according to needs of the agency, no changes occurred in 2023.

ANNEX II

STATISTICS ON FINANCIAL MANAGEMENT

Budget out-turn and cancellation of appropriations (EUR)

Budget out-turn	2021	2022	2023
Reserve from the previous years' surplus (+)			
Revenue actually received (+)	23 058 211	39 227 392	25 293 934
Payments made (–)	– 17 989 374	– 20 396 780	– 21 118 392
Carryover of appropriations (–)	– 5 082 548	– 18 836 095	– 4 228 452
Cancellation of appropriations carried over (+)	209 385	248 745	149 739
Adjustment for carry-over of assigned revenue appropriation from previous year (+)	125 622	33 743	53 469
Exchange rate differences (+/–)	– 428	– 17	
Adjustment for negative balance from previous year (–)			
TOTAL	**320 868**	**276 988**	**150 298**

Execution of commitment appropriations in 2023

In 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 (including fund source R0).

Execution of payment appropriations in 2023

In EUR	Chapter	Payment appropriations authorised *	Payments made	% Payment rate
A-11	Staff in Active Employment	11 023 274	11 012 691	99.90%
A-12	Recruitment/ Departure Expenditure	265 321	246 710	92.99%
A-13	Socio-Medical Services and Training	1 034 063	710 813	68.74%
A-14	Temporary Assistance	371 000	258 818	69.76%
	TITLE I	12.693.659	12.229.033	96.34%
A-20	Buildings and Associated Costs	1 188 215	815 578	68.64%
A-22	Current Administrative Expenditure	465 252	236 691	50.87%
A-23	ICT	2.095.952	1 309 713	62.49%
	TITLE II	3 749 419	2.361 982	63.00%
B-30	Activities Related to Outreach and Meetings	506 134	399 355	78.90%
B-37	CSA Core Operational Activities	8 398 192	6.128 023	72.97%
	TITLE III	8 904 326	6 527 378	73.31%
	Total	25 347 404	21 118 393	83.32%

(*) 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 (including fund source R0).

Carry-forward to 2024 (amounts open as of 31 December 2023)

In EUR	Chapter	Commitments made	Payments made	Amount to be paid in 2024 *	% Amount to be paid
A-11	Staff in active employment	11 023 274	11 012 691	10 583	0.10%
A-12	Recruitment/ departure expenditure	265 321	246 710	18 611	7.01%
A-13	Socio-medical services and training	1 033 886	710 813	323 072	31.25%
A-14	Temporary assistance	371 000	258 818	112 182	30.24%
	TITLE I	12 693 482	12 229 033	464.449	3.66%
A-20	Buildings and associated costs	1 171 715	815 578	356 137	30.39%
A-22	Current administrative expenditure	453 839	236 691	217 148	47.85%
A-23	Information and communication technologies	2 074 447	1 309 713	764 734	36.86%
	TITLE II	3 700 001	2 361 982	1 338 019	36.16%
B-30	Activities related to outreach and meetings	490 669	399 355	91 314	18.61%
B-36	CSA Core operational activities	8 358 389	6 128 023	2 230 365	26.68%
	TITLE III	8 849 058	6 527 378	2 321 680	26.24%
	Total	**25 242 541**	**21 118 393**	**4 124 148**	**16.34%**

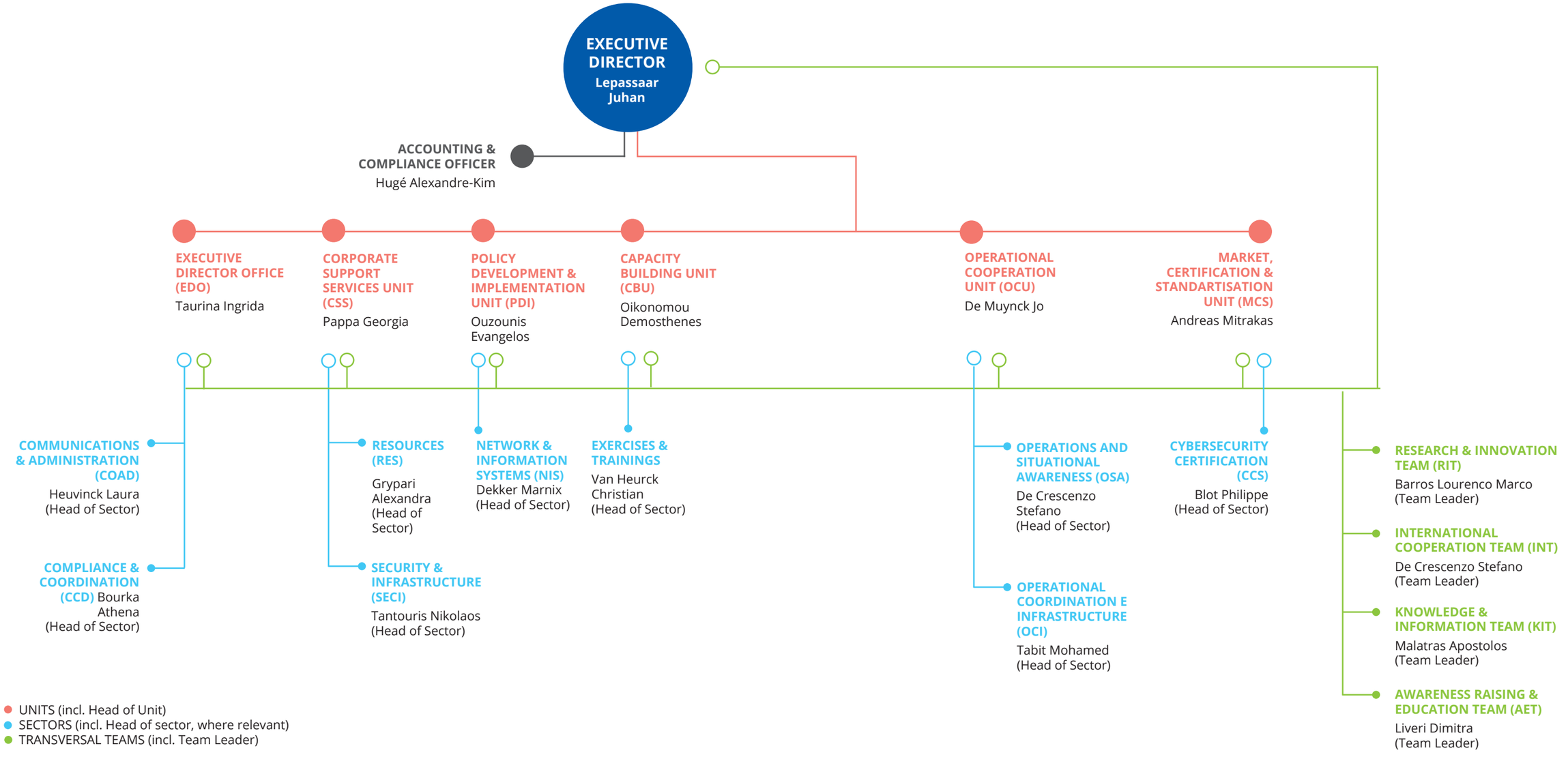
(*) Includes automatic carry-over for fund source R0 for the total of EUR 163 909.

Revenue and income during 2023 (EUR)

Type of revenue	Entitlements established	Revenue received	Outstanding at the end of the year
Subsidy from the EU Budget	25.183.495,00	24.906.506,00	276.989
Subsidy from Hellenic Authorities	-	-	-
Revenue from Administrative Operations	110.439,84	110.439,84	-
Total	**25.293.935**	**25.016.946**	**276.989**

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.

ANNEX III
ORGANISATION CHART



ANNEX IV

2023 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT

2023 establishment plan

Function group and grade	Establishment plan in 2023 voted EU budget (82)		Positions filled as of 31 December 2023	
	Officials	Temporary agents	Officials	Temporary agents
AD 16				
AD 15		1		
AD 14				1
AD 13		2		1
AD 12		4		3
AD 11		2		2
AD 10		4		3
AD 9		11		13
AD 8		25		10
AD 7		10		13
AD 6		4		16
AD5				
Total number of ADs		63		62 (83)
AST 11				
AST 10				
AST 9				
AST 8		2		3
AST 7		4		0
AST 6		7		6
AST 5		5		4
AST 4		1		3
AST 3				1
AST 2				1
AST 1				
Total number of ASTs		19		18
AST/SC 6				
AST/SC 5				
AST/SC 4				
AST/SC 3				
AST/SC 2				
AST/SC 1				
TOTAL		82		80

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

(82) The 2023 establishment plan was modified by Management Board Decision No MB/2023/11 of 24 November 2023 to add one AST 8 post (applying the flexibility rule set out in Article 38(1) of the framework financial regulation).

(83) ENISA considers that it has reached full implementation of its establishment plan, as an offer for one open post (AD 12) was accepted in December 2023 and it has been confirmed that the new member of staff will start in early 2024.

Information on entry level for each type of post

Job title	Type of contract	Function group / grade	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	Operations
Officer	Contract agent	FG IV	Administrative/operations
Assistant	Contract agent	FG III	Administrative/operations
Assistant	Contract agent	FG I	Administrative/operations
Coordinator	Temporary agent	AST 6	Administrative
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

Job title	Type of contract	Function group / grade	Function (administrative support or operations)
Seconded national expert	Seconded national expert	NA	Operations

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

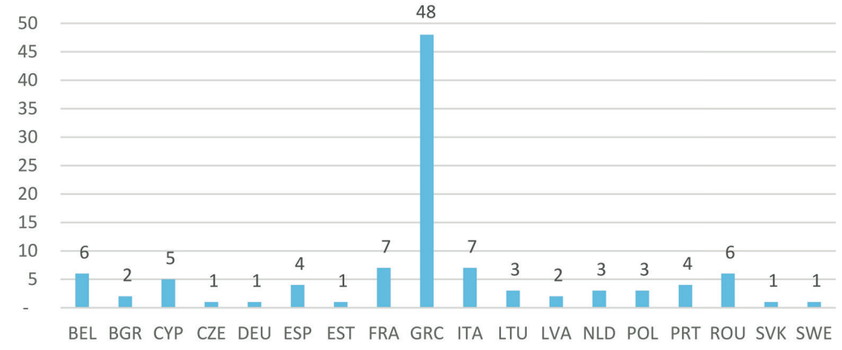
Information on benchmarking exercise

Job type	2021	2022	2023
Total administrative support and coordination	20.34 %	20.97 %	25.76 %
Administrative support	16.95 %	14.19 %	19.05 %
Coordination	3.39 %	6.77 %	6.72 %
Total operational	64.41 %	71.21 %	66.55 %
Total operational coordination	5.93 %	11.05 %	11.27 %
Programme management and implementation	NA	58.39 %	53.64 %
General operational activities	58.47 %	1.77 %	1.64 %
Total neutral	15.25 %	7.82 %	7.69 %
Finance and control	15.25 %	7.42 %	7.31 %
Linguistic activities	NA	0.40 %	0.37 %

Human resources statistics

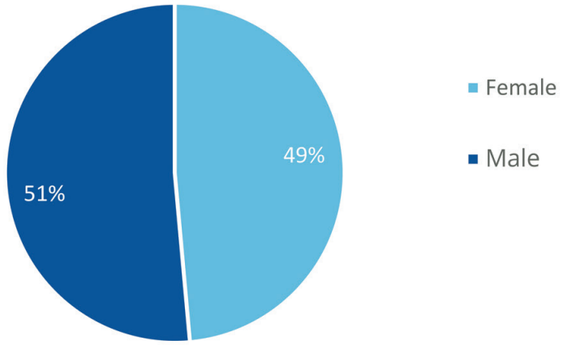
On 31 December 2023, the agency had a total of 105 statutory staff members (temporary agents and contract agents) in house.

Nationalities, statutory staff, as of 31/12/2023

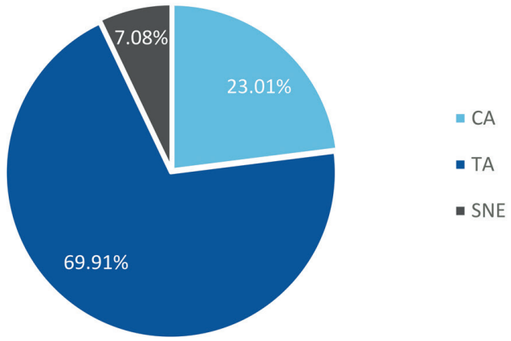


Most represented nationality	2023		2022	
	Number	%	Number	%
Greek	48/105	45.7	41/100	41.0

Gender distribution, statutory staff, as of 31/12/2023



Staff distribution by contract type, as of 31/12/2023



Management	2023		2022	
	Number (84)	%	Number (85)	%
Female managers	3	27	3	27
Male managers	8	73	8	73

(84) Managers are the executive director (1), heads of unit (6), and team leaders (4).
(85) Managers are the executive director (1), heads of unit (6), and team leaders (4).

Implementing rules

MB/2020/10	On procedure for dealing with professional incompetence
MB/2020/13	On laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings

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

Grade	2019 (reference year 2018)	2020 (reference year 2019)	2021 (reference year 2020)	2022 (reference year 2021)	2023 (reference year 2022)	Actual average over 5 years	Average over 5 years according to decision C(2015)9563
AD0 5	—	—	—	—	—	—	2.8
AD 06	3	0	1	1	1	3.5	2.8
AD 07	0	1	0	2	1	4	2.8
AD 08	1	2	1	3	1	3.9	3
AD 09	0	0	0	0	2	6.4	4
AD 10	0	0	0	2	2	10.5	4
AD 11	0	0	0	0	0	0	4
AD 12	0	0	1	0	0	10	6.7
AD 13	0	1	0	10	0	0	6.7
AST 1	-	-	—	—	—	—	3
AST 2	-	-	—	—	—	—	3
AST 3	1	0	0	1	0	5.2	3
AST 4	1	1	0	0	1	3,3	3
AST 5	0	0	1	0	1	5,3	4
AST 6	0	1	1	0	0	3.5	4
AST 7	0	0	1	1	1	4	4
AST 8	—	—	—	—	—	—	4
AST 9	—	—	—	—	—	—	NA
AST 10 (senior assistant)	—	—	—	—	—	—	5

AD, administrator, AST, assistant; NA, not applicable.

Reclassification of contract agents

Contract agents	Grade	Staff members reclassified in 2023 (reference year 2022)	Average number of years in grade of reclassified staff members	Average number of years in grade of reclassified staff members according to decision C(2015)9561
FG IV	17	—	—	Between 7 and 10 years
	16	—	—	Between 5 and 7 years
	15	—	—	Between 4 and 6 years
	14	2	4.5	Between 3 and 5 years
	13	1	5.3	Between 3 and 5 years
FG III	11	—	—	Between 6 and 10 years
	10	—	—	Between 5 and 7 years
	9	—	—	Between 4 and 6 years
	8	—	—	Between 3 and 5 years
FG II	6	—	—	Between 6 and 10 years
	5	—	—	Between 5 and 7 years
	4	—	—	Between 3 and 5 years
FG I	3	—	—	NA
	2	—	—	Between 6 and 10 years
	1	—	—	Between 3 and 5 years

FG, function group; NA, not applicable.

Schooling

Agreement in place with the European School of Heraklion	Type of agreement
Contribution agreements signed with the European Commission on type I European schools	No
Contribution agreements signed with the European Commission on type II European schools	Yes
Number of service contracts in place with international schools	EDD 2021–41 on financial support for the staff of ENISA in relation to the cost of schooling remains in place.

ANNEX V

HUMAN AND FINANCIAL RESOURCES BY ACTIVITY

Human resources by activity

The allocation in 2023 of human and financial resources for the operational and corporate activities described in Part I of this report is presented in the table below. The allocation was determined according to the direct budget and number of FTEs reported for each activity, with the indirect budget being assigned based on drivers such as the number of directly employed 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 of 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 of cost allocation was the number of directly employed FTEs assigned to for each operational activity in 2023.
- For the purpose of the allocation of human and financial resources, the executive director's office activity (activity 11, as described in Part I) (budget and FTEs), which includes coordination, compliance, communication and administration, was allocated to all of the agency's operational activities.
- For the purpose of the allocation of human and financial resources, CSS activity (activity 12, as described in Part I), including human resources, IT services, procurement and finance, facilities and logistics, was allocated for all of the agency's operational activities.

Activities as referred to in PART 1	Budget allocation (in EUR)	FTE allocation
Activity 1	685.149,03	2,49
Activity 2	2.184.963,86	9,90
Activity 3	3.431.079,23	12,03
Activity 4	3.148.642,37	7,73
Activity 5	2.265.238,41	9,55
Activity 6	1.897.832,93	7,71
Activity 7	1.159.070,48	6,08
Activity 8	1.757.071,27	6,84
Activity 9	1.610.449,89	7,93
Activity 10	657.331,70	3,34
Activity 11	2.758.381,07	16,74
Activity 12	3.627.725,20	14,31
	25.182.935,43	104,64

ANNEX VI

GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENT

ENISA does not receive any form of grant.

		Date of signature	Total amount (EUR)	Duration	Counterpart	Short description	FTEs
Service-level agreements							
1	SLA with the ECCC	20 December 2022	54 604	1 year	ECCC	The scope of this SLA covers support services offered by ENISA to the ECCC: data protection officer, accounting officer	0.4
2	SLA with eu-LISA (M-CBU-23-C35)	13 July 2023	120 000	Until 31 December 2023	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	2
Contribution agreements							
1	Cybersecurity support action funds	Draft	20 million (estimate)	Until 31 December 2025	DG 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) penetration tests in key sectors; and (3) the party's contribution to the Cyber Analysis and Situation Centre	13.5 (estimate)

(non-income generated agreement)

SLAs with other EU agencies that were active in 2023 (non-income-generated agreement) are as follows:

- With Cedefop for the purposes of increasing cooperation and sharing services between the two agencies
- With Cedefop for cooperation and synergies
- 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 cooperatio
- 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 eu-LISA for a 2021–2023 cooperation plan,
- 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.

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 European Commission Green Deal initiative, in line with its SPD objectives and the values set by the management board.

In 2021, ENISA's management board included in the agency's 2022–2024 SPD the goal that the agency should achieve climate neutrality (defined as zero CO2, methane and nitrous oxide emissions) across all its operations by 2030.

In 2023, ENISA carried out a technical study to calculate the agency's carbon footprint in 2022. Since 2022 several actions to reduce GHGs emissions reduction have been implemented, such as recycling of office waste, the establishment of a watering system and the incorporation of specific provisions for GHG emissions in the agency's procurement procedures / tenders. In addition, the agency installed solar radiation protection film on external windows to reduce energy bills, increase comfort and more effectively protect staff from UV rays.

The next step, for 2024, is the development of an environmental statement, an external verification and the implementation and registration of an environmental management system (in accordance with the EMAS regulation).

ANNEX VIII
ANNUAL ACCOUNTS

Statement of financial position (EUR)

	31 December 2023	31 December 2022
I. Non-current assets	1 453 737	2 073 836
Intangible fixed assets	0	0
Tangible fixed assets	1 453 737	2 073 836
II. Current assets	1 849 496	4 661 489
Short-term receivables	1 849 496	4 661 489
Cash and cash equivalents	0	0
TOTAL ASSETS (I + II)	3 303 233	6 735 325
III. Non-current liabilities	0	0
Long-term provision for risk and charges	0	0
IV. Current liabilities	1 512 131	1 406 595
Commission pre-financing received	150 298	0
Accounts payable	84 717	74 662
Accrued liabilities	1 277 116	1 331 933
TOTAL LIABILITIES (III + IV)	1 512 131	1 406 595
V. Net assets	1 791 102	5 328 730
Accumulated result	5 328 730	6 347 678
Surplus/(deficit) for the year	– 3 537 628	– 1 018 948
TOTAL LIABILITIES AND NET ASSETS (III + IV + V)	3 303 233	6 735 325

Statement of financial performance (EUR)

	2023	2022
Revenue from the EU subsidy	36 756 208	24 207 625
Revenue from administrative operations	104 840	16 666
Total operating revenue	36 861 048	24 224 291
Administrative expenses	– 18 611 406	– 16 817 269
Staff expenses	*– 12 614 825*	*– 11 354 679*
Fixed asset related expenses	*– 783 056*	*-– 737*
Other administrative expenses	*– 5 213 525*	*– 696 853*
Operational expenses	– 21 786 370	– 8 425 808
Total operating expenses	– 40 397 776	– 25 243 077
Surplus/(deficit) from operating activities	– 3 536 730	– 1 018 786
Financial revenue	0	68
Financial expenses	– 898	– 212
Exchange rate loss	0	– 18
Surplus/(deficit) from non- Operating Activities	– 898	– 162
Surplus/(deficit) from ordinary activities	– 3 537 628	– 1 018 948
Surplus/(deficit) for the year	– **3 537 628**	– 1 018 948

ANNEX IX
ABBREVIATIONS

ABAC	accruals-based accounting
AD	Administrator
AHWG	ad hoc working group
AI	artificial intelligence
AR	augmented reality
AST	Assistant
AST/SC	assistant-secretary
BEREC	Body of European Regulators for Electronic Communications
Blue OLEX	Blueprint Operational Level Exercise
CAB	Conformity Assessment Body
Cedefop	European Centre for the Development of Vocational Training
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	common vulnerabilities and exposures numbering authority
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
CSOA	Cyber Solidarity Act
CSS	Corporate Support Services
CTF	capture the flag
CTI	cyber threat intelligence
CVD	coordinated vulnerability disclosure
CVE	common vulnerabilities and exposures
Cyberhead	Cybersecurity Higher Education Database
Cybersopex	Cyber Standard Operating Procedure Exercise
Cysopex	Cyclone Standard Operating Procedure Exercise
DG Connect	Directorate-General for Communications Networks, Content and Technology
DORA	Digital Operational Resilience Act
EASA	European Union Aviation Safety Agency
EBA	European Banking Authority
EC3	European Cybercrime Centre
ECA	European Court of Auditors
Ecasec	European Competent Authorities for Secure Electronic Communications
ECATS	European Competent Authorities for Trust Services
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECSC	European Cybersecurity Challenge
ECSF	European Cybersecurity Skills Framework
ECSM	European cybersecurity month
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EFTA	European Free Trade Association
eID	Electronic identification
eIDAS	electronic identification and trust services
EMAS	Eco-Management and Audit Scheme
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ERA	European Union Agency for Railways
ERM	enterprise risk management
ESMA	European Securities and Markets Authority
ESO	European standards organisation
ERM	enterprise risk management
ETSI	European Telecommunications Standards Institute
EU5G	EU certification scheme for 5G networks
EUCC	EU common criteria
EUCS	European cybersecurity certification scheme for cloud services
EU CSI	EU Cyber Security Index
EUCC	EU Common Criteria
EU-Cyclone	EU Cyber Crisis Liaison Network
EUDIR	EU Digital Infrastructure Registry
EUIBAs	EU institutions, bodies and agencies
eu-LISA	EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Europol	EU Agency for Law Enforcement Cooperation
EU VBD	EU vulnerability database
FTE	full-time equivalent
GHG	greenhouse gas
GSMA	Global System for Mobile Communication Association
HR	human resources

HWPCI	Horizontal Working Party on Cyber Issues
IAS	Internal Audit Service
ICC	International Cybersecurity Challenge
ICT	information and communications technology
ISAA	integrated situational awareness and analysis
ISAC	information sharing and analysis centre
ISO	International Organization for Standardization
IT	information technology
Jasper	Joint awareness and preparedness cybersecurity exercise
JCAR	joint cyber assessment report
KPI	key performance indicator
Letra	learning and training
MeliCERTes	a project funded by the EU to connect CSIRTs around the Member States
MEP	Member of the European Parliament
MoU	memorandum of understanding
MS	Member State
NA	not available
NCC	national coordination centre
NCSS	national cybersecurity strategy
NIS	network and information security
NLO	national liaison officer
PPMT	Public Procurement Management Tool
OOTS	once only technical system
OSINT	open source intelligence
R & I	research and innovation
SCCG	Stakeholder Cybersecurity Certification Group
SLA	service-level agreement
SMEs	small and medium-sized enterprises
SOC	security operation centre
SOP	standard operating procedure
SPD	single programming document
SPOT	self-paced online training

TP-AH-24-001-EN-C

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA 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 the 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 978-92-9204-664-4