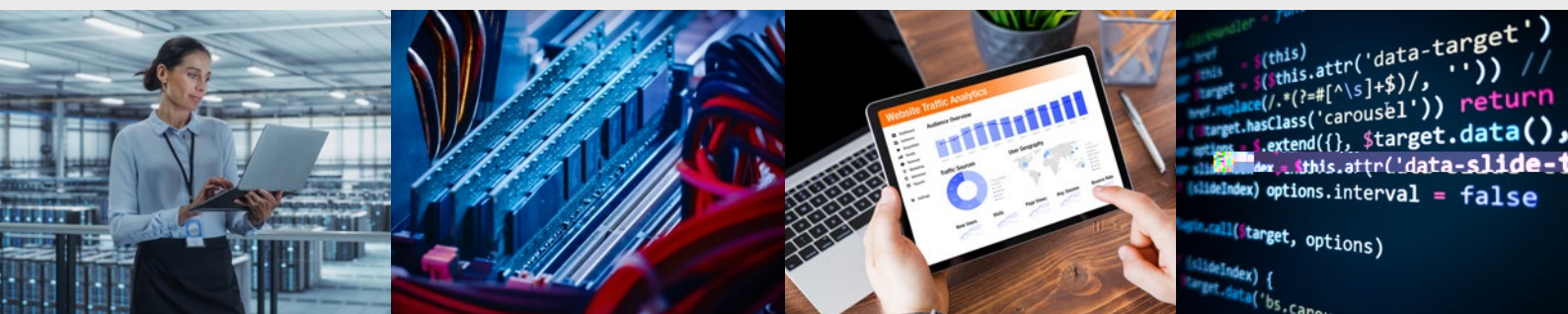


CONSOLIDATED ANNUAL ACTIVITY REPORT



2022

CONTACT

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

LEGAL NOTICE

This publication presents the annual activity report of ENISA for 2022. The report is based on the 2022 work programme as approved by the Management Board of ENISA in Decision No MB/2021/17 and amended budget approved by the Management Board of ENISA in Decision No. MB/2022/08.

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

© European Union Agency for Cybersecurity, 2023

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

Copyright for images on the cover and internal pages: © Shutterstock.

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

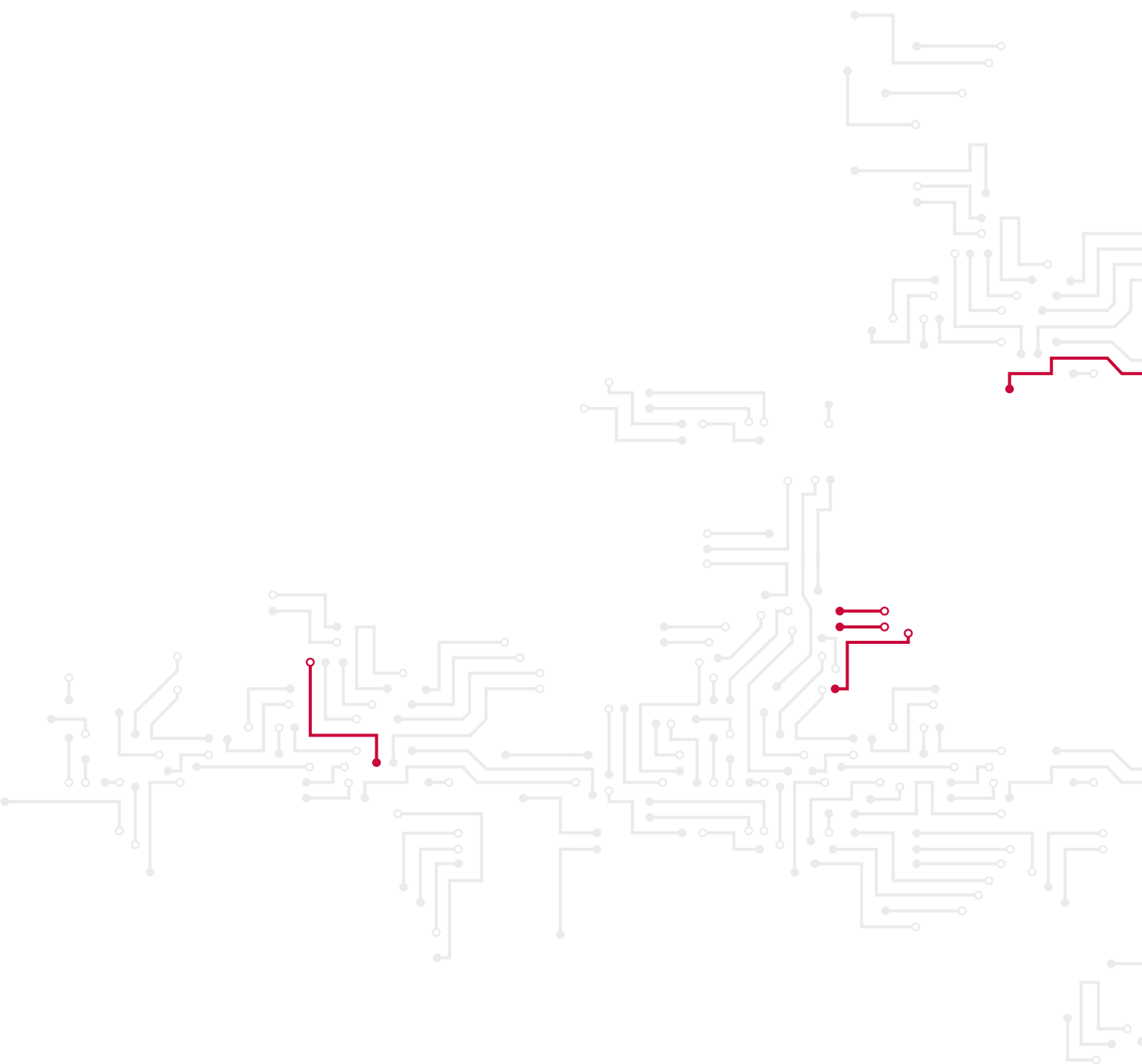
Print	ISBN 978-92-9204-640-8	ISSN 1830-981X	doi:10.2824/23110	TP-AB-23-001-EN-C
PDF	ISBN 978-92-9204-639-2	ISSN 2314-9434	doi:10.2824/000854	TP-AB-23-001-EN-N



CONSOLIDATED ANNUAL ACTIVITY REPORT 2022

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PART IV	
MANAGEMENT ASSURANCE	135
4.1. REVIEW OF THE ELEMENTS SUPPORTING ASSURANCE	135
4.2. RESERVATIONS	135
PART V	
DECLARATION OF ASSURANCE	137
ANNEX I	
CORE BUSINESS STATISTICS	139
ANNEX II	
STATISTICS ON FINANCIAL MANAGEMENT	155
ANNEX III	
ORGANISATIONAL CHART	158
ANNEX IV	
2022 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT	160
ANNEX V	
HUMAN AND FINANCIAL RESOURCES BY ACTIVITY	166
ANNEX VI	
GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENT	167
ANNEX VII	
ENVIRONMENTAL MANAGEMENT	168
ANNEX VIII	
ANNUAL ACCOUNTS	169
ANNEX IX	
LIST OF ACRONYMS, INITIALS AND ABBREVIATIONS	171





FOREWORD

by the Executive Director

Last year began in earnest with the Russian war of aggression against Ukraine, which included a strong cyber dimension. Within this context, the European Union Agency for Cybersecurity (ENISA) emphasised strengthening the resilience of Member States and EU institutions, bodies and agencies. The one-off support payment of EUR 15 million that the European Commission allocated to ENISA in autumn 2022 allowed the agency to capitalise on its existing operational cooperation, and its agile organisational structure that was put in place over previous years, and thus lay the foundations for massively scaling up and expanding its *ex ante* and *ex post* services provided to Member States. Unfortunately, this came at the cost of planned work programming activities that needed to mobilise resources to support the cybersecurity support action. Given this, some outputs were not able to deliver their expected objectives, and other work programme outputs delivered reduced services. The cybersecurity support action highlighted once again the need for the agency to be resourced sufficiently to meet stakeholder expectations, including the need for a resource buffer to cater for unexpected cybersecurity challenges.

The strategic discussions held with the Management Board throughout 2022 on the development of service packages in key areas of the agency's mandate came at the right time to address and respond to rapidly escalating challenges, thus stress-testing the agency's ability to operationalise and contribute to cooperative responses. The service packages integrate ENISA's various outputs across different activities, help the agency to prioritise its actions, build and make use of internal synergies, and ensure that adequate resources are reserved across the organisation.

The agency continued its endeavours mandated by the Cybersecurity Act by pursuing a resilient and clear path towards making Europe more cybersecure, and adapting ENISA's activities to changing circumstances. The agency fully carried out its mandate and tasks in support of the Union by way of the following activities.

ENISA continued to inform policymakers about the effectiveness of the existing policy frameworks through the third iteration of the network and information security (NIS) investments report, which helped support the Cyber Resilience Act (CRA) impact assessment, the impact assessment of the second network and information security directive (NISD2) and European Parliament policy documents on NISD2.

ENISA supported six sectors of the first network and information security directive (NISD): digital infrastructures, energy, health, rail, maritime and aviation. The agency provided different services depending on each sector's needs and, following the Russian war of aggression against Ukraine, organised a series of preparedness calls with stakeholders in critical sectors, including national authorities, sectoral EU agencies and key industry groups, in order to better understand the threats, gaps and issues.

The adoption of NISD2 in December last year was a good moment to look back and take stock of the success of the NISD and the impact achieved by ENISA in supporting policy implementation across the Union. However, one of the key issues with implementing the NIS1D was the lack of harmonisation across the EU, resulting in a fragmented policy landscape, which NISD2 aims to address, among other things. NISD2 increases the number of sectors within its scope and introduces several new horizontal tasks for ENISA, such as the EU register for digital entities. This means there is a need to prioritise and streamline the use of ENISA's resources. Therefore, the agency has developed and adopted an NIS strategy to support and reorganise its services.

Capacity-building activities significantly contributed to the enhancement of the cybersecurity capabilities of key stakeholders and brought the agency closer to the overall strategic objective that drives capacity-building efforts. Cyber Europe 2022, originally planned as Cyber Europe 2020, successfully simulated a major crisis in the EU healthcare sector, enabling stakeholders from Member States and other participants to extensively test and evaluate their business continuity plans and crisis management procedures. In addition, ENISA's training catalogue delivered against its strategic objective by organising training events that target attendees with similar knowledge and expertise levels but from different backgrounds, thus fostering information and experience sharing.

The European Cybersecurity Challenge of 2022 was held in September and was attended by 27 EU and European Free Trade Association countries, as well as five guest countries. A total of 33 teams and over 600 participants competed in the annual exercise to empower the younger generations worldwide, who will act as digital shields of tomorrow's workforce. In addition, ENISA presented the European cybersecurity skills framework during the first Cybersecurity Skills Conference, which was followed by the declaration of the President of the European Commission that 2023 will be the 'Year for Skills', thus providing another arrow in the quiver in the quest to upskill professionals in cybersecurity by offering a common 'language' for professionals so that they can make an informed decision when choosing cybersecurity as a career path.

The agency supported the operations of the computer security incident response teams (CSIRTs) network and the European cyber crisis liaison organisation network (EU-CyCLONe) during a challenging year, given the overall escalation of cybersecurity-related incidents connected to the Russian war of aggression against Ukraine. The CSIRTs network was already operating in escalated mode at the turn of the new year, and its operations further escalated to monitor activity after the initiation of the Russian war of aggression against Ukraine. ENISA was able to demonstrate its ability, as an organisation, to react to and address unforeseen challenges during cybercrises. ENISA supported the functioning of the CSIRTs network and EU-CyCLONe, providing both the secretariat function and infrastructure, and facilitated an improved exchange of information among cybercrisis management authorities in the EU via high-level meetings, secure communications channels, portals, dashboards and mailing lists for EU-CyCLONe.

ENISA contributed to cooperative response at Union and Member State levels with the initiation of several new services, primarily driven by the establishment of an operational and situational awareness sector, thus increasing its efficiency in generating and consolidating information, assessing incidents and facilitating information handling. As such contributed to the EU priority of situational awareness by supporting the consolidation of information on strategic, tactical and technical levels, and the exchange of such information with operational communities. The agency established a flash report service to enable fast communication of information; piloted the first two EU joint cyber assessment reports (JCARs); produced an integrated report providing a threat assessment of the Union based on input from EU institutions, bodies and agencies; and finally, as part of structured cooperation with the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies, established the joint rapid report service, providing joint operational and technical guidance to tackle large-scale cross-border threats to the EU.

In addition to situational awareness, the agency continued to develop its operational framework and expanded it after the EU ministers in charge of telecommunications unanimously called for 'the implementation of a new Emergency Response Fund for Cybersecurity to be put in place by the Commission'; the ministers noted that 'the current geopolitical landscape and its impacts in cyberspace strengthen the need for the EU to fully prepare to face large-scale cyberattacks. Such a fund will directly contribute to this objective.' Thus, as mentioned above, ENISA was able to operationalise and expand its programme into the cybersecurity support action after the Commission provided an additional budget of EUR 15 million in 2022 for the reinforcement of ENISA's support capabilities, which were to be made available to Member States. As part of this effort, the agency reallocated

posts from across the organisation in order to work closely with the Member States and the Commission to further design and set up framework contracts for each Member State so that ENISA's services could be scaled up. In particular, the services offered include penetration testing, threat hunting, threat landscapes, support for incident responses, risk monitoring, training and exercises.

In terms of certification, the Agency made new meaningful contributions to the EU cybersecurity certification framework by assisting the Stakeholder Cybersecurity Certification Group and supporting the Commission in discharging its duties concerning governance of the European Cybersecurity Certification Group, while further processing draft candidate cybersecurity certification schemes. ENISA reinforced its strategic goal of a 'high level of trust in secure digital solutions' through new components of certification schemes, some of which will have to be adopted and implemented by Member States. In addition, the agency supported cybersecurity certification by monitoring and analysing standards that are currently in use in European cybersecurity certification schemes, and it recommended appropriate technical specifications. In certain areas, this activity supported emerging policy concerning the standards for the European Digital Identity Wallet, for example, and vulnerabilities.

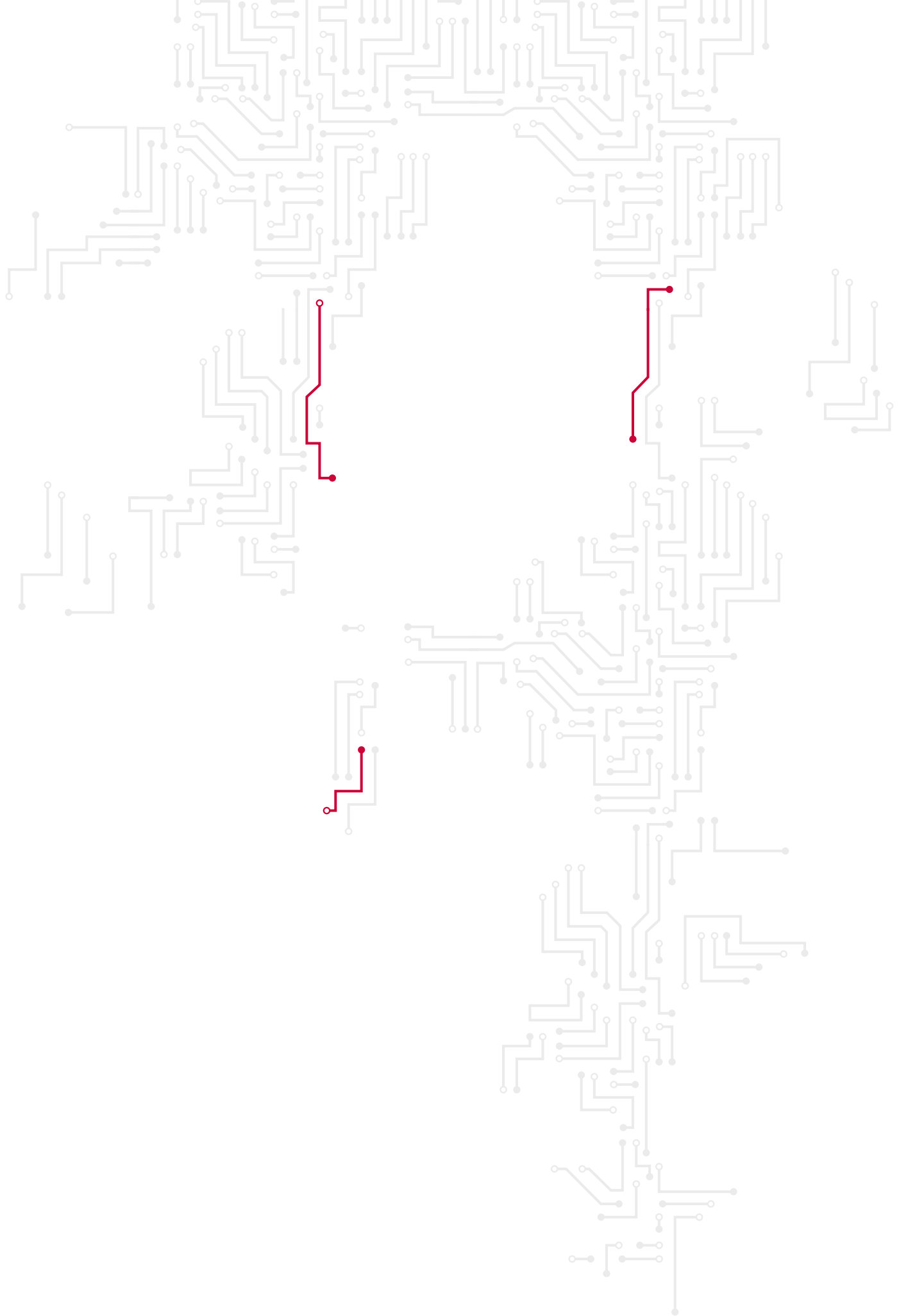
In terms of emerging cybersecurity challenges, ENISA has set the grounds and followed a multiannual perspective with the first pilot of the EU cybersecurity index, which will greatly contribute to the efficient and effective delivery of the report on the state of the cybersecurity in the union required by Article 18 of NIS2.

ENISA carried out multiple activities with the European Cybersecurity Competence Centre (ECCC) and the network of national coordination centres. A memorandum of understanding was prepared, providing a framework for cooperation and development of synergies with the ECCC, including the preparation of a service-level agreement to assist the ECCC with accounting and data protection services.

The agency conducted a survey of all its operational activities at the beginning of 2023 in order to ascertain stakeholders' satisfaction with both the results of the work carried out by ENISA over the previous 2 years and how the work was planned and implemented with stakeholders. The aggregated results demonstrate the high added value of ENISA's deliverables, with 93 % of stakeholders finding significant added value in the outcome/ results of ENISA's work. Only 7 % found limited added value and no stakeholder found no added value. In terms of take-up, 85 % of stakeholders said that they were likely to take up the results of ENISA's work in support of their tasks in the immediate to medium term. Operational cooperation Activities 4 and 5 scored the highest in terms of immediate take up (50 %), which, given the nature of these activities, is a good result. The extent to which ENISA's work duplicates Member States activities is low, with 83.7 % of stakeholders finding that ENISA deliverables do not duplicate or only somewhat duplicate Member State activities, which is a mark of ENISA's efforts to involve stakeholders in all stages of its work and ensure that the outcomes/results are fit for purpose.

The achievements of the year would not have been possible without the support of the cybersecurity community, including statutory bodies such as the Management Board, Advisory Group, the national liaison officers, the CSIRTs network and EU-CyCLONe, among many others. The community worked alongside ENISA staff in both planning and implementing the work programme. This is why I cannot be thankful enough to all our stakeholders and staff who contributed to these endeavours and without whom ENISA could not deliver its work in raising the level of cybersecurity across the Union in cooperation with the wider community.





ENISA MANAGEMENT BOARD ASSESSMENT

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

The conclusions of the Management Board are as follows:

1. 2022 was a pivotal year for the agency requiring it to respond rapidly to escalated cybersecurity challenges, thus stress testing its ability to operationalise and contribute to cooperative response. Whilst the agency had seasoned services that supported operational cooperation it lacked sufficient operational reserves to absorb the increased demand for urgent support services due to escalations in cybersecurity threats in connection with the Russian war of aggression on Ukraine.
2. The Cyber Assistance Mechanism under output 5.2 of activity 5 “contribute to cooperative response at Union and Member States level” was expanded to strengthen the need for the EU to fully prepare to face large-scale cyberattacks by delivering the cybersecurity support action simultaneously to all Member States. The Commission provided additional budget (15 million) to ENISA with a view to increasing its level of support to Member States, in line with ENISA's mandate under the Cybersecurity Act. As such the agency was able to leverage on its' existing planned activities in order to rapidly operationalise and expand a programme of this scale; and take advantage of its agile organisational structure. The agency re-allocated 10.5 FTEs from across the agency, the majority of which were re-allocated from the operational cooperation unit responsible for activities 4 and 5, that amounted to 8 FTEs and the remaining 2.5 FTEs from the other work programme activities. Thus, the agency achieved its goal of having framework contracts in place in 27 Member States and a pan-European lot by year end, but this came at the expense of other work programme outputs. Moreover, at least the same re-allocation of resources shall continue in 2023 for the implementation of the cybersecurity support action and as such impacting the planned allocation of resources in the 2023 work programme.
3. The MB acknowledges the excellent effort made by ENISA to re-allocate staff from across the activities to deliver the cybersecurity support action and acknowledges the strain on human capital due to insufficient operational reserves available to the agency to manage times of escalation.
4. The MB concludes that the agency will need to invest further in its operational cooperation activities and can only do so with increased human resources that also include an operational reserve component to be able to manage heightened cybersecurity challenges during times of escalation.
5. The MB concludes the results of the stakeholder satisfaction survey sheds much important light on how stakeholders perceive the added value

of ENISA's work. On aggregate the results demonstrate high added value of ENISA's deliverables with 93 % of stakeholders finding significant added value in the outcome / results of ENISA's work. Only 7 % find limited added value and no stakeholder finds no added value. In terms of take up, 85 % of stakeholders also rate the likelihood of taking up the results of ENISA work in support of their tasks in the immediate to medium term, of which the operational cooperation activities 4 and 5 scored the highest in terms of immediate take up (50 %), which, given the nature of these activities, is a good result.

6. The mandate of the agency requires that the agency carry out its tasks while avoiding the duplication of Member State activities, therefore the result that 83,7 % of stakeholders find that ENISA deliverables do not duplicate or only somewhat duplicate Member State activities is tantamount to ENISA's effort to involve stakeholders in all stages of its work and ensure that the outcomes / results are fit for purpose. The MB notes that duplication in some areas is unavoidable due to the nature of the work and the need for MS to have their own capacities, but requests ENISA to increase efforts to focus its work even more on high added-value / low-duplication areas.
7. The AAR2022 outlines in detail those outputs that did not meet their objectives due to the re-prioritisation of resources, more specifically the MB notes outputs 4.2 "Develop and enhance standard operating policies, procedures, methodologies and tools for cyber crisis" and output 5.3 "Initiate the development of a trusted network of vendors/suppliers" did not achieve their objectives in full as set out in ENISA's work programme 2022, due to de-prioritisation. The MB also takes note that the level of services for output 4.1 also suffered due to reallocation of resources to support action, and that sectorial activities for the NIS1 sectors under output 2.1 was also impacted due to the re-prioritisation of tasks to deliver the cybersecurity support action. In addition, and unrelated to the cybersecurity support action, the MB takes note that output 7.3 did not fully meet its objectives.
8. In order for the agency to be able to fulfil its mandate in the coming years the MB recommends that the agency reduce the scope and/or discontinue outputs in the 2024 work programme based on the assessment of outputs in the AAR2022. Particularly, the MB notes the assessment of outputs 3.4 & 3.6 in activity 3 building capacity; outputs 7.3 and 7.4 in activity

7 supporting European market and industry and 9.4 in activity 9 outreach and education. The MB invites the agency to also consider resourcing specific outputs including via a payable services model in-line with the directions and framework outlined in the draft corporate strategy (especially for services delivered under outputs 3.7 and 9.1) and create synergies with relevant partner organisations to cover some of the potential gaps emerging from reprioritisation.

9. The MB also takes note of the estimated 5 FTEs highlighted by the operational activities that have been used to support technical/administrative tasks within the activities and recommends that these types of services be covered in the future via corporate support cost model in line with directions and framework outlined in the draft corporate strategy, thus liberating the 5 FTEs to operational activities.
10. The AAR also describes how ENISA managed its resources and presents the budget execution of the EU subsidy. In the course of 2022, the agency has been operating with a budget of EUR 39,2 million equivalent to a 67 % increase in 2022 compared to the 2021 budget (EUR 23,5 million), this includes the additional budget of EUR 15 million for the Pilot Implementation of a cybersecurity support action, which was given to the agency only in August 2022.
11. During 2022, ENISA committed a total amount of EUR 39 179 405 representing 99.93 % of the total budget for the year. Payments made during the year amounted to EUR 20 396 780 representing 52,02 % of the total budget. A majority of the commitments under cybersecurity support action were signed late in the year which explains the relative low payment rate (and the subsequent large carry forward). The MB take notes of the exceptional large amount carried forward from 2022 to 2023 of EUR 18 783 000 (47,91 % of the budget). This exceptional significant amount carried over to 2023 constitutes a major risk to the 2023 budget execution and shall need to be actively monitored to mitigate inherent risks.

As compared to 2021, there has been a slight increase in commitment execution 99,93 % in 2022 as compared to 99,51 % in 2021. Overall payment execution has decreased due to cybersecurity support action funds and reached 52,02 % as compared to 77,40 % in 2021. However, comparing only the initial budget allocated to ENISA payment execution increased to 84,11 % which is a noticeable achievement. The target of 95 % for

commitment rate set by the Commission (DG Budget) was reached. The turnover of staff was greatly reduced in 2022. The ratio was only 4 % percent which shows improvement in retaining staff members in the agency.

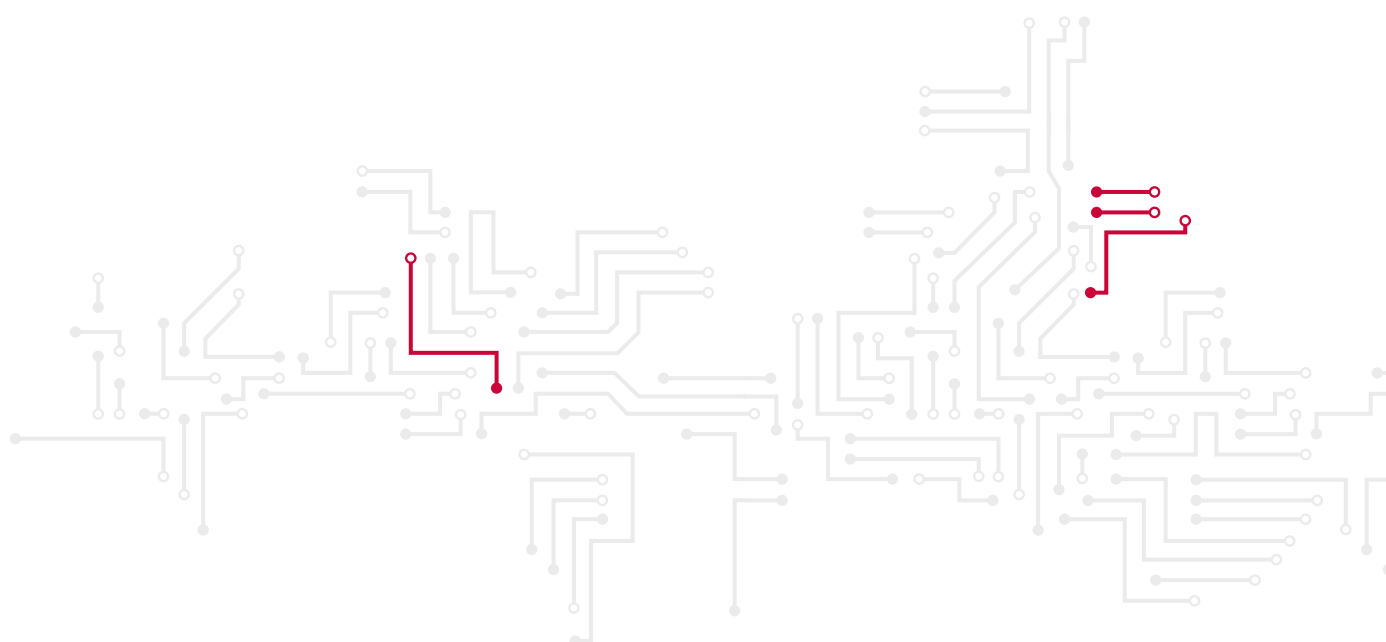
- 12.** The AAR also provides information on the internal control assessment for 2022. This section notes the main categories of deviation that led to exceptions reported.

In 2022 the agency reported 27 exceptions in the AAR. None of these exceptions was assessed as high risks. In 2022 the MB amended internal control indicators to allow the agency better assessment of its application. Whilst some improvements are required the internal control are present and functioning. The 2022 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 2022 to improve the overall efficiency of the agency in abiding to its principles and congratulates ENISA for all the efforts engaged to that end.

- 13.** 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 included in evaluations. Overall, the Management Board takes note of the successful achievements of ENISA in 2022.

- 14.** 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 2022 work programme. However, the MB takes notes on insufficient human resources of the agency and the detriment this has on its ability to achieve a high common level of cybersecurity across the Union.
- 15.** 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 and direct the Management Board chair to address a letter to the relevant institutions highlighting the conclusions of this assessment, in particular the need to increase staffing posts to ENISA, for the agency to be able to fully deliver its mandate in a sustainable manner.



EXECUTIVE SUMMARY

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. To do so, the agency acts as a centre of expertise on cybersecurity, and collects and provides independent, high-quality technical advice and assistance to Member States and EU bodies. ENISA is committed to strengthening trust in the connected economy, boosting the resilience of and trust in the Union's infrastructure and services, and keeping our society and citizens digitally secure. The agency therefore strives to be an agile, environmentally and socially responsible organisation focused on people.

The Russian war of aggression against Ukraine dominated the EU's security agenda in 2022. ENISA stepped up its coordination and preparedness, and contributed to the EU's shared situational awareness by providing regular situational reports of cyberactivity. There was also intensified coordination and exchange of information with cybersecurity networks, such as the European cyber crisis liaison organisation network (EU-CyCLONe) – which consists of national cybersecurity crisis management authorities – and numerous sectorial communities supported by ENISA. In addition, constant efforts ensured channels of communication between political, operational and technical levels, and enhanced cooperation with the computer security incident response teams network were realised.

Efforts to step up preparedness included a number of actions such as exercises, guidance, legislative measures, increasing resilience in critical sectors, and work with partners. During the French Presidency of the Council of the European Union, together with the European External Action Service, ENISA organised a scenario-based exercise in early 2022 called the Cyber Crisis Linking Exercise on Solidarity, with the aim of raising awareness at political level and strengthening cooperation between operational and political levels in cases of large-scale cyberattacks.

During 2022, the European Commission allocated a one-off support payment of EUR 15 million to ENISA so that the agency could massively scale up and expand its *ex ante* and *ex post* services to the Member States in 2023. In 2022, the agency worked closely with the Member States and Commission to set up the framework contracts in each Member State so that ENISA could scale up the services it offered to beneficiaries indicated by the Member States. This short-term support aimed to complement rather than duplicate efforts by Member States and at Union level to increase the level of protection and resilience to cyber threats, by providing ENISA with additional means to support preparedness (*ex ante*), and response (*ex post*) to large-scale cybersecurity incidents.

The agency managed the cybersecurity support action by reallocating staff from across its activities, and specifically from Activities 4 and 5, responsible for

operational cooperation and cooperative response in order to achieve the goal of having framework contracts in place in the 27 Member States and a pan-European lot by year end, but this came at the expense of other work programme outputs, as detailed in this annual activity report.

During 2022, legislative proposals were put forward to develop cybersecurity across the EU. ENISA worked together with Member States to identify the best EU practices in line with the provisions of the network and information security directive and share them among its stakeholders. The agency supported Member States with the implementation of the revised rules under the second network and information security directive, and new rules, including those of the Digital Operational Resilience Act (DORA), those of the future Electricity Network Code for Cybersecurity, and the ones that will be introduced with the Cyber Resilience Act.

During the development of the 2023 work programme, the agency identified a resource shortfall amounting to EUR 734 000 and two full-time equivalents (FTEs) in operations, and EUR 2.5 million in corporate services. In order to address the resource shortfall, each activity manager assessed what could and could not be delivered with the available resources, and what the impact of the shortfall would be on the activity by describing reduced scope, postponed projects and suppressed outputs.

The agency undertook a thorough assessment of its internal human resourcing needs for the programming period of 2023-2025, taking into account the legislative and political developments expected in the short term, as well as the heightened level of threat of the cybersecurity landscape. The assessment points out a significant human resource gap with approx. half of this gap linked to highly critical or critical activities needed to fulfil the tasks for 2023-2025. If no additional posts are made available to reduce this gap the agency will need to undertake a prioritisation exercise in the development of its forthcoming work programmes to offset the shortfall in resources.

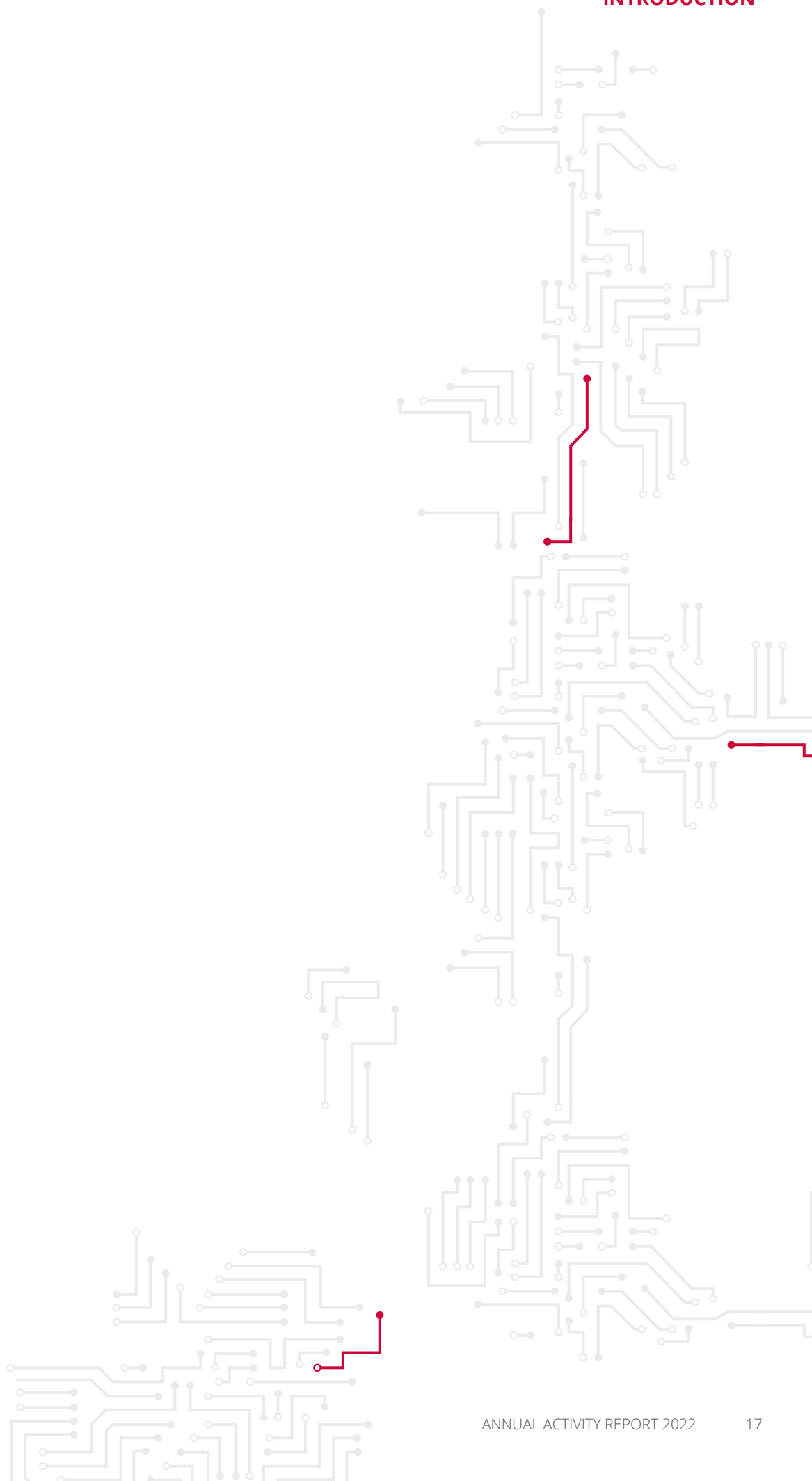
In terms of budget execution in 2022, ENISA executed 99.93 % of the annual budget for these, and 52.02 % in payment appropriations of the annual budget for these. A majority of the commitments under the cybersecurity support action were signed late in the year, which explains the relatively low payment rate (and the subsequent large amount carried forward). However, omitting the implementation of the cybersecurity support action funds, ENISA executed commitment appropriations representing

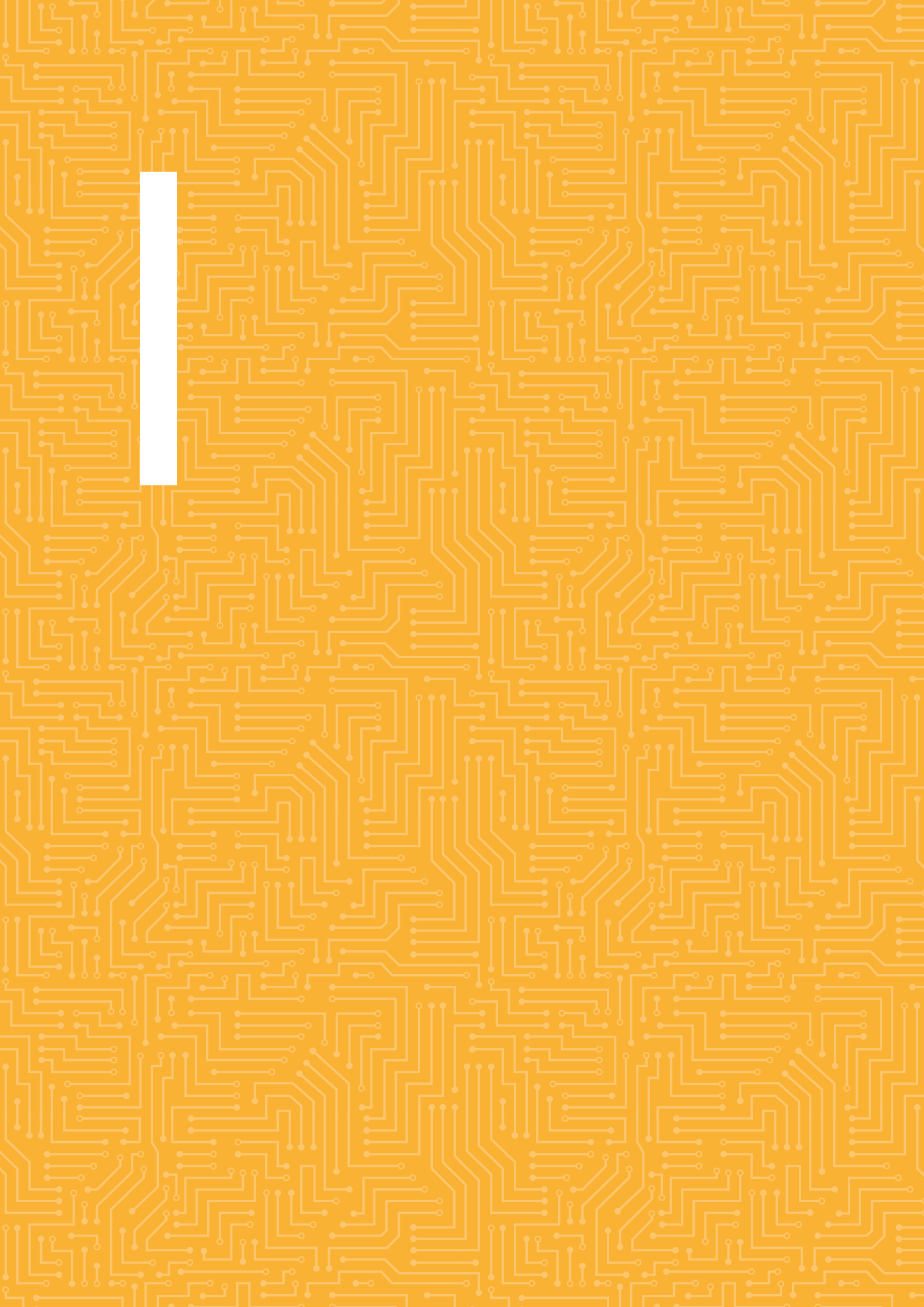
99.91 % of the annual budget for these, and payment appropriations amounting to 84.11 % of the annual budget for these. The exceptionally large amount carried forward from 2022 to 2023 of EUR 18 783 000 (47.91 % of the budget) is exceptionally significant, constitutes a major risk to the 2023 budget's execution and must be actively monitored to mitigate inherent risks.

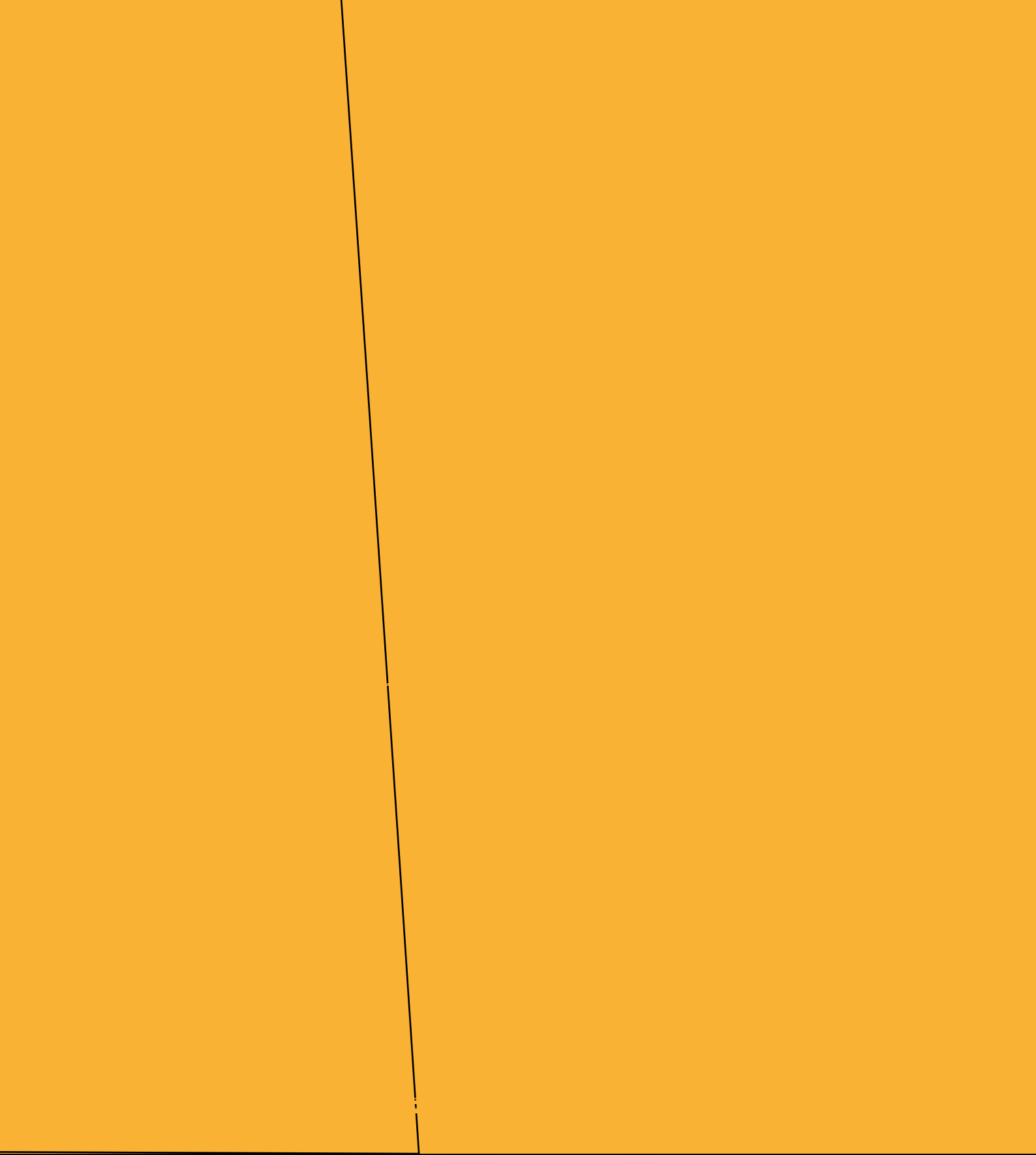
Compared with 2021, there was a slight increase in commitment execution: 99.93 % in 2022 of 0.42 %. Overall, payment execution decreased due to the cybersecurity support action funds, reaching 52.02 % in 2022, compared with 77.40 % in 2021 (68.62 % in 2020). However, comparing only the initial budget allocated to ENISA, payment execution increased to 84.11 %.

In terms of human resources, the corporate services continued to support the operational and administrative goals of the agency in terms of staff acquisition and development. In 2022, ENISA welcomed 16 newcomers (7 temporary agents, 4 contract agents, 4 seconded national experts and 1 trainee).

ENISA adopted a comprehensive methodology for enterprise risk management in 2022, based on the relevant guidelines of the European Commission. In this content, the agency also formalised its information technology security risk management methodology, which is interlinked with the enterprise risk management framework. On the basis of the adopted methodologies and related established internal procedures, ENISA performed its enterprise and information technology security risk assessments, which will feed into ENISA's activities in the years to come.







ACTIVITY 1

Providing assistance on policy development



The European Union Agency for Cybersecurity (ENISA) supported the objective of having cybersecurity included as an integral part of EU policy by:

- providing services related to the development of new policy files;
- collecting evidence to support the effectiveness of the existing policy framework;
- providing EU policymakers and stakeholders with policy recommendations on future cybersecurity challenges and opportunities.

Achievements

- In 2022, the budget commitment rate for Activity 1 was very high (98 %¹), and the minimal amount that was carried over to 2023 (3 % of the total EUR 363 000) was already committed in October and related to the organisation of the EU Cybersecurity Policy Conference in January 2023. Activity 1 also received a very high score in the ENISA stakeholder satisfaction survey (93 %), and received a perfect score from stakeholders on organisation and planning (100 %).
- ENISA continued to inform policymakers about the effectiveness of the existing policy framework through the third iteration of the network and information security (NIS) investments report. The report is referenced 16 times in EU and national policy documents, including in the Cyber Resilience Act (CRA) impact assessment, the impact assessment on the second network and information security directive (NIS2) and European Parliament policy documents on NIS2. At the same time, synergies with other ENISA activities (e.g. the cybersecurity index and the NIS sectoral strategies) were expanded.
- ENISA supported evidence-based policymaking to foster cybersecurity as an integral part of EU policy by supporting the Directorate-General (DG) for Communications Networks, Content and Technology (DG Connect) in the development of the CRA proposal, including the impact assessment and consultations with relevant stakeholders. This task was not foreseen in the 2022 single programming document (SPD), and to respond to it we had to reprioritise resources from within Activity 1 to account for the CRA and the 1.2 full-time equivalent (FTE) gap resulting from vacant posts and extended absences. This was achieved by delaying or postponing contributions in the areas of artificial intelligence (AI) (resulting in saving 0.4 FTEs) and the once and only technical solution (OOTS) (resulting in saving 0.25 FTEs), but also was possible because policy development activities were less than anticipated in policy areas that moved towards implementation in the second half of the year, making the reallocation of FTEs possible, such as the Digital Operational Resilience Act (DORA) (0.3 FTEs reallocated), the Electricity Network Code (0.2 FTEs reallocated), European Union Aviation Safety Agency (EASA) Opinion No 03/2021 on the management of information security risks in the aviation sector (0.2 FTEs reallocated) and NIS2 (0.3 FTEs reallocated).
- ENISA further supported fostering cybersecurity as an integral part of EU policy by also contributing to a number of sectoral policy files under development in 2022 that focused on cybersecurity. Examples include ENISA's support of policy files such as DORA, the Electricity Network Code (NCCS) and EASA Opinion No 03/2021 on management of information security risks in the aviation sector. Some of the policy files that were formally adopted in 2022, specifically NIS2, DORA and the Electricity Network Code, include specific tasks for ENISA and will be included from SPD 2023 onwards under Activity 2, which relates to supporting the implementation of EU policy.
- In order to support evidence-based policymaking, ENISA maintained and even further developed strategic relationships and cooperation with a number of DGs. Examples include the support given by ENISA to DG Connect and the European Parliament with regard to NIS2 negotiations and the CRA; its support to DG

¹ rounded

Financial Stability, Financial Services and Capital Markets Union, the European Insurance and Occupational Pensions Authority and the European Banking Authority in preparation for DORA; and its support to the European Union Agency for the Cooperation of Energy Regulators (ACER) and DG Energy for the development of the Electricity Network Code.

- ENISA further developed its offerings to policymakers by creating the first EU cybersecurity policy catalogue, which takes stock of all ongoing legislative initiatives with cybersecurity provisions to increase the level of awareness and understanding of emerging policy areas, and to support the identification of synergies, overlaps or even inconsistencies. In total, the policy catalogue analyses 13 policy files that were under development in 2022.
- ENISA also organised, in cooperation with DG Connect, the first EU Cybersecurity Policy Conference, which covered key EU cybersecurity policy files and aimed to bring together various communities affected by these policies, thus supporting community engagement across the cybersecurity ecosystem. In total, 220 participants attended the conference. The subsequent satisfaction survey revealed no negative opinions and also 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). Both the policy catalogue and the policy conference will be further developed in future years and will become regular products of this activity.

Resources

- There is a proliferation of new horizontal, sectoral and transversal cybersecurity policy initiatives where ENISA's contribution is requested or would be beneficial. While ENISA was able to offer its support to several policy files, such as NISD2, CRA and DORA, resource constraints prevented the agency from actively supporting policy files with cybersecurity provisions, such as the European Health Data Space, and other key files, such as the Digital Markets Act and the Digital Services Act. This year, ENISA's cybersecurity policy observatory is piloting a framework to optimise the agency's service provision in support of policy development and to prioritise specific policy files. However, ENISA typically supports these policy initiatives using internal human resources, so, unless these resources are somewhat increased, the agency may need to scale down its support of the Commission and Member States in that regard.
- ENISA's ability to support different stages of the policy development life cycle is currently limited by a lack of available human resources and the need for additional policy experts with the relevant skills, posing substantial challenges when it comes to properly following up on and engaging with each new policy initiative in order to ensure consistency and alignment. In 2022, the agency had to deliver its services under Activity 1 with fewer resources than originally planned due to absences and vacant posts. The lack of enough staff with appropriate seniority and specific skills to support policy development is also a challenge that ENISA will address through recruitment, and learning and development activities. The further development of internal competences to perform evidence-based policymaking analysis will be a key success factor in the following years. In the short term, an additional FTE corresponding to a suitable experience profile (a seconded national expert (SNE) or administrator of level AD6 or above) would be required, though 0.5 FTEs can be released from 2025 onwards, assuming EU cybersecurity policy development slows.
- The expanded scope of NISD2, which introduces more sectors and increases the number of operators in scope for existing sectors, in combination with macroeconomic factors (inflation) will introduce financial resource challenges for evidence collection through the NIS investments report. Unless a budgetary increase for this work is planned, it is likely that not all NISD2 sectors will be covered in future versions of the report and/or the operator samples may not be representative enough at sector or country level. Specifically, a EUR 150 000 budgetary increase is required; otherwise, the NIS investments report will only cover 15–18 Member States in 2024.
- It is estimated that approximately 0.35 FTEs are used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes, etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

Overall assessment

- In 2022, ENISA took further steps towards obtaining the strategic objective of fostering cybersecurity as an integral part of EU policies. The total number of ENISA contributions grew, primarily due to the increase in policy development activities that the agency was called on to support, but also due to the shift of focus of Activity 1 to the provision of services (e.g. in the form of providing policy advice on request and contributing to the work of task forces), as opposed to the drafting of ENISA reports on relevant topics. An indication of the impact of the agency's support of policy development can be seen in the number of references to ENISA's reports, analyses and/or studies in EU and national policy documents, which is 30 for ENISA's work delivered under the 2021 SPD and 10 for work delivered under the 2022 SPD so far ^(a). The added value of ENISA's work to provide assistance to policy development was recognised by 92 % of respondents to the stakeholder survey.
- Further progress towards meeting the strategic objective is expected as the policy catalogue builds synergies with the foresight capabilities currently being developed within the agency in order to enhance ENISA's advisory capabilities regarding emerging areas by bringing emerging/future topics of interest to the attention of EU policymakers and stakeholders.
- ENISA also supported the community empowerment and engagement strategic objective in the context of cybersecurity policy by organising the first EU cybersecurity policy conference and facilitating stakeholder engagement in policy development. ENISA's positive impact in facilitating community building was also acknowledged by 91 % of respondents to the stakeholder survey.
- Still, the proliferation of legislative initiatives and policies addressing cybersecurity, such as new sectoral legislation, in combination with internal resource constraints, limits the extent to which ENISA can support all new policy files. The service-based approach introduced by the cybersecurity policy observatory will mitigate this and allow for improved prioritisation and planning, but it is unlikely that ENISA will be able to support evidence-based policymaking for the full scope of policy initiatives. The activity would benefit from having additional experts familiar with the life cycle of EU policy development and from an increased budget.
- Given the increased stakeholder interest in ENISA's maintenance of a policy catalogue of new policy developments and in ENISA supporting the monitoring of the policy landscape, it would be beneficial to rescope current output 1.3 to focus on the support of policy monitoring and the maintenance of a policy catalogue.
- As regards the key performance indicators (KPIs), the measurement of references to ENISA's work in national policy documents (metric 1.2) proved difficult given the language constraints of the endeavour. Instead, the agency proposes focusing the metric on EU-level references only.

Objectives



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

Link to strategic objective (ENISA strategy)



- Cybersecurity as an integral part of EU policies
- Empowered and engaged communities across the cybersecurity ecosystem

Results



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

Outputs



- 1.1.** Issue reports, studies and analyses on the effectiveness of the current cybersecurity policy frameworks

Outcome



- ENISA published the third NIS investments report, providing policymakers with insights into the cybersecurity budgets of operators of essential services (OESs) and digital service providers (DSPs), and how these budgets were influenced by the NISD, in order to inform future policy decisions. Data from the report were also used to support the CRA impact assessment, and several ENISA activities, such as the cybersecurity index.
- ENISA produced a stocktaking report to support evidence-based policymaking in the health sector by providing sectoral national competent authorities with relevant facts and with a gap analysis to identify potential needs to support OESs in the sector.
- In the context of providing input to national competent authorities to inform policy decision-making on the topic of supply chains, ENISA drafted a report on good practices for information and communications technology (ICT) / operational technology (OT) supply chain cybersecurity, based on evidence collected through the survey on NIS investment, the 2022 ENISA threat landscape and desk research.
- ENISA produced a policy catalogue of all relevant EU policy files under development in 2022 to support policymakers in the identification of possible synergies, overlaps or even inconsistencies.
- In collaboration with DG Connect, ENISA organised the first EU Cybersecurity Policy Conference, focusing on key EU policy files with cybersecurity provisions and bringing together the relevant communities.

The NIS investments report is available online (<https://www.enisa.europa.eu/publications/nis-investments-2022>).

The output achieved its objectives in 2022. The scope of it remains timely and relevant. Based on ENISA's assessment, it should remain in the 2024 SPD.

- 1.2.** Carry out preparatory work and provide the European Commission and Member States with tailor-made advice and recommendations on new policy initiatives in emerging technological, societal and economic trends – such as AI, 5G, electronic ID, digital operational resilience in the finance sector and cyber insurance – and other potential initiatives (e.g. the OOTS)

- ENISA supported the European Commission with regard to the CRA proposal by:
 - providing technical expertise through written contributions and participation in technical meetings, and delivering technical briefings on various topics of the CRA;
 - supporting public consultations and interactions with stakeholders;
 - providing data from the NIS investments report for the CRA impact assessment.
- ENISA provided support to the European Commission and the Directorate-General for Financial Stability, Financial Services and Capital Markets Union in relation to the development of the legislation for DORA for the financial sector. ENISA supported the European Insurance and Occupational Pensions Authority and the European Banking Authority in the harmonisation of incident reporting in preparation for DORA legislation.
- In 2022, ENISA continued its support of DG Energy, ACER and European Network of Transmission System Operators for Electricity

(ENTSO-E) in drafting, reviewing and assessing the Electricity Network Code by contributing to consultation meetings, providing technical advice on relevant subjects (e.g. risk scenarios, certification, incident classification scheme) and by creating a mapping table of tasks for all entities involved in the network code.

- ENISA produced a report on the area of cyber insurance to analyse the requirements from the perspective of OESs and to identify recommendations to help policymakers increase the uptake of cyber insurance.
- ENISA supported the development of the Artificial Intelligence Act (AIA) by developing good cybersecurity practices for AI, taking into account the whole AI life cycle in order to contribute to the development of the cybersecurity requirements of the AIA, and supported the assessment of Member State readiness in monitoring and enforcing cybersecurity requirements for AI in anticipation of the AIA.
- ENISA supported the European Commission and the Member States in cybersecurity aspects of the OOTS by contributing to the activities of the OOTS security subgroup meetings and providing technical advice on the development of the OOTS security policy and framework.
- ENISA participated in the European Strategic Coordination Platform activities, namely within the scope of Opinion No 03/2021: Management of Information Security Risks, drafted by EASA. Having joined two expert groups (on risk management and incident response), ENISA provided contributions on the acceptable means of compliance and guidance materials, which support and further develop the details and specifications of this sectoral policy.

The cyber insurance report is available online (<https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu>).

The output achieved its objectives in 2022. The scope of it remains timely and relevant. Based on ENISA's assessment, it should remain in the 2024 SPD.

1.3. Assist the Commission in reviewing existing policy initiatives

- To support NISD2 policy development, ENISA worked together with stakeholders to collect and analyse requirements for the development of the registry for entities under NISD2, Article 27. This task was carried out in conjunction with Activity 2 (policy implementation) and also included the development of a mock-up of the registry.
- In the context of NISD2 policy development, the agency engaged in knowledge-building activities on the topic of coordinated vulnerability disclosure (CVD), including consultations with experts, organisation of a knowledge-building session on vulnerabilities, and meetings with stakeholders to support Member States in preparing for CVD implementation.
- In anticipation of the security requirements implementing acts under NISD2, Article 21(5), ENISA provided policy advice to the Commission based on the analysis of existing frameworks around security requirements and proposals for the approach to drafting the implementing acts.
- ENISA supported the Commission with the review of the second electronic identification and trust services (eIDAS) regulation and the European Digital Identity Wallet toolbox process by participating in multiple technical meetings and panels, and providing technical advice.

The output achieved its objectives in 2022. However, given the increased stakeholder interest in ENISA's maintenance of a policy catalogue of new policy developments and in ENISA supporting monitoring of the policy landscape, it would be reasonable to make some changes to the outputs. The review of existing policy initiatives move to outputs 1.1 and 1.2, and re-focus output 1.3 on the support of policy monitoring and the maintenance of a policy catalogue.

Key performance indicators: ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (<i>ex ante</i>)	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
1.1. Number of relevant contributions to EU and national policies and legislative initiatives ^b	Number	Annual	Manual collection from staff members	193	314
Contributions to task forces and bodies	%	Annual	Manual collection from staff members	13 % of 193 total contributions	9 % of 314 total contributions
Contributions to workshops and conferences	%	Annual	Manual collection from staff members	83 % of 193 total contributions	87 % of 314 total contributions
Support actions/contributions to European Commission and Member States for policies and legal initiatives following relevant requests	%	Annual	Manual collection from staff members	4 % of 193 total contributions	4 % of 314 total contributions
1.2. Number of references to ENISA reports, analysis and/or studies in EU and national policy documents	Number	Biennial	Report	30	10
1.3. Satisfaction with ENISA added value of contributions (survey)	%	Biennial	Survey	N/A	93 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	92 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	92 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	90 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	95 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	91 %
Allocated FTEs as per SPD based on full establishment at 2022 year end	6	Actual used FTEs		4.8	
Planned budget (direct costs only)	EUR 363 000	Consumed budget (direct costs only)		EUR 354 406	
		Of which carried over to 2023		EUR 13 495	

a Several ENISA reports were published in late 2022 or early 2023, so not enough time has passed since their publication for them to be referenced.

b Based on the internal satisfaction survey run by the network at the end of 2022.

ACTIVITY 2

Supporting implementation of Union policy and law



Activity 2 of the work programme includes the ENISA activities supporting EU Member States with the implementation of Union cybersecurity policy, including legislation such as the NISD, but also other policies in the areas of 5G, electronic communications (the European Electronic Communications Code (EECC)), trust services and digital identity (the eIDAS regulation), privacy and CVD. ENISA's objectives are to ensure consistency between sectoral and horizontal policy files, to support harmonisation between EU Member States, and to ensure the effectiveness of policy implementation by delivering practical solutions and developing and promoting good cybersecurity practices.

Achievements

- In 2022, the budget commitment rate for Activity 2 was very high (98 %) and a minimal amount was carried over to 2023 (> 1 % of the total EUR 780 000). Activity 2 also had the highest score of all the SPD activities in the ENISA stakeholder satisfaction survey (94 %) and received a perfect score from stakeholders on organisation and planning (100 %).
- An important milestone last year was the development of an ENISA NIS strategy, in consultation with the relevant stakeholders. The NIS strategy streamlines ENISA's policy implementation work by bundling ENISA services into targeted packages, based on the needs of a sector. These packages leverage the synergies with other ENISA units via internal workflows. The 'build' package, for example, is for sectors lacking maturity, and it offers a combination of awareness-raising campaigns (Activity 9), capacity building (Activity 3) and policy knowledge building (Activity 2).
- In 2022, ENISA supported six NISD sectors: digital infrastructures, energy, health, rail, maritime and aviation. ENISA provided different services depending on the sector's needs. In immature sectors, for example, there is a need to raise awareness and build up the community. In mature sectors where there are already established working groups of national authorities, ENISA can work with these groups on more specific sectoral issues. Across the board, ENISA developed close relations with the relevant sectoral stakeholders (e.g. EU agencies ACER, the Body of European Regulators for Electronic Communications, the European Union Agency for Railways (ERA), EASA, the European Central Bank and the European Banking Authority).
- The EU toolbox for 5G cybersecurity continues to be a high priority for the Commission, Member States and ENISA. Last year, ENISA finalised the 5G matrix (an action under the EU cybersecurity strategy). The 5G matrix is a comprehensive repository of technical security controls for 5G networks, aligned with the EECC, that addresses the 5G toolbox technical measures and supports national authorities with the supervision of 5G networks.
- ENISA continued to develop good practices for policy implementation and resilience for the telecom sector (subsea cables, security for embedded SIM, Signalling System 7 security), for trust service providers (on remote video identification) and for wallet providers, and cybersecurity good practices supporting data protection engineering.
- ENISA supported Member States with the implementation of national CVD policies by developing guidelines for Member States on how to set up national CVD policies, and facilitated the exchange of good practices between EU Member States by supporting a working group of Member States and collecting good practices in a technical paper.

The Russian war of aggression against Ukraine led to some tasks that were not foreseen in the ENISA SPD.

- In the first weeks of the Russian war of aggression against Ukraine, ENISA organised a series of 30 preparedness calls with stakeholders in critical sectors, including national authorities, sectoral EU agencies and key industry groups. These calls provided the agency and the sectoral stakeholders with a better understanding of the threats, gaps and issues. ENISA subsequently delivered sectoral preparedness leaflets, which were used by national authorities to prepare operators for potential threats.

- ENISA was invited to the informal council meeting of telecom ministers in Nevers, joining a strategic discussion with the 27 telecom ministers, the Commission and the Body of European Regulators for Electronic Communications about how to address the new geopolitical threats. The resulting joint call asked ENISA to support the NIS Cooperation Group (NISCG) in issuing recommendations to improve the resilience of the EU's telecom sector, based on a risk assessment. ENISA is a key player in this process, working closely with DG Connect and the NISCG 5G workstream, bringing to bear its experience in telecom security and 5G.
- Last year, the Council asked the Commission, the European External Action Service (EEAS) and the NISCG to carry out an EU-wide risk posture evaluation and develop risk scenarios with a cross-sector focus, with the support of ENISA.

To handle these unplanned extra tasks, we postponed the kick-off of some projects, recuperating the delays in summer, but this increased the stress levels of the team and would not be sustainable in the long term. In the future, we will need to anticipate some amount of unplanned work to be able to react to unexpected events.

Last year, for SPD Activity 2, ENISA also lacked about 2 FTEs with respect to the original resource planning, due to recruitment difficulties (~ 1.5 FTEs) and the need to support the ENISA cybersecurity support action with experts normally working on SPD Activity 2 (~ 0.5 FTEs). To accommodate this lack of resources, we reduced the sectoral activities for the NISD sectors maritime (~ 1 FTE), aviation (~ 0.5 FTE) and finance (~ 0.5 FTE), in line with the NIS strategy adopted in June. In the future, a model with payable services could be considered for the sectoral activities.

Resources

The high level of satisfaction expressed by stakeholders – with this activity scoring highest of all SPD activities, with 94 % satisfaction overall (breakdown: added value, 93 %; low duplication, 87 %; take-up, 90 %) – combined with the growing demands from the stakeholders, justifies an increase in resources for this activity from the level in 2022 (+ 3 FTEs). The breakdown of the increase in demand is as follows.

- NISD2 has now been adopted and there are important horizontal NISD2 tasks ENISA needs to carry out. For example, ENISA has to build up the EU registry for digital infrastructure providers. In addition, there is a need to support the Commission in updating the (horizontal) security requirements under the NISD (+ 1.5 FTEs).
- The work programme and the number of work streams under the NISCG are growing. Last year, ENISA was supporting 10 NISCG work streams. Since then some work streams have been closed, but also several new work streams have been created. Last year, the Commission also asked ENISA to take over the role of secretariat for six work streams (+ 0.5 FTE, + EUR 50 000).
- In addition to NISD2, there are several sectoral and thematic policy files that entered the implementation phase last year, such as DORA, the Network Code for cross-border electricity flows and the Commission recommendation on European Digital Identity Wallets. ENISA will need to provide support to ensure harmonisation and alignment between these 'transversal' and sectoral policy files and the horizontal NISD (+ 1 FTE).
- It is estimated that approximately 1 FTE is used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

It is a major challenge for ENISA to recruit and retain talented, senior cybersecurity experts with the necessary holistic policy and technical expertise (SNEs or posts at the levels of AD6–8). Supporting Member States with the implementation of policy files, such as the 5G toolbox, requires senior experts with both diplomatic and analytical skills.

Under NISD2, there are more sectors in scope, but in the short term the agency will focus on the horizontal NISD2 tasks, while the sectoral work will be limited to the main NISD sectors, in line with the NIS strategy. This approach will be re-evaluated every year using a specific project named "NIS360", which assesses the criticality and maturity of the NISD2 sectors across the board.

The overall budgetary needs for this activity are expected to remain stable because outsourcing is not a good option for policy implementation work and because we can now use the new Athens premises for working meetings with Member States.

Overall assessment

- The adoption of NISD2 in 2022 was a good moment to look back and take stock of the success of the NISD and the impact achieved by ENISA in supporting policy implementation across the Union. The NISD has helped the EU Member States improve their national capabilities, and it established a structured collaboration between Member States in the NISCG, for strategic matters, and in the computer security incident response team (CSIRT) network, for technical matters. With ENISA's support across all work streams, the NISCG has become a well-functioning platform for collaboration between EU Member States. The role of ENISA in supporting policy implementation continues to grow, and this evolution is also visible in NISD2, where, compared with the NISD, ENISA has many new tasks.
- NISD2 provides an important opportunity for consolidation and streamlining. Before, under the NISD, the policy landscape was rather fragmented, with major areas such as telecoms (EECC) and the eIDAS regulation outside the NISD and outside the NISCG.
- Outside the NISD/NISD2, ENISA has become a key technical advisor in the European Digital Identity Wallet toolbox process, developing the security functions and requirements for the EU's digital wallets. The area of privacy and data protection is maturing and ENISA has now established a collaboration with European Data Protection Supervisor, the European Data Protection Board and the Commission, focusing on how cybersecurity techniques can support personal data protection engineering.

There are several challenges for ENISA to address in policy implementation.

- One of the key issues for NISD implementation has been a lack of harmonisation across the EU, resulting in a fragmented policy landscape. NISD2, adopted in 2022, is now in place and aims to address this issue, among other things. To achieve harmonisation, ENISA will support the Commission early on in the drafting of the implementing rules on security measures and incident reporting, and with the development of technical frameworks that address practical needs. This work is currently under way.
- Under NISD2, the number of sectors in scope has doubled. NISD2 also introduces several new horizontal tasks for ENISA, such as the EU register for digital entities, which have to be delivered on time. This means there is a need to prioritise and streamline the use of ENISA resources. To achieve this, last year ENISA developed and adopted an NIS strategy (see output 2.1).
- In addition, there are now several sectoral and thematic cybersecurity initiatives outside the NISD (e.g. DORA, the Electricity Network Code, the aviation horizontal rule, digital identity wallets) that have entered the implementation phase. To ensure alignment and consistency with the horizontal security requirements, ENISA will have to support stakeholders with the implementation of these transversal policy files.

Looking ahead to next year's SPD, ENISA will make several changes to the structure of this activity and the underlying outputs.

- In last year's SPD, horizontal and sectoral NISD implementation were bundled into one output (output 2.1). For 2023, the structure of ENISA activities and SPD outputs will be aligned with the NIS strategy, separating horizontal activities from sectoral activities.
- In the upcoming NISD2 transposition phase, there are many urgent horizontal tasks that have to be tackled in time, such as the EU registry for digital entities and the delivery of a new framework for security measures under NISD2. Next year, following the ENISA Management Board decision adopting the NIS strategy, ENISA will prioritise the horizontal aspects of NISD2.

Finally, there is room for consolidation of SPD outputs. The area of CVD policies (SPD output 2.4) is now an NISD2 task and can be bundled with the other horizontal NISD2 tasks. The work on the 5G toolbox (SPD output 2.2) has been followed up by other (similar) EU-wide risk assessments (i.e. the Nevers process and the Council risk posture process) and can be bundled with these other risk assessments under one output.

Objectives



- Consistent development of sectoral Union policies with horizontal Union policy to avoid implementation inconsistencies
- Contribution to the efficient and effective monitoring of EU cybersecurity policy implementation in Member State
- Effective implementation of cybersecurity policy across the Union and aiming to support consistency of Member State laws, regulations and administrative provisions related to cybersecurity
- Improved cybersecurity practices, taking on board lessons learned from incident reports

Link to strategic objective (ENISA strategy)



- Cybersecurity as an integral part of EU policies
- Empowered and engaged communities across the cybersecurity ecosystem

Results



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

Outputs



- 2.1.** Support the NISCG and work streams as per NISCG work programme and sectors under the NISD

Outcome



- Last year, ENISA supported the NISCG and was an active member of 10 NISCG work streams. To streamline the work on NIS implementation and to prepare for the implementation of NISD2, ENISA developed an NIS strategy, in consultation with the relevant stakeholders. The strategy contains horizontal and sectoral activities. A key element of the strategy is NIS sector packages targeting NIS sectors based on their maturity and criticality. The package contains services from several ENISA SPD activities, for instance awareness-raising campaigns (SPD Activity 9) and cyberexercises (SPD Activity 3). A yearly project named "NIS360", evaluating all NIS sectors, will be used to calibrate the strategy from year to year, and to give timely input to the ENISA and NISCG work plans.

ENISA supported the sectoral implementation of the NISD in six critical sectors.

- Digital infrastructures. ENISA actively supported NISCG work stream 10 on digital infrastructures by developing a technical paper on identity verification of domain name owners, preparing the ground for the NISD2 task on Whois, and a report about the content delivery networks, a new subsector under NISD2. ENISA also supported the drafting of a new NISCG technical guideline on security measures for domain name system service providers.

- Energy. ENISA supported NISCG work stream 8 on energy with several activities, including the exchange of technical knowledge on ransomware, the provision of bimonthly sectoral threat reports, and a sector-specific online awareness-raising campaign in collaboration with the ENTSO-E cybersecurity subgroup. ENISA also actively supports and contributes to the European Energy Information Sharing and Analysis Centre (ISAC).
- Health. ENISA actively supported NISCG work stream 12 on health by providing technical expertise on the preparation of a sectoral threat landscape, and by organising a capacity-building exercise for the health sector. ENISA actively contributed to the work of the European Health ISAC, revitalising and supporting the formal establishment of this group in 2022. ENISA also organised the 7th eHealth Security Conference in collaboration with the Danish Health Data Authority, bringing the community together to discuss policy developments in the sector, and the evolving threat landscape.
- Rail. ENISA and ERA co-organised the second ERA-ENISA conference on cybersecurity in railways, bringing together stakeholders from the EU railway sector to discuss developments and good practices in railway cybersecurity. ENISA has advised ERA on the technical specifications for the European train control system. ENISA also contributed to the activities of the Expert Group on Land Transport Security's Working Party on Rail Security, which are organised by DG Mobility and Transport.
- Maritime. ENISA organised the 2nd ENISA Maritime Cybersecurity Conference in collaboration with the European Maritime Safety Agency, bringing together sectoral stakeholders to discuss policy developments and the evolving maritime threat landscape. ENISA also contributed to the activities of the European Maritime ISAC, and provided technical input to the port cybersecurity guidelines developed by DG Mobility and Transport and to the action plan of the EU maritime security strategy developed by DG Maritime Affairs and Fisheries.
- Aviation. In the aviation sector, ENISA is working closely with Member States, DG CONNECT, DG Mobility and Transport, and EASA, bringing periodic situational awareness updates to the Aviation Cybersecurity Working Group. ENISA continued its participation in the European Strategic Coordination Platform. ENISA has strengthened its cooperation with EASA: EASA joined the ENISA Transport Resilience and Security Expert Group and provided contributions to the ENISA transport threat landscape report for 2022. ENISA gives EASA technical advice on topics such as incident reporting, awareness raising and ISACs.
- The work under this output had resources of 2.75 FTEs and EUR 185 000.

2.2. Support Member States and the Commission in the implementation and monitoring of the 5G cybersecurity toolbox and its individual actions

Last year, ENISA continued its support of the NISCG 5G work stream and the implementation of the 5G toolbox.

- ENISA supported the 5G work stream in drafting the technical parts of the Report on the Cybersecurity of Open RAN. Industry experts refer to this report as the most comprehensive overview of open radio access network cybersecurity opportunities and risks. ENISA assisted the Commission and the EU Member States with the progress reporting about the implementation of the 5G toolbox. ENISA also organised a greatly appreciated technical training session on 5G security for national authorities to build up their knowledge of 5G networks.
- ENISA continued its work on the 5G matrix, a repository of security controls for 5G networks, which began in 2021. Last year, ENISA conducted a pilot with national authorities and EU telecom operators. The 5G matrix continues to receive positive feedback, not only from national authorities, ministries and agencies that need to supervise 5G networks, but also from operators who are seeking to comply with the requirements of the EU's telecom legislation and the EU's 5G toolbox. In 2022, ENISA also carried out a broad industry consultation on the 5G matrix. The 5G matrix will be published in 2023.
- ENISA delivered a report on fog and edge computing in 5G, which are new technologies used in 5G networks, to inform national authorities about the future of 5G networks and the cybersecurity challenges expected.
- The work under this output had resources of 2 FTEs and EUR 80 000.

2.3. Provide advice, issue technical guidelines and facilitate exchange of good practices to support Member States and the European Commission on the implementation of cybersecurity policies, in particular those on electronic ID and the trust services framework, the EEC and its implementing acts, and security measures for data protection and privacy

In the area of trust services and digital identity, ENISA achieved the following.

- ENISA supported the European Digital Identity Wallet process, as a technical advisor, participating in the weekly wallet toolbox meetings; giving input on cybersecurity risks and security measures for digital wallets; developing an ENISA framework that describes assets, threats and security functions for digital identity wallets; and developing a framework of security recommendations for wallet providers, fulfilling a request by the Commission's European blockchain services infrastructure project.
- ENISA continued its support for the implementation of the cybersecurity parts of the eIDAS regulation by supporting the EU's supervisory bodies for trust services, organising two physical meetings of the ENISA European Competent Authorities for Trust Services Expert Group (formerly known as the ENISA Article 19 Expert Group), analysing the cybersecurity challenges of cloud adoption by eIDAS regulation trust service providers, and organising a technical training on wireless technology and near field communication for smart card authentication.

- ENISA also supported industry collaboration and the development of industry good practices in the area of trust services by organising the eighth edition of the Trust Services Forum in Berlin (attracting more than 1 000 online participants), and by organising a joint ENISA and European Telecommunications Standards Institute (ETSI) workshop on remote identity proofing in Munich, discussing deepfakes and adversarial attacks on machine learning models.

In the area of electronic communications, ENISA achieved the following.

- ENISA supported the collaboration and exchange of good practices between national telecom security authorities as part of the ENISA European Competent Authorities for Secure Electronic Communication Expert Group (three physical meetings), and supported dialogue with the industry by organising the 2nd ENISA Telecom Security Forum in Brussels.
- ENISA helped national authorities build up technical knowledge on new issues and challenges, with technical deep dives on fixed line networks, resilience of subsea cables and security of embedded SIMs, and a deep dive on security issues with the signalling security (SS7) protocol. The embedded SIMs security technical paper and the paper on subsea cable security are to be published, whereas the signalling security deep dive resulted in an internal checklist, which is shared only with national authorities.

In the area of data protection and privacy, ENISA achieved the following.

- ENISA established a structured collaboration with the European Data Protection Supervisor, analysed data protection engineering considerations regarding personal data sharing in a dedicated workshop with experts, published a report on privacy for data spaces, supported dialogue and collaboration within the EU data protection community by organising the 10th edition of the Annual Privacy Forum in Warsaw, and supported the Union's policy implementation in the area of AI and data protection by performing a privacy analysis, available in the ENISA publication on cybersecurity and privacy in AI.
- The work under this output had resources of 4 FTEs and EUR 430 000.

2.4. Assisting in establishing and implementing vulnerability disclosure policies, also considering the NISD2 proposal

Last year, ENISA also worked closely with the NISCG and the Member States to support the development and implementation of national CVD policies across the EU.

- Within the NIS Cooperation group workstream, ENISA played a central role in the taskforce on vulnerability disclosure policies. In this taskforce ENISA leads the drafting of a technical NISCG guideline on how to implement national CVD policies
- ENISA published a report on industry expectations of national CVD policies, as well as addressing legal, technical and collaboration challenges in the implementation of national CVD policies in the EU Member States.
- ENISA has been using the NISCG meetings on CVD policies to also collect feedback on the expectations and needs surrounding the future EU vulnerability database, a new task for ENISA under NISD2, which will be addressed under Activity 4 in the 2023 SPD.
- The work under this output had resources of 1 FTE and EUR 85 000.

Key performance indicators: Contribution to policy implementation and implementation monitoring at EU and national levels (ex post)		Unit (of measurement)	Frequency	Data source	2021 results	2022 results
2.1. Number of EU policies and regulations implemented at national level supported by ENISA		Number	Annual	Manual collection from staff members	5	5
2.2. Number of ENISA reports, analyses and/or studies referred to at EU and national levels		Number	Biennial	Survey	N/A	65
2.3. Satisfaction with ENISA added value of support (survey)		%	Biennial	Survey	N/A	94 %
% of stakeholders rating outcome/result of ENISA work as high or some added value		%	Biennial	Survey	N/A	93 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities		%	Biennial	Survey	N/A	87 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term		%	Biennial	Survey	N/A	90 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work		%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA		%	Biennial	Survey	N/A	97 %
% of stakeholders satisfied with ENISA's community-building actions		%	Biennial	Survey	N/A	93 %
Linear adjustment to allow benchmarking with the allocated FTEs based on the full establishment plan at 2022 year end	12	Actual used FTEs		9.75		
Planned budget (direct costs only)	EUR 798 475	Consumed budget (direct costs only)		EUR 780 925		
		Of which carried over to 2023		EUR 1 700		

ACTIVITY 3

Building capacity



In 2022, under this activity ENISA continued contributing to the aim of enhancing capabilities of Member States, EU institutions, bodies and agencies (EUIBAs), and sectoral stakeholders, while boosting effective cooperation within the EU.

Achievements

Throughout the year, several key achievements have significantly contributed to the enhancement of the cybersecurity capabilities of our key stakeholders and brought us closer to the overall strategic objective that drives our capacity-building efforts. Cyber Europe 2022, originally planned as Cyber Europe 2020, successfully simulated a major crisis in the EU healthcare sector, enabling stakeholders from Member States and other participants to extensively test and evaluate their business continuity plans and crisis management procedures. The exercise had 918 participants from the EU, European Free Trade Association (EFTA) countries and various EU institutions, and facilitated valuable discussions, knowledge exchange and future collaboration opportunities. The feedback received confirmed that Cyber Europe 2022 was a success, and identified crucial areas for improvement.

Moreover, the 2022 European Cybersecurity Challenge (ECSC) final saw expanded participation from accession candidate countries and teams from outside Europe. Enhancements in competition content, such as defending against attacks and social engineering challenges, provided valuable lessons for improving future events even further. Building on the ECSC's success, ENISA, in collaboration with regional and international organisations, organised and hosted the inaugural International Cybersecurity Challenge (ICC). Attended by seven regional teams comprising 64 nations and 105 capture-the-flag (CTF) players, the event fostered collaboration between diverse regions and promoted the European principle of a cybersecure society worldwide.

The establishment of a steering committee with organisations from over 70 countries ensures the continuation of the ICC in 2023 and beyond. As ICC aims to attract young talent and raise global awareness of the necessary education and skills in cybersecurity, the initiative has already enabled capacity building in regions struggling to develop cybersecurity expertise.

In the area of training, we further implemented our strategy by organising training events that target attendees with similar knowledge and expertise levels, but possibly with different backgrounds, fostering information and experience sharing between them. At the beginning of the last quarter, 20 participants from Member States and EUIBAs attended a successful training session on information security management in Budapest. A week-long training event in the ENISA offices in Heraklion was organised in the autumn; this event made optimal use of the attendees being on-site together with the trainers, encouraging very useful interactions between experts and attendees with different backgrounds. The event had 25 participants who attended a 2-day workshop-style tactical training session on the zero-trust concept, and 13 participants who attended a very advanced technical training session on incident response in a compromised network environment. Because of the positive response to the training event and the useful feedback, this will become an annual event.

Finally, in September 2022, the European cybersecurity skills framework (ECSF) was presented during the first cybersecurity skills conference, which took place a few days after the declaration by the President of the European Commission that 2023 was the 'Year for Skills', one more tool for upskilling professionals in cybersecurity.

In summary, the year's achievements have brought us closer to the overall strategic objective of strengthening cybersecurity resilience and fostering international collaboration.

Resources

Work planned under Activity 3 was duly fulfilled: the budget was implemented as planned with almost total accuracy, reaching 99.99 % commitment by the end of the year, from which a reasonable and justified 17 % was carried over to 2023; the carried-over amount relates to activities performed to ensure the development of the exercise and training platforms, and the ongoing preparation and training of Team Europe for the 2023 ICC.

In terms of human resources, the unit managed to carry out all the activities, despite having fewer actual resources than estimated (a delta of almost 3 FTEs) due to the contribution of the unit members to horizontal teams; through such contributions, we managed to streamline synergies, maximising collaboration within the unit and throughout ENISA. This included contributions to the cybersecurity support action that amounted to approximately 0.45 FTEs. The expectations for the future are to make up for this shortage in resources by filling the two vacant posts the unit has, although the commitment of the unit members to the horizontal teams and related synergies remains high.

In the areas of cyberexercises and training during 2022, more senior staff members were added to the team in an effort to reinforce the quality of services offered to Member States. At the same time, in 2022 the team working on the national cybersecurity strategies (NCSSs) was reinforced by the addition of a new manager as a team member.

Finally, in the area of cyberexercises and training, in order to cater to ENISA stakeholders' requirements, the activity moved part of the implementation of the new ENISA strategy into this area in 2023. In this way, the area was sufficiently resourced to support stakeholders.

It is estimated that approximately 0.75 FTEs are used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

Overall assessment

This has been undoubtedly a prominent year for capacity-building activities; throughout 2022, Activity 3 has successfully contributed to the strategic objectives on cutting-edge competences and capabilities in cybersecurity across the EU, empowering and engaging with communities across the cybersecurity ecosystem through various and diverse lines of action. We have launched our new training and exercise strategy, which allows us to focus on specific stakeholders while putting more emphasis on linking specific training and exercise events with better-defined medium- and long-term goals for building capacity. We have organised and successfully conducted five exercises, among them being our sixth pan-European exercise, and expertly organised the fifth ECSC, which is the biggest competition of its kind worldwide. On top of that, the ICC was inaugurated, with ENISA co-hosting the event, showing once more the continued commitment ENISA has to identifying and developing young cybersecurity talent in Europe, and promoting collaboration and networking within the global cybersecurity community. As shown by the KPI values, the maturity of NCSSs has significantly improved, the usefulness, added value and relevance of ENISA's capacity-building activities, which are positively assessed by our stakeholders, and the participation and number of cybersecurity programmes is steadily increasing. Finally, valuable tools for the imminent priorities of EU Member States have been produced, and significant guidance on topics of high interest with a view to NISD2 has been provided.

We strongly believe that the course set by the newly defined strategies in terms of training, exercises, NCSS services, the recognised establishment of the ICC and the technological enhancements implemented for the ECSC will lead to further successes in building capacity throughout the EU.

Objectives



- Increase the level of preparedness and cooperation within and between Member States, sectors and EUIBAs
- 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
- Increase the supply of skilled professionals to meet market demand, and promote cybersecurity education

Link to strategic objective (ENISA strategy)



- Cutting-edge competences and capabilities in cybersecurity across the EU
- Empowered and engaged communities across the cybersecurity ecosystem

Results



- Enhanced capabilities across the community
- Increased cooperation between communities

Outputs



3.1. Assist Member States in developing national cybersecurity strategies

Outcome



Regarding the work in assisting Member States to develop, implement and evaluate their NCSSs, the following activities were carried out during the year:

- ENISA produced a report emphasising best practices related to building effective governance frameworks for the implementation of NCSSs (<https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies>). Moreover, an additional statistical outline was published to give an overview of the key findings of the study, link them with the main elements of the proposed governance framework and support them by sharing insightful statistics (<https://www.enisa.europa.eu/publications/a-governance-framework-for-national-cybersecurity-strategies>).
- ENISA upgraded the NCSS interactive map to include new features, including statistics of the adopted objectives included in the strategies of the Member States, and a timeline of NCSS publications. The map was also updated with information on NCSSs recently published by the Member States and their adopted objectives (<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>).

- ENISA developed an online tool to support the assessment of the maturity of small and medium-sized enterprises (SMEs), helping them understand their cybersecurity maturity level and providing them with an adaptive progressive enhancement plan to handle cyber risk and improve their cybersecurity posture (<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/>).
- ENISA organised the annual NCSS workshop, which took place online on 14 November 2022 and served as a kick-off for the newly established national liaison officer (NLO) subgroup on NCSS. ENISA presented and validated the year's work, and Italy had the opportunity to present its recently published national cybersecurity strategy.

In the area of NCSSs, all objectives were met in 2022, and a new vision was developed for the evolution of this area. For 2023, the aim is to launch and start refining the recently defined services catalogue, including the iterative process of reviewing and improving the NCSS map, and use it to respond to the needs of the increased tasks for ENISA and the Member States defined in NISD2, and other capacity-building needs identified. Collaboration with the cybersecurity index project remains crucial for the topic of maturity assessments, and coordination between different stakeholder forums will be ensured (namely the NLO subgroup on NCSS and NISCG work stream 9).

Outputs



- 3.2.** Organise large-scale biennial exercises and sectoral exercises (including Cyber Europe, blueprint operational level exercise (BlueOLEx), cyber standard operating practice exercise, etc.), including through cyber ranges

Outcome



The exercises team of the agency organised or co-organised the following exercises during the reporting period.

- Cyber Europe 2022. The scenario revolved around healthcare and included national/governmental CSIRTs, cybersecurity authorities, ministries of health, healthcare organisations (e.g. hospitals/clinics), eHealth service providers, internet service providers and health insurance providers. The incidents built up into a major crisis at all levels: local, organisational, national and European. Business continuity plans and crisis management procedures were put to the test.
- Western Balkans tabletop exercise (WEBEx). WEBEx was a significant initiative aimed at fostering greater cooperation between the western Balkan nations and the EU. WEBEx focused on enhancing situational awareness; promoting information sharing, understanding of EU initiatives and tools related to cybercrises; and identifying potential synergies within the region. It also served as a crucial platform for strengthening ties and building collective resilience. By empowering participants through training and collaboration, the exercise, using a fictional energy-sector cybercrisis, played an essential role in fortifying the region's defences against cyber threats and further integrating the western Balkans into the broader European cybersecurity framework.

- EU cybercrisis-linking exercise on solidarity (EU Cycles). EU Cycles was a tabletop exercise at EU level, organised by the French Presidency of the Council of the European Union with the support of ENISA. It involved a fictitious cyberattack against an EU Member State. The action led to a draft defence strategy against massive cyberattacks and a calendar for operational exercises at EU level, which involves all actors involved in security operations.
- 2022 BlueOLEx. The aim of this exercise was to test the European Cyber Crisis Liaison Network (EU-CyCLONe) standard operating procedures (SOPs), focusing on EU-CyCLONe's decision-making and internal communication at executive level. This was co-organised and conducted by ENISA.
- 2022 Jasper. This was the first joint awareness and preparedness cyberexercise of its kind, organised by ENISA in collaboration with the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU). Based on the lessons learned from post-incident analysis and the need for elevated awareness of the evolving threats that affect EUIBAs, CERT-EU and ENISA joined forces to create a focused exercise to test preparedness and awareness.
- The European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) corporate information technology (IT) exercise for 2022. The objective of this was to validate the security policies and procedures of the business continuity policies, business continuity plans and disaster recovery plans applicable to corporate IT infrastructure. It also intended to identify gaps in the coordination and communication taking place among the different stakeholders concerned in the event of a crisis. ENISA was involved in supporting the exercise preparation and providing the cyberexercise platform.

The main achievements in this area in 2022 were:

- the execution and closure of Cyber Europe 2022, with the publication of the after-action report containing valuable conclusions for all participants (<https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report>);
- implementation of a new ENISA strategy on exercises and training courses, meeting the requirements of the Cybersecurity Act (CSA);
- the successful launch of a new set of exercises (Jasper), aimed at the EUIBAs and potentially Member States, in collaboration with CERT-EU.

At the same time, the Exercises Team also started the necessary preparatory work for switching to the new cyberexercise platform in 2023. Stakeholders from Member States and EUIBAs were involved from an early stage to provide input on their needs, feedback and crucial involvement in the development process.

As provided for by the CSA, ENISA will inform all relevant communities about the new strategies on exercises and training.

3.3. Organise trainings and other activities to support and develop maturity and skills of CSIRTs (including the NIS sectoral CSIRT) and other communities

In early October, a comprehensive training week was held at ENISA's Heraklion facility, offering two specialised courses aimed at enhancing cybersecurity capabilities for participants (including participants from Ukraine). The first course delved into the zero-trust security model, exploring deployment options and providing practical guidance on its implementation within organisations. The second course, focused on defending against adversary actions, was a hands-on technical training session designed for incident responders. The latter emulated the actions of an adversary, showcasing how CSIRTs or incident response teams can effectively employ well-known open-source tools and robust procedures to improve their operational preparedness. Overall, the training week offered a valuable opportunity for participants to expand their knowledge and skills in the ever-evolving realm of cybersecurity. Based on the positive feedback and useful tips for potential improvement, this event will become an annual event and it will aim to take as much advantage as possible of the unique added value of having instructors lead training with trainers and attendees physically present.

In late October, in a collaboration between the European Security and Defence College (ESDC), the University of Public Service and ENISA, a comprehensive course on information security management and ICT security was organised for public employees from EU Member States and EU institutions involved in information security management and risk management. The course was part of the ESDC's cyber education, training, exercise and evaluation platform, and consisted of an asynchronous eLearning segment introducing information security and risk management, followed by a classroom course, focusing on implementing information security management and applying controls to minimise risks. The primary objectives of the course included imparting significant knowledge on implementing an information security management system; reinforcing technical knowledge of cybersecurity through the identification and implementation of technical controls; improving skills in managing risk assessment programmes, and identifying measures necessary to protect information and ICT systems; and providing guidelines and best practices in managing information security policies, analysing critical assets, and identifying threats and vulnerabilities.

ENISA developed a framework for creating a platform dedicated to self-paced online training modules, concentrating primarily on enhancing technical skills and capabilities in cybersecurity. Recognising the critical need for continuous learning in this rapidly evolving field, ENISA's platform has been designed to offer flexible and accessible educational resources that cater to diverse learning needs and schedules. By focusing on technical skills, the platform empowers professionals across various sectors to stay up to date with the latest tools, techniques and best practices in cybersecurity. This innovative approach to education not only helps to build a strong foundation for individuals but also contributes to the overall resilience and security of organisations within the EU. It is also in line with our strategic approach: allowing participants to gather an initial level of knowledge and even skills that prepare them to get the most out of capacity-building events that are taught by trainers and require physical presence.

3.4. Develop coordinated and interoperable risk management frameworks

In 2022, the work performed under the topic of interoperable risk management frameworks was carried out through the following activities.

- An updated Interoperable EU Risk Management Framework report was published, based on new inputs collected by stakeholders, therefore complementing and building on the topic (<https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework>).
- An interoperable EU risk management toolbox was created that aims to facilitate the smooth integration of various risk management methods in an organisation's environment or across organisations, and consequently bridge the gaps associated with various methods. (<https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox>).
- A workshop on the interoperability of the EU risk management toolbox was conducted as a means to present to relevant stakeholders the work done by ENISA in the field of risk management, with a focus on the interoperability of EU risk management frameworks.

The main achievement of 2022 in this area was the transformation of the proposed risk management framework into an interoperable risk management toolbox. Two hands-on workshops were delivered as part of the ENISA training portfolio, focusing on the use of the interoperable risk management toolbox. Output 3.4 was suppressed in the 2023 work programme and in the draft 2024 work programme.

3.5. Support the capacity-building activities of the NISCG and work streams as per the NISCG work programme

In 2022, ENISA has continued to actively support the NISCG work streams in terms of capacity building by performing the following activities.

- ENISA organised a 2-day capacity-building activity, which included a joint non-technical capacity-building subactivity on cyberawareness program development and the use of exercises, for work streams 8 (energy) and 9 (capacity building), with 30 participants from eight different job profiles. In addition, a technical capacity-building activity for work stream 9 was carried out.
- ENISA organised a capacity-building activity for national competent authorities on an introduction to industrial control system cybersecurity; the activity gathered 25 participants from nine sectors and two Member States (Finland and Sweden).

All activities were performed successfully, actively contributing to increasing the level of preparedness and cooperation within and between Member States and sectors.

3.6. Support European information-sharing communities through ISACs based on the core service platform of the Connecting Europe Facility (CEF), and other collaboration mechanisms such as public-private partnerships; support the reinforcement of security operations centres (SOCs) and their collaboration, assisting the Commission and Member State initiatives in this area in line with the objectives of the EU cybersecurity strategy in the building and improving of SOCs ^(a)

In 2022, the work related to ISACs was performed through the following activities.

- An EU ISACs conference was organised, gathering representatives from 14 EU ISACs to further promote the use of the ISACs platform.
- Regarding the ownership of the ISACs platform, a proper handover to ENISA was ensured and successfully performed.
- ENISA supported the creation of two new ISACs – the ISAC for Cities and the Telecom ISAC.

With regard to the work on SOCs, the development of a maturity model for SOCs participating in a network of SOCs, along with the establishment of common practices for cyber threat intelligence (CTI) and a landscape for sharing playbooks, has significantly bolstered cybersecurity efforts. ENISA supported the European Commission in European Cybersecurity Competence Centre (ECCC) meetings by offering valuable insights gleaned from the SOCs community on capacity-building initiatives related to CTI sharing, playbooks and maturity indicators. To facilitate this process, ENISA created three internal reports that informed the DIGITAL-ECCC-2022-CYBER-03-SOC call and presented the results at several ECCC meetings. By providing guidance to countries interested in participating in the call, ENISA has played a crucial role in fostering a more robust and collaborative cybersecurity landscape across the region.

3.7. Organise and support cybersecurity challenges including European Cyber Security Challenge

The 2022 ECSC was held from 13 to 16 September and was attended by 27 EU and EFTA countries, as well as five guest countries (Canada, Israel, Serbia, the United Arab Emirates and the United States). In total, 580 people participated in the event, including contestants, coaches, judges and other personnel. The competition had 330 contestants, of whom 20 were female. The finalists of the 2022 ECSC were from Denmark, Germany and France.

In addition to the main competition, the ECSC also featured OpenECSC, an open online platform that allows anyone to practise and improve their cybersecurity skills by participating in an online 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 Member States as a qualifier platform for their national selection.

During 2022, Team Europe, a European team assembled by ENISA, also participated in the ICC held in Athens in June 2022 and organised by ENISA. The team was composed of 15 participants representing 21 European countries. The ICC is a global cybersecurity competition that brings together teams from different regions to compete in various challenges, and foster collaboration and networking.

Team Europe participated in various training and preparatory activities, including boot camps, online training sessions, public CTF events, CTF qualifiers, side events and other engagements. The team's objectives included training candidates and identifying their profiles, assessing their strengths and weaknesses, organising qualifiers,

building a community, and following up on the assessments to identify recommendations for future activities.

Overall, the 2022 ECSC and Team Europe's participation in the ICC demonstrated a continued commitment to identifying and developing young cybersecurity talent in Europe 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 we used for the organisation of the ICC. The latter will now become an integral part of it. ENISA's objectives regarding the ECSC are to improve the governance structure and future organisation through improvements in decision-making, sponsorship and funding programmes, and support to countries. In addition, ENISA aims to enhance the ECSC competition through additional types of challenges, platforms and OpenECSC, communication channels, and linking to the ENISA cybersecurity skills framework to identify potential market needs. ENISA supported Team Europe's participation in the ICC by assembling a European team, holding boot camps and online qualifiers, and providing training activities for young talent. The emphasis of the ECSC for the next 5 years will be on setting priorities and challenges, while the ICC will focus on establishing a governance structure for the future. In terms of evaluation, the emphasis obviously can no longer be on the number of European countries participating (we have already reached the objective of all EU Member States and EFTA countries participating), so the focus has now shifted to the number of national competitions being organised and the participation in them.

Going forward, the agency could consider resourcing the work under this output using a payable services model.

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

The cybersecurity higher education database provided data on the status of cyber higher education in the EU and EFTA countries, becoming the main point of reference for all citizens looking to upskill their knowledge in the cybersecurity field. The web tool has emerged as the largest updated database of cybersecurity academic programmes in Europe.

The ECSF was released at the first ENISA cybersecurity skills conference. Among the 100 people who attended the event, one could find representatives of public administrations that deal with policies on skills, cybersecurity private organisations interested in building a competent workforce, professional associations, researchers, academics and providers of training programmes.

The ECSF helps in the identification of the critical skills set required from a workforce perspective, which enables learning providers to support the development of this critical skills set, and policymakers to support a targeted initiative to mitigate the skills gap identified.

Two reports that shaped the ECSF were published in 2022.

- the ECSF role profiles document lists the 12 typical cybersecurity professional role profiles, along with their identified titles, missions, tasks, skills, knowledge and competences (<https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>);

- the ECSF *User Manual* provides guidance on and practical examples of how to leverage the framework and benefit from it as an organisation, provider of learning programmes or individual (<https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>).

Output 3.8 has moved under Activity 9 and relabelled as output 9.5 in the 2023 SPD, further information will be reported under Activity 9.

Key performance indicators: Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
3.1. Increase/decrease in maturity indicators ^b					
Maturity of NCSSs					
Number of Member States that rate the overall maturity of their cybersecurity strategy					
High maturity	Number	Annual	Survey	3	6
Medium maturity	Number	Annual	Survey	4	5
Low maturity	Number	Annual	Survey	3	0
Number of Member States planning to use ENISA framework to measure the maturity of their national cybersecurity capabilities					
Already using	Number	Annual	Survey	1	2
Not using but planning to use	Number	Annual	Survey	5	9
Don't know or will not use in the foreseeable future	Number	Annual	Survey	4	2
Number of Member States that have set KPIs to measure progress and effectiveness of the implementation of their strategic objectives when drafting their NCSS					
Already using	Number	Annual	Survey	3	9
Not set but planning to use	Number	Annual	Survey	4	5
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	3	0
The frequency with which Member States update their strategies to adapt to technological advancements and new threats					
Every 2–3 years	Number	Annual	Survey	2	1
Every 4–5 years	Number	Annual	Survey	6	12
More than 6 years or don't know	Number	Annual	Survey	2	1
Sectoral ISACs coverage					
Percentage of NISD2 sectors with an EU ISAC	%	Annual	Report	—	60 %
3.2. Outreach, uptake and application of lessons learned from capability-building activities					
2021 cyber standard operating practice exercise (number of improvements proposed by participants)	Number	Per exercise		5	5

Key performance indicators: Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
3.3. Number of cybersecurity programmes (courses) and participation rates ^c					
Total number of students enrolled in the first year of the academic programmes (2020)	Number	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	4 843	5 205
Student gender distribution (% female: % male)	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	20 %: 80 %	19 %: 81 %
Total number of cybersecurity programmes (2020)	Number	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	119	122
Number of postgraduate programmes	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	6 %	5 %
Number of master's degree programmes	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	77 %	80 %
Number of bachelor's degree programmes	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	17 %	15 %
3.4. Number of exercises executed annually					
Number of exercises executed annually	Number	Annual	Report	5	5
3.5. Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey)					
% of stakeholders rating outcome/ result of ENISA work as high or some added value	%	Biennial	Survey	N/A	97 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	77 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	80 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	96 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	97 %

Key performance indicators: Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
Standard operating practice exercise (SOPEX) series					
Usefulness low	%	Per exercise	Survey	9 %	6 %
Usefulness medium	%	Per exercise	Survey	71 %	54 %
Usefulness high	%	Per exercise	Survey	20 %	40 %
Relevance low	%	Per exercise	Survey	4 %	7 %
Relevance medium	%	Per exercise	Survey	53 %	53 %
Relevance high	%	Per exercise	Survey	43 %	40 %
Cyber Europe exercise series (biannual)					
Usefulness low	%	Per exercise	Survey	—	6 %
Usefulness medium	%	Per exercise	Survey	—	54 %
Usefulness high	%	Per exercise	Survey	—	40 %
Relevance low	%	Per exercise	Survey	—	7 %
Relevance medium	%	Per exercise	Survey	—	53 %
Relevance high	%	Per exercise	Survey	—	40 %
Jasper series					
Data to be made available from 2023	%	Per exercise	Survey	—	—
Allocated FTEs as per SPD based on full establishment at 2022 year end	13		Actual used FTEs	10.32	
Planned budget	EUR 1 921 265		Consumed budget	EUR 1 921 221	
			Of which carried over to 2023	EUR 328 339	

- a In particular (i) continue developing and updating the mapping of the current landscape of SOC in the EU, including public and private, and in-house or as a service; main operators of SOC services in the EU; and (ii) provide other relevant support to the Commission in implementing the SOC-related objectives of the EU cybersecurity strategy (e.g. support the design of calls for expression of interest, procurements, etc. and liaison with stakeholders and research activities).
- b This KPI should be viewed over a number of years. The 2021 KPI establishes the 'baseline' that allows ENISA to gauge the evolution of the corresponding maturity indicator in the coming years.
- c This KPI should be viewed over a period of a number of years. The 2021 KPI establishes the 'baseline' that allows ENISA to gauge the evolution of the corresponding maturity indicator in the coming years. As of 2023, this KPI will be moved under Activity 9.

ACTIVITY 4

Enabling operational cooperation



Under Activity 4, ENISA supports operational cooperation among Member States and EU institutions, bodies, offices and agencies. It aims to establish synergies with the different national cybersecurity communities (including civilian, law enforcement, cyber diplomacy and cyber defence) and EU actors – notably CERT-EU – with a view to exchanging know-how and best practices, providing advice and issuing guidance.

Within the scope of this activity, the agency supported the operations of the CSIRTs network and EU-CyCLONe during a challenging year, given the overall escalation of cybersecurity-related incidents connected to the Russian war of aggression against Ukraine, which started in February at the borders of the EU. It should be noted that the year began with the CSIRTs network operating in escalated mode due to log4j (<https://www.enisa.europa.eu/news/enisa-news/log4j-vulnerability-update-from-the-csirts-network>); and the network further escalated to monitor activity after the initiation of the Russian war of aggression against Ukraine. The agency executed the planned tasks that are covered below to support the daily operations of the EU's incident response and crisis management networks, while it also took up unplanned, new and unexpected activities triggered by the Russian war of aggression against Ukraine. ENISA was able to demonstrate its ability, as an organisation, to react to and address unforeseen challenges during cybercrises.

Achievements

ENISA supported the functioning of the CSIRTs network and EU-CyCLONe, in terms of providing the secretariat function and infrastructure, tools and communication channels. 2022 was an exceptional year when, on top of business as usual, during the escalation to the CSIRTs network, the secretariat hosted over 20 coordination calls and created executive summaries, created summaries for EU-CyCLONe and shared over 70 situational awareness reports on relevant matters, supported a doubling in the information exchanged and enabled incident response in the EU.

In addition, ENISA facilitated improved exchange of information among cybercrisis management authorities in the EU via high-level meetings, secure communications channels, portals, dashboards and mailing lists for EU-CyCLONe.

In June 2022, both the CSIRTs network and EU-CyCLONe participated for the first time in Cyber Europe. This allowed the testing of the updated EU-CyCLONe and CSIRTs network SOPs, and EU Member States' reaction and escalation challenges. The results and findings from the exercise were translated into the working documents of the networks and associated tools.

In November 2022, during BlueOLEx, the EU-CyCLONe Executives exercise was organised in Vilnius by the Lithuanian Ministry of National Defence together with ENISA and with the support of the Czech Presidency of the Council of the European Union. The exercise tested the SOPs of the EU-CyCLONe Executives, including the support from ENISA. The exercise focused on the horizontal interaction between Member States and EUIBAs, and was performed in light of the then upcoming implementation of NISD2.

Regarding the cooperation with other EUIBAs and relevant blueprint stakeholders, ENISA developed a maturity framework for EU cybercrisis management stakeholders and continued the work regarding the memorandum of understanding (MoU) with the European Defence Agency (EDA), the European Cybercrime Centre (EC3) of the European Union Agency for Law Enforcement Cooperation (Europol) and CERT-EU. The preparatory work for an endorsed set of SOPs between the EUIBAs dealing with cybercrisis management was completed, but these SOPs were not endorsed by all. The agency also hosted the Council Horizontal Working Party on Cyber Issues in order to discuss ENISA's mandate and strategy, and, more specifically, operational cooperation, NISD2 and certification.

During 2022, ENISA supported and maintained the tools and services that it provides to its operational stakeholders, and proceeded with developing additional features. In particular, it enabled the CSIRTs network to host the Melicertes 2 portfolio, and provided infrastructure and tools for EU-CyCLONe.

ENISA also onboarded new tools such as the ISACs platform, for which a dedicated plan was developed in order to mitigate some limitations in security and monitoring. In delivering its work, ENISA set the baseline security measures for all operational cooperation tools, following international standards and complying with ENISA's internal policies and IT strategy.

Resources

The resource needs for enabling operational cooperation have been growing over the past few years, alongside the growing needs to support the operations of the CSIRTs network and EU-CyCLONe, develop incident response and crisis management, and maintain and operate the operational tools and platforms.

2022 was a test year for the agency, as it was by no means business as usual. While the agency is quite experienced in providing the secretariat function under output 4.1 and planned enough resources to provide the daily support for the operational networks, it lacked the operational reserves to absorb the increased demand for services due to cybersecurity escalations and the take-up of the cybersecurity support action. This had the side effect that some projects were done in a more lightweight fashion, for example the study on CSIRT / law enforcement agency cooperation, but also that ENISA's support, for example in the working groups of the CSIRTs network, was of lower quality than what the stakeholders are used to receiving from ENISA in this area.

Output 4.2 operated in a challenging environment, as things changed rapidly at EUIBA level, for example through the creation of the Interinstitutional Task Force. This, combined with the fact that resources were stretched too thin to be able to cope with this challenge, meant that the output partially failed to achieve its ultimate goal, which was to have an endorsed set of EUIBA SOPs in place. In 2023, this output is absorbed by output 4.1, allowing it to tap into a bigger pool of talent to deal with these topics.

Output 4.3 also suffered from the shifting of resources to the cybersecurity support action. The initial resources planned were deemed not to be enough to cover the large portfolio of infrastructures and tools for which the Operational Cooperation Unit is responsible. This is a critical risk for the agency. In 2024, this output should be reinforced, namely in terms of human resources, as many of these activities cannot be outsourced due to their sensitive nature. In parallel, the agency should try to seek synergies between corporate IT and operational IT.

It should be noted that stress levels were high throughout the whole year, with staff performing overtime, cancelling holidays over the summer and completing voluntary weekend work. The workload was very high and this continued the whole year, so the activity was affected by the loss of 4 FTEs from mid 2022. This is not sustainable and the agency should be able to build up operational reserves to deal with escalations.

It is estimated that approximately 0.75 FTEs are used by its operational human resources to perform technical/ corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

Overall assessment

The role of the secretariat in the networks is defined by Article 7 of the CSA and Articles 15 and 16 of NISD2, and the secretariat aims to fulfil the objective of strategic objective SO3: 'effective cooperation amongst operational actors within the Union in case of massive cyber incident'. Both networks continuously (24/7) share data and information related to cybersecurity incidents and crises that could affect the Union's digital economy and society. The added value of ENISA is that it supports these networks with timely responses, information sharing, and situational awareness during incidents and crises, and does this as a trusted partner vis-à-vis its members, as acknowledged by the feedback received in its stakeholder survey (8.5 out of 10) ^(a). This forms the basis for mutual trust, which is a core tenet of effective cooperation during escalation, but also in everyday operations. Five operational cooperation SNEs joined ENISA during the course of 2022, which helped to further align the agency's efforts with Member States' needs.

Positive feedback from the CSIRTs network, EU-CyCLONe, the Horizontal Working Party on Cyber Issues, EUIBAs and CSIRT law enforcement was received by ENISA in the course of 2022. Based on the results of the survey of the networks, ENISA took actions to address all comments and also noted the very positive feedback received about ENISA's work. In the survey, 78 % of the CSIRTs network members self-assessed their participation in the network as 8/10 and evaluated the ENISA secretariat team's performance as 8/10. At the same time, for EU-CyCLONe, 81 % of the EU Member States – 22 Member States (out of 27) – self-assessed their participation in the network as 8/10 and evaluated the ENISA secretariat team's performance as 9/10.

The positive and constructive feedback confirms the maturity of ENISA in enabling operational cooperation. Going forward, this activity will require additional human resources to be able to deliver further success in this field, maintain the service in times of escalation, and operate and maintain the infrastructures and tools in a secure and sound manner. Furthermore, there is an increasing need to provide 24/7 support for incidents; current resources are insufficient for the agency to be able to deliver this in a sustainable manner.

Objectives



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

Link to strategic objective (ENISA strategy)



- Effective cooperation among operational actors within the EU in case of massive cyberincidents
- Empowered and engaged communities across the cybersecurity ecosystem

Results



- All communities (EU institutions and Member States) use rationalised and coherent set of SOPs for cybercrisis management
- Efficient framework, tools (secure and high availability) and methodologies for effective cybercrisis management

Outputs



- 4.1.** Support the functioning and operations of the CSIRTs network (also through Melicertes), EU-CyCLONE, the Joint Cyber Unit (JCU), SOCs network (b) and with relevant Blueprint stakeholders (e.g. Europol, CERT-EU, EEAS and EDA)

Outcome



Incident response in the EU

ENISA supported the escalation of the CSIRTs network in reaction to the Russian war of aggression against Ukraine in the first 6 months of 2022 through:

- 20 coordination calls,
- executive summaries and summaries for EU-CyCLONE,
- 70 situational awareness reports on relevant matters.

Despite the geopolitical situation and lack of resources in the first part of the year, and the allocation of output 4.1 resources for the cybersecurity support action in the second part of the year, both the CSIRTs network and EU-CyCLONE ran as usual, albeit with a reduced level of services. This resulted in:

- the 16th CSIRTs network meeting – 28 February to 1 March (online),
- the 17th CSIRTs network meeting – 16–17 May, Paris, under the French Presidency of the Council of the European Union,

- the 18th CSIRTs network meeting – 21–23 September, Brno, under the Czech Presidency of the Council of the European Union,
- the 11th ENISA–EC3 workshop on CSIRT and law enforcement cooperation, 28–29 September 2022, Heraklion,
- two dedicated studies, only available to CSIRTs network members, on preparation for NISD2 implementation and on workforce exhaustion,
- a report on CSIRT and law enforcement cooperation, which covers all Member States and Norway and addresses the legal and organisational framework, roles and duties of CSIRTs, law enforcement agencies and the judiciary.

Crisis management in the EU

For EU-CyCLONe, under the French Presidency of the Council of the European Union, ENISA supported:

- an EU Cycles exercise,
- the 6th EU-CyCLONe Officers meeting – Brussels, moved to physical due to Russian war of aggression against Ukraine,
- an executive summary provided to the Horizontal Working Party on Cyber Issues,
- the 7th EU-CyCLONe Officers meeting – 18 May, Paris,
- the 1st EU-CyCLONe Executive meeting – 19 May, Paris.

Under the Czech Presidency of the Council of the European Union, ENISA supported:

- the 8th EU-CyCLONe Officers meeting – 22–23 September, Brno,
- the 9th EU-CyCLONe Officers meeting – 22 November, Brussels,
- two dedicated EU-CyCLONe studies, only for EU-CyCLONe members, on information flow and on cybercrisis management frameworks,
- the EU-CyCLONe SOP update,
- continuous improvement of the EU-CyCLONe tools.

Joint response

ENISA supported:

- Cyber Europe – June,
- BlueOLEx's EU-CyCLONe Executives exercise – November.

Cooperation with EUIBAs

ENISA supported:

- the maturity framework for EU cyber crisis management stakeholders – EUIBAs,
- the MoU with EDA, EC3 and CERT-EU,
- the visit of the Council Horizontal Working Party on Cyber Issues to ENISA headquarters – 11 November, Athens.

It should be noted that, even while suffering from reduced human resources compared with those originally planned, all goals were achieved under this output; however, the quality of the services was the main aspect affected, for example through narrowing down the scope of the CSIRT-LE study and the support given to the different working groups. The staff assigned to this output really stretched themselves and overperformed in 2022, leading to increased stress levels that cannot be sustained in the long run.

4.2. Develop and enhance standard operating policies, procedures, methodologies and tools for cybercrisis management (also related to a future JCU)

In 2022, ENISA, with the support of key partners, developed a set of SOPs to be used by EUIBAs to respond at operations level to cybersecurity incidents.

In 2023, these SOPs are still under discussion with the key partners from EUIBAs, such as DG Connect, Europol/EC3, EEAS and CERT-EU, and were thus not endorsed.

In parallel, in 2022 ENISA developed a set of tools. In particular, the agency has developed the following:

- SOP awareness-raising, exercise and training materials,
- scripts for presentations and exercises,
- operational reporting templates,
- use-case analysis.

The resources allocated to this output in terms of both human and budgetary resources are minimal. The output did not fully deliver what was envisaged, partially because of the very challenging and fast-changing environment and situation. In particular, at the time of drafting, new structures such as the Interinstitutional Task Force emerged. Due to the cybersecurity support action, the agency was not able to assign more staff and talent to this output in order to deliver the expected results. In 2023, this output is absorbed into output 4.1, allowing a bigger pool of staff to contribute to this area.

4.3. Deploy and maintain operational cooperation platforms and tools (Melicertes, EU-CyCLONe, MoU, etc), including preparations for a secure virtual platform for a future JCU

During 2022, ENISA supported and maintained the tools and services that it provides to its stakeholders, and in some cases proceeded with development of additional features.

In particular, in 2022 all central systems of the Melicertes 2 project were installed in pre-production and production environments, the services were assessed, and the mitigation actions were implemented and made ready to be rendered online.

Workshops for the CSIRTS network's tooling working group were organised, where the architecture of tools, hardening policies and extra monitoring services were communicated to the stakeholders.

ENISA participated in Cyber Europe 2022, providing support and monitoring for the activity and the performance of the tools during the exercise. In addition, in the context of the Melicertes 2 project, risk assessment and business continuity planning tabletop exercises were conducted.

Furthermore, ENISA defined the process for secure end-to-end encrypted sessions with stakeholders from various organisations.

ENISA onboarded new tools such as the ISACs platform, for which a dedicated plan was developed in order to mitigate some legacy limitations in security and monitoring.

In delivering its work, ENISA set the baseline security measures for all operational cooperation tools, following international standards and complying with ENISA's internal policies and IT strategy.

ENISA provided the technical expertise on the tooling required for the cybersecurity support action. ENISA continues to support and maintain the tools that assist ENISA to implement the cybersecurity support action, and it continues to provide a help desk for them.

An internal situational awareness system was deprioritised and decommissioned in 2022, and more focus was given to the Open CTI as the main platform for situational awareness and open threat intelligence activities.

Services offered to the CSIRTs network and EU-CyCLONe should be secure and available. It is of great importance that these services are rendered online and offered to the beneficiaries once all components are secure. Extra resources are needed to support the output, given the range of tasks, the responsibility, the sensitivity, the great variety of tools and technologies to be managed, and ENISA's role as service provider. Not having enough human resources assigned to this output would be a huge risk for the agency.

Key performance indicators: Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation		Unit (of measure- ment)	Frequency	Data source	2021 results	2022 results
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	115 %	19 %
Number of exchanges/interactions year on year		%	Annual	Platform	291 %	104 %
EU-CyCLONe increase year on year						
Active users % increase year on year		%	Annual	Platform	143 %	2 %
Number of exchanges/interactions % increase year on year		%	Annual	Platform	1 011 %	548 %
4.2. Uptake of platforms/tools/SOPs during massive cyberincidents					N/A	N/A ^c
4.3. Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs provided by ENISA (survey)		%	Biennial	Survey	N/A	89 %
% of stakeholders rating outcome/result of ENISA work as high or some added value		%	Biennial	Survey	N/A	94 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member State activities		%	Biennial	Survey	N/A	84 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term		%	Biennial	Survey	N/A	83 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work		%	Biennial	Survey	N/A	94 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA		%	Biennial	Survey	N/A	87 %
% of stakeholders satisfied with ENISA's community-building actions		%	Biennial	Survey	N/A	94 %
Allocated FTEs as per SPD based on full establishment at 2022 year end	10	Actual used FTEs		5		
Planned budget (direct costs only)	EUR 1 703 350	Consumed budget (direct costs only)		EUR 1 682 555		
		Of which carried over to 2023:		EUR 602 393		

- a Based on the internal satisfaction survey run by the network at the end of 2022.
- b Provide support for the design and development of cross-border platforms for pooling of CTI data at EU level (including definition of a blueprint architecture, data infrastructure requirements, data-processing and analytics tools, and data-sharing protocols); CTI exchange initiatives already in place; legal aspects; interoperability, etc.
- c Although the networks were in escalated mode, this situation was not deemed a large-scale cybersecurity incident as defined by NISD2, Article 6 (7).



ACTIVITY 5

Contributing to cooperative response at Union and Member State levels



ENISA contributed to cooperative responses at Union and Member State levels primarily through three main activities:

- common situational awareness in cooperation with Member State and EUIBA partners, primarily DG Connect, CERT-EU, Europol/EC3, the European Union Intelligence and Situation Centre, EEAS Security and Defence Policy – Cyber Security, and EEAS Strategic communications (Stratcom),
- operational frameworks that allow the agency to support technical cooperation (including through Melicertes) and operational cooperation, incident response coordination and EU-wide crisis communication during large-scale cross-border incidents or crises,
- frameworks 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.

Achievements

2022 was a pivotal year for Activity 5, with the initiation of the development of several services, primarily driven by the establishment of an operational and situational awareness sector. The Russian war of aggression against Ukraine, with its associated cyberactivities and risk of spillover within the Union, also shifted the efforts undertaken within this activity. In addition, in 2022, and as part of the agency's transformation into a service-oriented organisation, a situational awareness service package was established, with the objective of further consolidating ENISA's efforts in this area.

The agency increased its efficiency in generating and consolidating information, assessing incidents and facilitating information handling, and thus contributed to the EU priority on situational awareness by supporting the consolidation and exchange of information on strategic, tactical and technical levels with operational communities. In doing so, the agency leveraged its internal capabilities, such as its operational toolsets and ability to actively incorporate lesson learning into its operational response processes and after-action reviews.

In particular, the agency expanded its situational awareness portfolio to tackle different types of threat landscapes and stakeholder situational awareness needs. The agency established a flash report service to enable the fast communication of information internally, to DG Connect and, on request, to other operational entities, increasing the ability to respond to such events.

ENISA piloted the first two EU joint cyber assessment reports (JCARs), integrated reports responding to the legal requirement of the CSA, Article 7 (6), which provides a threat assessment of the Union based on input from EUIBAs (primarily CERT-EU, ENISA and EC3, but also contributions from EEAS and DG Connect). These reports are used in the context of situational awareness briefings to the Horizontal Working Party on Cyber Issues, and other political or strategic stakeholders.

ENISA continued to deliver its weekly open-source intelligence reports to a large number of entities – including the CSIRTs Network, EU-Cyclone, EUIBAs, and sectoral entities across the EU – which provide regular information about ongoing threats and public cyberincidents and events, and are used to augment Member States and EUIBAs' understanding of the threat landscape and their situational awareness capabilities. This was achieved while ENISA worked on the reorganisation of the creation process in order to provide business continuity.

ENISA established a joint rapid report service, and released the first joint publication. This public document provides joint operational and technical guidance to tackle large-scale cross-border threats to the EU and to help public- and private-sector organisations in the EU adopt a minimum set of cybersecurity best practices. This work is part of the structured cooperation with CERT-EU signed in 2021 and follows on the pilot initiated then.

As part of the response to the Russian war of aggression against Ukraine, the agency piloted a weekly Union heat map report, primarily used to monitor cyberevents related to the conflict and, in particular, the risk and impact of spillover events for the Union. The agency has also regularly contributed, in accordance with tasks set within the blueprint^(a), to the integrated situational awareness and analysis report released by the Commission.

In addition to situational awareness, the agency continued to develop its operational framework (the Cyber Assistance Mechanism) initiated in 2021, which enables the agency to support Member States in accordance with the CSA, Article 7 (4). On 9 March 2022, the EU ministers in charge of telecommunications unanimously called for 'the implementation of a new Emergency Response Fund for Cybersecurity to be put in place by the Commission', noting that 'the current geopolitical landscape and its impacts in cyberspace strengthen the need for the EU to fully prepare to face large-scale cyberattacks. Such a fund will directly contribute to this objective.'

To operationalise this support in the short term, the Commission provided additional resources to ENISA, with a view to increasing its level of support to Member States, in line with ENISA's mandate under the CSA. To this end, the Commission increased ENISA's budget by EUR 15 million in 2022 to reinforce ENISA's support capabilities, which were to be made available to Member States in the short term.

As a result of this, ENISA designed and operationalised an expanded programme (the cybersecurity support action) to provide both ex ante and ex post services to Member States identified beneficiaries (the NISD/NISD2), morphing and shifting what it had already established under the Cyber Assistance Mechanism. The agency was therefore able to leverage its earlier activities in order to rapidly operationalise a programme of this scale. As part of this effort, the agency worked closely with the Member States and Commission to further design and set up framework contracts in each Member State so that ENISA could scale up the services it offered to beneficiaries indicated by the Member States. In particular, the services offered include penetration testing, threat hunting, threat landscapes, support for incident responses, risk monitoring, training and exercises.

With regard to the design and operationalisation of a framework to enable collaboration with partners from the private sector, the agency worked on establishing rules of engagement and the appropriate legal framework that would allow the agency to collaborate with said partners. The programme is expected to be piloted in 2023.

Resources

The resource needs for contributing to cooperative response have been growing with the evolving threat landscape. The majority of the activity's resources go towards generating and consolidating the situational awareness portfolio of services, more precisely 7.35 FTEs and EUR 824 000 in budget. These resources do not include the additional injection of EUR 15 million that the agency received in the context of the cybersecurity support action, the preparation and implementation of which required resources amounting to approximately 10.5 FTEs to be reallocated from existing work programme outputs from across the agency, mainly pulling resources from Activity 4 (4 FTEs) and Activity 5 (4 FTEs), with the remaining 2.5 FTEs coming from the other activities.

In terms of budget, the activity operated with reduced finances from 2021 (approximately 40 % less) due mainly to the realignment of carried-over budget but also to the optimisation of some services. However, further optimisation is limited, and the current inflation environment is driving up the cost of external services, which causes additional strain on the delivery of several services. The outlook for the activity to maintain the quantity, quality and timeliness of services is bleak, given current budgeting levels, which can only be combated by reducing the services offered, or through finding synergies with initiatives such as the future Situation Centre.

Although 2022 saw an improvement over 2021 in terms of both competence and mix of talent within the activity, including the addition of two newcomers with backgrounds in threat analysis, the acquisition of resources remains challenging due to the lack of availability of people within the market with the correct experiences, and the limited ability of the agency to quickly attract qualified talent. Ultimately, the total resources for the activity are still not at the level where the activity would be able to provide timely and high-quality services to match stakeholder needs, especially in the event of multiple large-scale cross-border events taking place in parallel or in sequence, protracting a level of high alert for a significant amount of time.

It is estimated that approximately 0.5 FTEs are used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

Overall assessment

During 2022, the activity laid down the foundations for contributing to the Union's common situational awareness and those for its operational capability to respond to Member States' requests in cases of large-scale cross-border incidents and events.

The formalisation of a new sector within the Operational Cooperation Unit specifically responsible for situational awareness (and with a situational awareness service package) provided the focus required for developing the situational awareness portfolio of services needed to address the ever-increasing needs of stakeholders for information exchange. This change came just in time to respond to and manage the increased needs as a consequence of the high-level threat stemming from the Russian war of aggression against Ukraine and the risk of spillover due to cybersecurity operations related to this.

In response to the changing geopolitical landscape, the agency was tasked in the second half of the year with setting up the cybersecurity support action in preparation for its implementation in 2023. The agency achieved its goal of having framework contracts in place in all 27 Member States and a pan-European lot by year end. This was achieved at the expense of the Cyber Assistance Mechanism, which was morphed into the support action halfway through the year.

The priority for the coming years is to continue transforming the service by moving towards better optimisation of internal processes, thus reducing manual work on low-value tasks by automating where possible, reviewing the mix of insourced/outsourced activities and establishing metrics to better assess the effectiveness and efficacy of the actions that seek to achieve the objectives of the activity. In addition, within this activity the agency will seek to identify possible synergies with other activities already performed at Member State level and/or by EUIBAs, as indicated in the result of the biannual stakeholder satisfaction survey. This will be done by narrowing the targets of products and introducing a faster feedback cycle to better address stakeholder needs.

Outputs 5.2 and 5.3 serve as inputs to the situational awareness activities under output 5.3, creating synergies and feedback loops.

2023 will be the first year of the agency delivering services at the scale requested. This will pose a number of challenges, specifically in terms of resources. Furthermore, there is an increasing need to provide 24/7 support in response to cybersecurity incidents; however, the current resources are not sustainable to support such needs. In 2023, the agency will incrementally put into production services that were piloted in 2022, and will further optimise the service delivery and possibly re-evaluate the delivery model, taking into account the lessons learned from these actions.

Objectives



- Effective incident response and cooperation among Member States and EU institutions, including cooperation of technical and political actors during incidents or crises
- Common situational awareness on cyberincidents and cybercrises across the Union
- Information exchange and cooperation, both across layers and borders between Member States, and with EU institutions

Link to strategic objective (ENISA strategy)



- Effective operational cooperation within the EU in cases of massive cyberincidents
- Communities empowered and engaged across the cybersecurity ecosystem

Results



- Member States and institutions cooperating effectively during large-scale cross-border incidents or crises
- Public informed on a regular basis of important cybersecurity developments
- Stakeholders aware of the current cybersecurity situation

Outputs



- 5.1.** Generate and consolidate information (including for the general public) on cyber situational awareness, technical situational reports, incident reports, threats and support consolidation, and exchange information on strategic, operational and technical levels

Outcome



- ENISA expanded its situational awareness portfolio to tackle different type of threat landscapes and stakeholder situational awareness needs. ENISA is now ready to tackle most of the possible scenarios.
- The agency established a flash report service to quickly communicate information internally and to DG Connect. In 2022, ENISA produced 48 flash reports.
- ENISA piloted the first two JCARs (CSA, Article 7 (6), reports), providing threat assessments of the Union based on cooperation with CERT-EU and EC3, with contributions from EEAS and DG Connect.
- It established the joint rapid report service after an initial pilot, and piloted the joint publication with CERT-EU to provide operational and technical guidance to tackle large-scale cross-border threats to the EU.
- ENISA continued to deliver weekly open-source intelligence reports to a large number of entities, including the CSIRTs Network, EU-Cyclone, EUIBAs, and sectoral entities across the EU, providing information about ongoing threats and public cyber incident and events. In 2022, ENISA analysed 1 010 incidents and events. The report received a score of 8/10 for 2022, one point higher than 2021.
- The agency piloted the Union heat map, which aimed to provide a quick overview of cyberincidents and cyberevents affecting the EU's critical sectors as a result of the cyberactivity related to the Russian war of aggression against Ukraine. The sectors contributed to the integrated situational awareness and analysis report from the Commission, with 52 updates on the current situation and incidents in regard to the Russian war of aggression against Ukraine, contributing to the Union's Crisis Management Mechanism (blueprint).
- ENISA established the duty officer role (including piloting after-hours work / holidays), and created a process for daily stand-up coordination within the unit and with relevant internal stakeholders.
- It established a daily collection and curation process, which includes an incident assessment for level 1 and level 2 analysis, setting the foundation for the service's transformation for 2023.
- ENISA established an agency-wide process for a cybercrisis management emergency response team.
- The agency established a process to provide in-depth analysis of specific threats (ENISA threat research) affecting the EU, setting the foundation for the flagship publication of the CSIRTs Network.
- It consolidated the knowledge management platform through the URSA project. This will benefit operational situational awareness, and strategic threat landscape (knowledge and information team) and sectoral overviews (policy, development and implementation unit I). In the long term, it will be open for use by EU Member States and other EUIBAs.
- ENISA consolidated its role within EUIBAs' relevant stakeholder groups by providing relevant information on ongoing incidents, threats and events.

- The agency established synergies and collaboration with EC3 and CERT-EU (structured cooperation – JCAR, joint rapid report, joint publication and others), and cooperation with EC3 (heat map, ransomware report, JCAR).
- It tested situational awareness processes through Cyber Europe 2022.

Based on the assessment of needs from our stakeholders and current resources, this output will continue as is in 2023. The agency will seek further synergies and optimisation to be able to continue to deliver on this output, while some resources will be shared to support ENISA's cybersecurity support action programme.

It should be noted that several of the services that were piloted in 2022 remained in pilot mode and were not fully put into production due to the reprioritisation of resources.

In 2022, the Interinstitutional Task Force was established in view of the Russian war of aggression against Ukraine. The agency has put a significant amount of effort into supporting this initiative by providing situational awareness, participating in meetings, etc. In particular, ENISA has provided briefings, technical assistance and advice during the preparation of dedicated situational awareness products and technical tenders, such as the establishment of new threat-monitoring and CTI services for DG Connect. Moreover, ENISA was engaged in regular calls with DG Connect to support its Cyber Task Force Unit's presence in the Interinstitutional Task Force. The effort can be quantified as 0.2 FTEs.

Furthermore, in 2022 ENISA organised 22 ad hoc calls covering eight critical infrastructure sectors as part of its process for cybercrisis management. This effort – including the continuation of distinct reporting activity for ENTSO-E, the EU distribution system operators, and the European Network of Transmission System Operators for Gas – can be quantified as 0.2 FTEs as well.

Additional budgetary resources could further improve the quality of these services. The agency has strengthened its structured cooperation with CERT-EU, which has the potential to be further extended. In addition, ENISA could benefit from synergising with other initiatives, such as the Situation Centre.

5.2. Support technical cooperation (including through Melicertes) and operational cooperation, incident response coordination and EU-wide crisis communication during large-scale cross-border incidents or crises

Cybersecurity Assistance Mechanism

Initially, this output was dedicated to further operationalising the Cyber Security Assistance Mechanism. The Cyber Security Assistance Mechanism is based on Article 7 of the CSA, which states that, at the request of Member States, ENISA should provide advice in relation to a specific cyber threat; assist in the assessment of incidents; facilitate the technical handling of incidents; provide support in relation to ex post technical inquiries regarding incidents; and support the public communication efforts relating to these incidents or crises. The mechanism complements existing national and EU-level efforts. Within this scope, the following results were achieved.

The service catalogue was developed, including the following ENISA services:

- providing assistance with threat assessments, including particular threat assessment (including penetration testing), advice on the

threat assessment process implementation / life cycle, and threat descriptions for emerging or sector-specific threats, according to requirements defined by requestor;

- providing technical help with incident investigation, including incident analysis, artefact and forensic evidence analysis, and support for information security incident coordination;
- performing threat actor actions analysis (CTI), including advice on detection; analysis of potential impact; threat hunting; analysis of adversary tactics, techniques and procedures; support for internal and external communication; and advice on reporting and recommendations.

An expert database prototype was developed with internal ENISA resources and number of external experts available for assistance. The procedure was developed with swift response to incidents in mind. In 2022, the discussion continued in the CSIRTs Network both in dedicated meetings as well as at the plenary session. The initial proposal was to create a dedicated working group in the CSIRTs Network, but due to the Russian war of aggression against Ukraine it was instead decided to use the Mattermost channel and have ad hoc meetings when necessary.

Assistance was provided to two Member States at their request. These were test cases for the mechanism, and the constructive and positive feedback helped further fine-tune the service and internal procedures for incident response and management.

Cybersecurity support action

During 2022, the European Commission allocated ENISA a one-off budgetary injection of EUR 15 million so that the agency could massively scale up and expand its ex ante and ex post services to the Member States. This short-term support aimed to complement rather than duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, by providing ENISA with additional means to support preparedness (ex ante), and response (ex post) to large-scale cybersecurity incidents.

While the additional funds were a very substantial increase of budgetary resources, the implementation needed to be executed by existing ENISA staff. The agency quickly reassigned 10.5 FTEs (4 from Activity 4, 4 from Activity 5 and 2.5 from the other activities), and decided to transform and shift the abovementioned Cyber Assistance Mechanism to prioritise quick implementation of the cybersecurity support action. This was a huge endeavour, which started in summer 2022. The agency assigned service managers for every Member State, and the Member States appointed points of contact (by sending a request to EU-Cyclone).

The work from the Cyber Assistance Mechanism was shifted and resulted in:

- input to procedures and supporting documents;
- input to tender specifications for support service providers (27 Member State lots + 1 pan-EU lot + 1 training tender);
- the basis for tooling used for request handling;
- input to discussion on the cybersecurity support action's internal and external stakeholders.

Given the timing and the limited human resources, the agency was under huge pressure to be able to commit the full amount before year end. This brings with it an inherent financial risk of the agency not being able to execute the committed budget if the Member States do not make full use of their allocated budgets. However, the agency succeeded in doing so with constructive help from the Member States through the points of contact. In 2023, ENISA should put organisational structures for the implementation of such programmes in place. The agency also lacks operational reserves, which means that in times of escalation, or when an initiative such as the cybersecurity support action arrives in an ad hoc and unexpected manner, it needs to shift resources away from other outputs in the work programme. The agency should have operational reserves to be able to cope with this, and in addition should have a flexible and rapid mechanism to temporarily deprioritise other projects/outputs/activities.

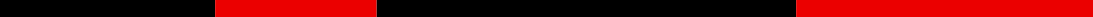
5.3. Initiating the development

In order to ensure the development and operationalisation of the work to enable collaboration with partners from the private sector, the agency

This output contributes to the following objectives: M M e ecti
ntivities.
cy erinci ent~

the agency to work closely with industry partners from the private sector.
This ENISA programme is developed for private sector, like-minded
set of to increase the situational awareness of cyber incidents

The Agency's resources are used for the development of the work programme. The Agency's resources are used for the development of the work programme. The Agency's resources are used for the development of the work programme.

[illegible]

ACTIVITY 6

Development and maintenance of EU cybersecurity certification framework



In 2022, against the background of supporting the EU cybersecurity certification framework, Activity 6 facilitated the preparation of draft candidate cybersecurity certification schemes in line with Article 49 of the CSA and Commission requests for the preparation of three cybersecurity certification schemes. These requests include a scheme for the certification of products, with reference to common criteria (European Union common criteria scheme (EUCC)), a scheme on cloud services (European Union cloud services scheme (EUCS)) and a scheme concerning the certification of network products and identification on 5G networks (European Union certification scheme for 5G networks (EU5G)). ENISA provided assistance to the European Commission in discharging its duties towards the European Cybersecurity Certification Group (ECCG) and, along with the Commission, ENISA co-chaired the Stakeholder Cybersecurity Certification Group (SCCG) and provided it with secretariat services. ENISA finalised the dedicated European cybersecurity certification website, in accordance with Article 50 of the CSA and the associated workflow for the publication of certificates to be issued under an adopted scheme. This activity led the certification service package and contributed to the NIS service package.

The legal basis for this activity is Article 8 and Title III of the cybersecurity certification framework of the CSA, and it served the agency's strategic objective of a 'high level of trust in secure digital solutions'.

Achievements

By the end of 2022, ENISA had made new meaningful contributions to the EU cybersecurity certification framework by assisting the Commission in discharging its duties concerning governance of the ECCG and SCCG, and further processing draft candidate cybersecurity certification schemes in terms of planning and content development. By advising broadly in terms of cybersecurity standardisation, ENISA further served the strategic objective of a 'high level of trust in secure digital solutions'. ENISA reinforced this strategic goal with new components of certification schemes, some of which will have to be adopted and implemented by Member States. In 2022, the accomplishments of ENISA include:

- supporting the European Commission with respect to finalising the implementing regulation for EUCC;
- supporting a proposal for a maintenance organisation for the EUCC to follow scheme adoption;
- completing the technical finalisation of the EUCS scheme;
- supporting the Commission and the Member States in formulating the additional requirements, required by some Member States, on independence from non-EU laws;
- supporting the development of cybersecurity requirements in relation to EUCS by the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (Cenelec) JTC13 along two discrete items;
- undertaking a gap analysis of existing technical specifications available in the industry, which provided the foundation of EU5G;
- finalising the design and implementation of the ENISA website on certification;
- finalising the implemented workflow for the publication of certifications on the ENISA website;
- providing support to awareness-raising activities on certification;
- providing advice concerning emerging legislation in relation to certification;
- supporting the Commission concerning the CEF core service platform for cybersecurity certification stakeholders.

Resources

The certification activity required approximately EUR 1 million, and the utilisation of the 11 FTEs planned was deemed sufficient to meet the requirements at EU level. The difference between the resources available and resources planned, while visible, was not detrimental to the performance of the agency on certification because the risk was mitigated by reprioritising and requiring a slightly higher number of external experts, who supported ENISA staff. To maintain the designated appropriations level, no actions outside the EU were carried out, thus limiting the scope of the activity to the Member States, supporting a critical mass in the EU and containing costs. The headcount was balanced and it saw two new recruits joining and one person leaving, which was duly mitigated. Finally, 0.3 FTEs were provided for the cybersecurity support action.

In terms of budget consumption, ENISA facilitated stakeholder engagement in the post-COVID-19 period, which permitted a return to a more regular work pattern that included physical meetings, from mid 2022 at least. The slight shortfall in budget consumption between financial resources planned and actually consumed was a result of the shortfall in headcount and reprioritisation to meet actual needs.

Carry-forwards were planned with a view to facilitating the continuous life cycle of certification, which is not limited in terms of content production by the annual budget cycles of the agency; this is a particular feature that the agency has adopted in certification to allow the development of the framework in a way that avoids peaks and valleys in the activity.

It is estimated that approximately 0.3 FTEs are used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

Overall assessment

In 2022, ENISA continued administering the ad hoc working groups across the three schemes that are currently under way and at different stages of completion. ENISA remained engaged with the Member States by continuing to encourage participation and dialogue with the Member States at the level of the ad hoc working groups. ENISA also launched a dedicated round of visits to national cybersecurity certification authorities (NCCAs) in selected Member States, starting with NCCAs that had expressed a stronger interest in certification. Throughout this period, ENISA continued assisting the European Commission on a regular basis.

ENISA's delivery planning regarding the EUCS was adapted to meet Commission expectations. While delivery fell short of formally submitting the EUCS, in Q1 and in due consideration of the ongoing discussions among Member States, the scheme had been completed in terms of meeting formal requirements for submission to the Commission. Still, ENISA continued working on the scheme in an effort to progressively assist in finding the right balance. By the end of 2022, no conclusion point had been reached on the outstanding aspects that had led the discussion at Member State and Commission levels throughout 2022. It was sufficiently clear that ENISA operated as a facilitator in a broader discussion concerning certification and a continuous caretaker of the development of the cybersecurity certification framework at large.

Furthermore, ENISA continued engaging with and supporting CEN and CENELEC in developing a European standard on cybersecurity controls for cloud services, conformity assessment criteria for cloud services and a dedicated assurance level methodology based on the ENISA sectoral cybersecurity assessment that was developed in 2020–2021. ENISA continued its dialogue with the private-sector associations that produce technical specifications that may be used in EU5G, and it extended this further by attracting the interest of and obtaining admittance to other associations with a similar orientation in producing technical specifications for 5G.

ENISA extended its analytical services to the draft CRA, the European Digital Identity Wallet, the AI Act, etc. At the end of 2022, the Member States, acting on a Commission proposal, had yet to adopt any implementing act(s) based on an ENISA (draft) candidate scheme.

In addition, ENISA extended its efforts to better prepare the Commission and the Member States for the future maintenance of the EUCC, vulnerability handling and the promotion of certification once the schemes are adopted. It also reinforced its support of other regulatory proposals that may rely on CSA schemes for presumption of conformity, through direct support of Commission regulation development (the eIDAS regulation / wallet) and the development of feasibility studies to be better prepared for new certification schemes.

The KPI survey results suggest a general interest of the broader stakeholders' community in the cybersecurity certification framework; replies concerning submetrics of the KPI-related question are affected by the profile of the respondents, who, for instance, may not make use of products on the market when considering certification, as they may be public authorities, for instance. It is also important that good-quality service has been made available by ENISA thanks to the continuous efforts of its staff, who seek to engage directly with Member States to the extent permitted. Regarding KPIs involving citizens, ENISA extended the survey to consumer protection organisations and it reached out to the two notable federations (the European Association for the Co-ordination of Consumer Representation in Standardisation AISBL and Bureau Européen des Unions de Consommateurs), which responded positively, and put ENISA in contact with their members to allow for richer and more representative data collection. The survey outcome highlights the interest of stakeholder respondents in the outcomes of ENISA's work on certification. ENISA takes note of the need to better monitor the spread of likely responses, with a view to prevent data skewing and uneven distribution of underlying data.

ENISA seeks to fund certification in a way that remains commensurate with the task at hand; in view of this, a spike in resources could be motivated by several concurrent requests for schemes. As the number of requests remains predictable, resource changes are not a priority. In 2024, a new component under outcome 6.4 will gradually enter the domain of ENISA: the CEF platform. The platform will gradually become operational and competence will pass from the Commission to ENISA, calling for appropriate resources to be allocated.

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

Link to strategic objective (ENISA strategy)



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

Results



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

Outputs



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

Outcome



ENISA assisted the Commission in laying out the draft implementing regulation for the EUCC, transformed relevant Senior Officials Group Information Systems Security documents into state-of-the-art documents supporting the scheme, and presented the draft outlines to the ECCG.

Due to the 'presumption of conformity' references to the EUCC in EU regulatory initiatives such as the CRA, the preparatory work on the implementing regulation was scrutinised with regard to the likely impact on the EUCC.

While the substantial work on cybersecurity controls and conformity assessment for the draft candidate EUCC had already been carried out, in 2022 ENISA supported and facilitated the discussions on risk-based mitigation measures related to independence from non-EU law. As these discussions progressed, ENISA took due note of the concerns of the industry, which were frequently communicated or published. ENISA looks forward to the conclusion of these discussions in the

	<p>ECCG, with a view to supporting the Commission in the drafting of the implementing regulation on the EUCS.</p> <p>ENISA also participated in regular CEN and Cenelec meetings, at which the EUCS security controls and evaluation criteria initially developed by ENISA are currently being further discussed and maintained for the first time, with a view to their becoming European standards.</p> <p>The development of the candidate EU5G by ENISA aimed to analyse the existing GSMA network equipment security assurance scheme, the security accreditation scheme for subscription management, the security accreditation scheme for universal integrated circuit card (UICC) production and embedded UICC activities. This resulted in a gap analysis submitted to and endorsed by the two main stakeholders of the scheme: the ECCG and the NISCG / NIS subgroup on certification and standardisation. Around 100 industry representatives – including developers of network equipment and embedded UICCs, CABs, MNOs, ESOs and national authorities – are supporting ENISA in this activity, as is the European Co-operation for Accreditation.</p> <p>In addition to scheme developments, ENISA's revised certification strategy currently includes feasibility studies for areas (e.g. AI) where certification is expected, to help define the possible scope and related certification elements reusing schemes under development or new schemes; such feasibility studies will be conducted from 2023.</p>
--	---

6.2. Implementation and maintenance of the established schemes including evaluation of adopted schemes, participation in peer review, etc.

With the support of an ad hoc working group, ENISA further developed guidance, and established a first draft describing a possible organisation for the maintenance of the EUCC. This proposed organisation is based on two pillars – a dedicated ECCG subgroup and an ISAC – and will continue to closely involve ENISA. It will serve as the basis for ECCG discussions and for the industry to establish an ISAC proposal under the digital Europe programme.

ENISA also engaged with some Member States in the transformation of their national interpretations of the common criteria into future state-of-the-art documents supporting the EUCC.

ENISA supported the Commission in analysing how EUCC certificates could further serve other regulations, such as the CRA and the eIDAS regulation / wallet. This is ongoing work to be continued in 2023.

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

The ECCG received regular updates on the main projects related to the market, certification and standardisation, and the schemes under development.

ENISA supported the Commission in analysing and processing the initial comments of the ECCG members on the draft of the EUCC Implementing Act, and on the outcome of the gap analysis resulting from the EU5G activities.

ENISA also presented its certification strategy and the feasibility studies proposal, which were both approved.

In relation to the SCCG – composed of representatives of stakeholders of industry and consumer groups, small and medium-sized entities, academia, cybersecurity certification interest groups and trade association groups – and due to the fast-evolving cybersecurity landscape, the Commission proposed new EU regulatory initiatives using Article 54 (3) of the CSA to indicate that European cybersecurity

6.4. Development and maintenance of necessary tools for making effective use of the Union's cybersecurity certification framework (incl. certification website, the Core service platform of CEF (Connecting Europe Facility) for collaboration, and publication, promotion of the implementation of the cybersecurity certification framework etc.)

ENISA further developed its cybersecurity certification website, which is composed of two main parts. There is dashboard displaying schemes and supporting documentation, the catalogue of certificates and a directory of key certification stakeholders (NCCA and notified bodies). There is then a back-office function providing APIs to CABs issuing certificates. Associated processes were presented and discussed with the Member States, the ECCG and the SCCG.

ENISA supported the Commission in the development of the CEF platform, on which cybersecurity certification stakeholders will interact with each other. ENISA and the Commission have developed use cases concerning stakeholders' interactions. Examples are proposals for EUCC Protection Profile developments, and looking for other stakeholders to create alliances for European funding calls.

ENISA organised two hybrid editions of cybersecurity certification weeks, one in May (Athens) and one in December (Brussels), gathering the various ad hoc working groups and the Thematic Group on Vulnerability Handling. These weeks allowed for interactions and

synergies among the schemes' participants, and opportunities to update them on new legislation that may impact the schemes or reuse their certificates (such as the CRA and the eIDAS regulation / wallet).

In the May session, the cybersecurity certification conference was organised as a hybrid event, gathering more than 800 participants online and 100 in person. The Commission, the Member States, 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 December 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 and Cenelec, ETSI, CSIS, FIC, ICCG, IT-SA, Jornadas de ciberseguridad, EUCW, and the European 5G Conference and One conference.

Key performance indicators: 1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions. 2. Effective preparation of candidate certification schemes by ENISA	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
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	79 %	86 %
% of respondents planning to use the cybersecurity schemes to have solutions certified	%	Annual	Survey	24 %	29 %
% of respondents planning to use the cybersecurity schemes to use certified solutions	%	Annual	Survey	37 %	32 %
% of respondents planning to use the cybersecurity schemes to certify solutions	%	Annual	Survey	44 %	40 %
% of respondents planning to refer to certifications within regulations	%	Annual	Survey	36 %	44 %
% of respondents planning to use the EUCC	%	Annual	Survey	53 %	57 %
% of respondents planning to use the EUCS	%	Annual	Survey	49 %	52 %
% of respondents that need assistance from ENISA in the process of preparing to use the EU certification schemes	%	Annual	Survey	66 %	76 %
6.2. Stakeholders' trust in digital solutions of certification schemes (citizens, public sector and businesses (survey))	%	Biennial	Survey	N/A	74 %
6.3. Uptake of certified digital solutions (products, services and processes) using certification schemes under the CSA framework	%	Biennial	Survey	N/A	73 %
6.4. Number of candidate certification schemes prepared by ENISA	Number	Annual	Numerical	N/A	Three in different stages of adoption
6.5. Number of people/organisations engaged in the preparation of certification schemes	Number	Annual	Numerical	N/A	Approximately 150
6.6. Satisfaction with ENISA's support for the preparation of candidate schemes (survey)	%	Biennial	Survey	N/A	82 %
% of stakeholders rating outcome/result of ENISA's work as high or some added value	%	Biennial	Survey	N/A	75 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	88 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	75 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	75 %

Key performance indicators: 1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions. 2. Effective preparation of candidate certification schemes by ENISA		Unit (of measurement)	Frequency	Data source	2021 results	2022 results
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA		%	Biennial	Survey	N/A	83 %
% of stakeholders satisfied with ENISA's community-building actions		%	Biennial	Survey	N/A	93 %
Allocated FTEs as per SPD, based on full establishment at 2022 year end	11	Actual used FTEs			8.35	
Planned budget (direct costs only)	EUR 1 025 750	Consumed budget (direct costs only) ^(b)			EUR 959 343	
		Of which carried over to 2023			EUR 277 604	

- a Examples are (i) NISD2, where Member States may require essential and important entities to use cybersecurity certification for their ICT products, ICT services and ICT processes to demonstrate compliance with particular cybersecurity requirements; (ii) the eIDAS directive, where cybersecurity certification is proposed as obligatory for demonstration of cyber compliance; and (iii) and (iv) the AIA and the CRA, where cybersecurity certification may be used as a presumption of conformity if the AIA's and CRA's applicable cybersecurity requirements are met.
- b Resources related to the ongoing EU5G scheme were only minimally utilised, in view of timing constraints and absence of due delegation, as long as meeting formal requirements remained a work in progress in a multi-stakeholder environment.

ACTIVITY 7

Supporting the European cybersecurity market and industry



In 2022, supporting the EU cybersecurity market and industry aimed to produce analytical market outcomes, thus supporting the evolution of ENISA's relationship with European, international and private standard-setting organisations. In terms of support actions, ENISA further examined the prospect of a cybersecurity certification label, and it continued analysing aspects of vulnerability handling for certified products, services and processes. This activity contributed to the certification service package and the NIS service package.

The legal basis for this activity has been Article 8 of the CSA, and it served the agency's strategic objective of a 'high level of trust in secure digital solutions'.

Achievements

In 2022, ENISA sought to foster the cybersecurity market for products and services in the EU. With this aim, ENISA surveyed and analysed the market segment concerning cloud cybersecurity services and it mobilised a range of stakeholders for the purpose of collecting data. Along with the survey and analysis, ENISA reviewed and redrafted the applicable framework methodology for market analysis. This activity provided context-rich information and analysis concerning the market, specifically in relation to the cybersecurity of cloud services.

Operating in a collaborative, value-friendly manner, this activity supported cybersecurity certification by monitoring and analysing standards that are currently in use in European cybersecurity certification schemes, and it recommended appropriate technical specifications. In certain areas, this activity supported emerging policy concerning the standards for the European Digital Identity Wallet, for example regarding vulnerabilities. Activity 7 produced a preliminary example of a cybersecurity certification label to keep up the interest of the stakeholder community. Looking to the future, Activity 7 operates in a way that means it can further accommodate the expectations of the agency in the advent of the adoption of the CRA.

Resources

Resource allocation was sufficient to meet the moderate goals of 2022; consumption was high, particularly in outputs 7.1 and 7.2, which exceeded the budget allocated and expectations. The remaining two outputs the budget was reallocated to support other, centrally positioned, policy areas across the market, certification and standardisation. In addition, the activity contributed approximately 0.2 FTEs to delivering the cybersecurity support action. Looking to the future, good practices and vulnerabilities can continue supporting and feeding into their main centre of gravity in certification. The CRA could carve out a role for the market, and, in this light, further input from vulnerabilities can play an instrumental role for ENISA in terms of building a service for the stakeholders. Good practices can be leveraged to approach new market niches and stakeholder communities in a way that ensures that the message of ENISA propagates further afield, thus allowing ENISA to learn from and interact with non-institutional stakeholders and communities alike. This approach would assist in managing resource scarcity and reinforce the production of compelling outputs.

It is estimated that approximately 0.2 FTEs are used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

Overall assessment

The outcomes of this activity have exceeded annual expectations with respect to the market, standardisation and vulnerabilities; regarding output 7.3 and 7.4 the efforts remained inconclusive. Regarding the market, this was the second vertical analysis of a cybersecurity market segment, and it was evident from interacting with stakeholders that there is keen interest in this area. Carving out a discrete role for ENISA is a key challenge for the market. The challenge of the market analysis consists of having to work with cybersecurity stakeholders in a data-poor

environment to produce analytical outcomes on market metrics. Regarding standardisation, ENISA recently stepped up its game with the three standardisation requests issued to CEN and Cenelec, which complement the good relationship with ETSI, the regular exchanges with the GSMA, and the rapport with the 3rd Generation Partnership Project and GlobalPlatform. This is all referred to in order to highlight the complexity of the work of ENISA when it drafts certification schemes. There is also an important repercussion of these efforts: as ENISA shares tasks with the standardisation stakeholders (requests to CEN and Cenelec, guidance to change technical specification related to EU5G, etc.), it influences policy outcomes even when a certification has yet to be adopted. As a result, ENISA has started meeting the expectations of the strategic objective and it has operated as a cohesive element in an otherwise challenging multi-stakeholder environment.

The advent of the CRA and the promise that it holds for ENISA could be managed within this activity in relation to vulnerabilities for example market sweeps, vulnerability handling, etc. If so, the resources for the market should be strengthened, as should the organisational model, which could allow one more sector to emerge. The output could then be further instrumentalised to reach out to and prepare new market segments, and resources across outcomes 7.1, 7.3 and 7.4 could be leveraged.

In terms of assessing the outcome of the KPIs, ENISA has managed to attract and maintain the interest of stakeholders over time and extend this interest into new areas, including the market. At times, seemingly lower metrics suggest that not all outcomes are actionable because ENISA produces analytical outcomes that can be used further afield, for instance as general information, context or raw data for third-party outcomes. Responding stakeholders have diverse profiles, rarely representing a single interest area, least of all in an atypical cybersecurity area such as market analysis. Clearly the high-quality work on standardisation that follows a well-established pattern remains a performance staple in ENISA. ENISA needs to remain observant of the composition of its KPI respondents to prevent data skewing and the uneven distribution of underlying data.

In 2022, individual outputs across the market and standardisation were produced at a high level, and a sound organisational framework has been established for the analytical work. The overall impact of ENISA could be enhanced by ensuring the output of the analytical work is more visible and accessible to the relevant stakeholders.

Outputs



- 7.1. Market analysis on the main trends in the cybersecurity market on both demand and supply sides

Outcome



In 2022, ENISA analysed aspects of the cybersecurity market. With a view to contributing to a further enhanced internal market and to a more robust European cybersecurity industry, the agency concentrated its efforts on the cloud cybersecurity market. Based on the additional experience gained through this analysis, the agency updated the cybersecurity market analysis framework to extend indicators that reach out to lateral policy areas (e.g. research, operational cooperation, cybersecurity index). In addition, ENISA organised the 1st Cybersecurity Market Analysis Conference. ENISA was supported in these activities by its ad hoc working group on the EU cybersecurity market.

- Cloud Cybersecurity Market Analysis. Based on data also collected through a survey, this analysis provided an insight into the needs and requirements of consumers in terms of cloud cybersecurity products, services and processes. It identified trends and potential issues at stake in terms of demand and supply (<https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis>).
- Updated ENISA Cybersecurity Market Analysis Framework V2.0. This guide for the development of the analysis of a vertical cybersecurity market segment was improved and enriched, with the steps to take to perform the analysis simplified and some of them, such as the scoping of the market segment, further explained (<https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0>).
- 1st Cybersecurity Market Analysis Conference. This was organised on 23 and 24 November as a hybrid event (in Brussels and online), bringing together around 300 stakeholders, including suppliers and consumers of cybersecurity services, but also those involved in market analysis; policymakers; regulators of cybersecurity products, services or processes; and research organisations (<https://www.enisa.europa.eu/events/cybersecurity-market-conference>).
- ENISA ad hoc working group on the EU cybersecurity market. This group provided knowledge and support, for instance in selecting the market segment to focus the analysis on, in scoping and analysing it, in developing the survey and in validating the results. It helped update the framework and contributed to the definition of the agenda of the Cybersecurity Market Analysis Conference (https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-cybersecurity-market).

The cybersecurity market analysis, a recently launched area of ENISA work, calls for an interdisciplinary approach. With the support of various stakeholders and of the dedicated ENISA ad hoc working group, a framework for guiding the cybersecurity market cybersecurity analysis was developed and is kept updated and constantly improved based on the experience gained with the pilot analyses focused on selected market segments. The Cybersecurity Market Analysis Conference, with its first edition in 2022, aims to become an established forum for stakeholders to meet and share experience and knowledge in cybersecurity market analysis, identify challenges and best practices, and present novel ideas in the area.

7.2. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international standards for risk management in relation to certification

In 2022, this output was split across three tasks.

- **Contacts with SDOs.** This involved maintaining contacts; participating in meetings of and liaising with multiple relevant technical committees of ETSI, CEN and Cenelec, and private initiatives; organising the largest cybersecurity standardisation conference together with CEN, Cenelec and ETSI; participating in conferences and workshops related to cybersecurity standardisation; and being involved in discussions between ENISA and ESOs.
- **Support to policy.** Two studies were performed – one on digital identities (in support of the second eIDAS regulation) and one on AI (following a request from the European Commission, in support of the draft AI Act).
- **Support to certification.** Relations with relevant groups working on 5G standards were maintained.

7.3. Guidelines and good practices on cybersecurity certification requirements for ICT products, services and processes

In 2022, the output concerning good practices sought to implement an example of a label for cybersecurity certification and complement it with relevant technical specifications. While the goal was to have a practical and readily usable label, this had to be adjusted to be just an example of a label. The Thematic Group on Labelling of ICT Trusted Solutions, which had previously been set up, continued rendering its support to this output. The first internal report presented the legal requirements for setting up a labelling framework. The second internal report presented an example for the visual identity of such a labelling framework, including video teasers, and aimed to assist stakeholders in the implementation of a future European cybersecurity label. These two reports were presented to the NLOs and SCCG on various occasions for the purpose of validation.

In addition, under this output, support contributions were made to drafts of other outputs (e.g. certification, CRA).

The KPIs suggest that the percentage of respondents interested in using ENISA's consolidated certification labelling process (if it became available) reached 93 % in 2022 compared with 84 % in 2021. This output remained an ongoing concern in Q1/Q2 of 2023, and ENISA continued its efforts to support the Commission on the basis of adjusted objectives; however, as the results obtained didn't fully meet our objectives, the continuation of this output is intended to be reassessed in the 2024–2026 draft SPD.

7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services

The Thematic Group on Vulnerability Handling for Certified Solutions continued rendering support to this analytical output. Certification of products, services and processes remains the centrepiece of the vulnerability-related work of this output.

The group operated in a complementary manner, and as a horizontal layer across various schemes. The members of all certification ad hoc working groups on the EUCC, EUCS and EU5G were invited and most joined, with members from industry, Member States and representatives of some organisations.

In 2022, the group had 30 meetings, with two physical plenaries.

The first draft of the Guidance for the Vulnerability Handling on Certified Solutions was finalised in July 2022.

There are five ongoing proof of concepts of the guidance document.

It is proposed that this output be reassessed during the drafting of the 2024–2026 SPD and, if required, merged with other outputs in the work programme dealing with vulnerability handling.

Key performance indicators: Effectiveness of ENISA's supporting role for participants in the European cybersecurity market	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
7.1. Number of market analyses, guidelines and good practices issued by ENISA					
Cybersecurity market analysis framework	Number	Annual	Reports	Two	Five in different stages (two reports pending publication, two internal reports, one report published)
7.2. Uptake of lessons learned / recommendations from ENISA reports					
% of respondents interested in using ENISA's good practice on market analyses	%	Annual	Survey	87 % (fully and partially interested)	85 % (high and medium interest)
% of respondents interested in using ENISA's standards mapping related to digital identities	%	Annual	Survey	N/A	89 % (high and medium interest)
% of respondents interested in using ENISA's standards mapping related to IOT	%	Annual	Survey	88 % (high and medium interest)	89 % (high and medium interest)
% of respondents interested in using ENISA's standards mapping related to AI	%	Annual	Survey	N/A	82 % (high and medium interest)
% of respondents interested in using ENISA's risk-based approach for their cybersecurity certification activities	%	Annual	Survey	72 % (high and medium interest)	86 % (high and medium interest)

Key performance indicators: Effectiveness of ENISA's supporting role for participants in the European cybersecurity market	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
% of respondents interested in using ENISA's consolidated certification labelling process	%	Annual	Survey	84 % (high and medium interest)	93 % (high and medium interest)
% of respondents interested in using ENISA's vulnerability management process for certified products services and processes	%	Annual	Survey	82 % (high and medium interest)	89 % (high and medium interest)
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work (survey)	%	Biennial	Survey	N/A	88 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	88 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	84 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	72 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	93 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	94 %
Allocated FTEs as per SPD, based on full establishment at 2022 year end	8	Actual used FTEs		4.35	
Budget planned (direct costs only)	EUR 373 800	Budget consumed (direct costs only)		EUR 366 473	
		Of which carried over to 2023		EUR 105 230	

N/A, not applicable.

ACTIVITY 8

Knowledge on emerging cybersecurity challenges and opportunities



Through Activity 8, ENISA provides strategic long-term analysis, guidance and advice on the cybersecurity threat landscape, emerging technologies and cybersecurity challenges. It also serves the purpose of providing topic-specific recommendations and general assessments on the impact of cybersecurity's requirements and challenges. The activity also focuses on identifying and giving advice in relation to cybersecurity research and innovation, and thus contributes to the relevant EU strategic agenda.

In line with the strategic objectives of efficient and effective cybersecurity information and knowledge management for Europe (SO7) and foresight regarding emerging and future cybersecurity challenges (SO6), the activity builds on aggregating and analysing information across the ecosystem (legal, regulatory, technical, societal, etc.), and leverages expertise to provide relevant analyses. The activity builds on and leverages the input and active contributions of relevant stakeholder groups to the work of which it contributes, thus fulfilling the strategic objective on empowered and engaged communities across the cybersecurity ecosystem (SO1).

Activity 8 collects, consolidates, analyses, and provides recommendations and reports on information and knowledge across the cybersecurity ecosystem and ENISA SPD activities (e.g. incident reporting, situational awareness, NIS investments, threat landscapes). A prime example is the work on the EU cybersecurity index, which consolidates information from across all ENISA activities in order to assess the maturity levels of cybersecurity in the Member States and the EU, while generating qualitative and quantitative results that yield significant information on both ENISA's and the EU's progress in raising the level of cybersecurity. The EU cybersecurity index belongs to the five service packages identified by the Management Board as a strategic priority for the Agency. Moreover, the analyses and recommendations under Activity 8 feed into the work and prioritisation of topics of other activities, with a notable example being the threat landscape that guides the selection of topics for training and exercises (Activity 3) and European Cyber Security Month (ECSM) (Activity 9), and feeds into the NIS strategy (Activity 2). An effective cycle of information and knowledge management is thus achieved by consolidating information across ENISA's ecosystem of activities, analysing them and feeding back to the activities of ENISA.

Achievements

In 2022, ENISA worked on various facets of consolidating information, analysing it, and providing analyses and recommendations to serve stakeholders' expectations. The agency worked closely with the stakeholders' communities (three ad hoc working groups, and a subgroup of the NLO Network).

ENISA has followed a multiannual perspective in the delivery of Activity 8, engaging in the refinement and first pilot of the EU cybersecurity index; the annual threat landscape; the threat landscape methodology, and the ransomware and foreign information and manipulation threat landscapes; its first ever cybersecurity foresight exercise on cyber threats in 2030; the efforts on incident reporting across legislative files (the EEC, the eIDAS regulation, the NISD); the piloting of the information hub (infohub); the work on AI on security and privacy in distinct use cases; and the efforts on post-quantum integration. In addition, ENISA provided continuous support to the EU research and innovation agenda, and in particular to the EEC, by helping with the identification of research and innovation priorities. All those projects have long-term plans and established and transparent methodologies, are supported by IT tools and platforms, and adhere to a service-oriented approach to cater to stakeholders' needs in an agile manner.

In terms of cohesion and vision, the work of Activity 8 looks at cybersecurity information and knowledge across the timeline by looking into past and present data (incident reporting, threat landscapes and the cybersecurity index) to understand the status quo and identify trends for the future (foresight and emerging challenges), and uses these to feed into the research and development agenda (research and innovation priorities), with the aim of raising awareness using a procedural knowledge management framework (infohub). It needs to be highlighted that all outputs under Activity 8 are based on stakeholder priorities, thus promoting outputs'

acceptance by the agency's stakeholders. This is particularly evidenced by the numerous ad hoc working groups (e.g. on AI, cyber threat landscapes, foresight) and interactions with statutory bodies such as the NLO Network (e.g. infohub and the index), the Management Board (e.g. the index) and the ENISA Advisory Group (e.g. foresight).

To attain the Activity 8 objectives and overall vision, in 2021 a multiannual perspective was followed using a 3-year time horizon, with notable examples being the work on foresight, the index, threat landscapes, infohub, and research and innovation. In 2022, there was noteworthy maturity growth across all streams, utilising the methodological frameworks set up in 2021 to lay the groundwork for the deployment of actual solutions in 2023. Accordingly, pilot projects for the cybersecurity index, the infohub, the identification of research priorities and cybersecurity foresight were successfully conducted, while the work on consolidating knowledge and information management progressed with the identification of relevant workflows and interdependencies. To this end, the objectives of the activity were met and the vision is on course to be successfully delivered.

In order to achieve agency-wide consolidated information and knowledge management, ENISA needs to engage further work and additional resources. Substantial steps were therefore taken in order to promote this goal. For instance, knowledge management frameworks were introduced for the following activities: cybersecurity index, situational awareness / threat landscapes workflows or the info hub. The work engaged follows up on the findings of the 2021 annual activity report where common tooling requirements and common analysis techniques were established. However, given the target scope of outputs and the efforts required to deliver the results expected, further exploration of synergies and optimisation of knowledge management workflows across outputs and activities would be beneficial for the entire agency. The overall work under Activity 8 constitutes in itself a pilot in relation to how an integrated knowledge management approach may yield significant results, albeit at the cost of additional resource utilisation, and brings ENISA closer to the overall strategic objective.

Resources

Budget implementation for Activity 8 reached 99.2 % at the end of 2022, up from 95 % in 2021. The improvement in the figures and the nearly full implementation of planned budget allocation indicates a growth in financial planning maturity.

In terms of FTE resources, Activity 8 faced the challenge of having two horizontal teams, with team members contributing various full time equivalent employee percentages towards the team and one operational unit working together to meet the objectives. Accordingly, and also identifying the significance of research and innovation as a standalone topic that merits attention, a new activity was introduced in the 2023 SPD. Activity 8 is a prime example of an activity fully delivered by ENISA staff in a matrix organisation and, to this end, FTE utilisation is considered to be at a high level despite the inherent challenges of multitasking. Finally, 0.75 FTEs were provided for the cybersecurity support action.

The KPIs of Activity 8 cover different aspects, but admittedly do not accurately reflect the level of attainment of the strategic objectives. KPI 8.1 deals with the visibility and impact of the infohub, which, given its multiannual development plan, did not become operational during the reporting year. Therefore, KPI 8.1 was not assessed in 2022, since the only progress was that the design of the infohub and the knowledge management framework were refined and a pilot test was undertaken. KPI 8.2 assesses the quantity and depth of ENISA's work in terms of analyses, challenges and recommendations. With an average of 357 analyses, challenges and recommendations identified in each of the eight reports considered, the depth of ENISA's work in identifying cybersecurity challenges, highlighting relevant recommendations and providing analyses is considered significant. KPI 8.3 reflects the number of requests from Member States and EU research and innovation entities to contribute, provide advice or participate in activities. As the KPI has a value of 63, a clear indication of the extent of ENISA's outreach activities is evident. KPI 8.4 involves a biennial stakeholder satisfaction survey, which was held at the beginning of 2023. The results indicate high or some added value for the work under Activity 8 (94 %), and increased uptake of the results (86 %), also noting a 94 % satisfaction rate with the way the activity was planned.

It is estimated that approximately 0.1 FTEs are used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within the activity.

Overall assessment

Activity 8 met its objectives for 2022. KPIs revealed that ENISA had a notable impact on identifying recommendations, analysis and challenges, and that it delivered the results expected. However, the objective of increasing Member State and EU resilience and preparedness for handling future cybersecurity challenges and opportunities remains difficult to assess. Now, the agency expects the EU cybersecurity index to serve as a benchmark and therefore to help assess how this objective will be met in the future. Concrete steps have been taken in this direction and relevant KPIs have been introduced in the 2023 SPD accordingly. While the activity has made substantial and solid steps towards obtaining the strategic objective, it is yet to reach the desired level of agency-wide information and knowledge management. Further resources dedicated to that goal should be reserved. Moreover, looking ahead at the challenges and requirements posed by NISD2 in the context of incident reporting, additional human and financial resources should be allocated to the relevant output. With 2022 being the year when the first ever ENISA cybersecurity foresight exercise was conducted and noteworthy results obtained, the opportunity to streamline relevant efforts and commence the integration of foresight at the core of ENISA's planning is highly valued..

Objectives



- Identify and understand future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase Member States' and Union's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities
- Understand the current state of cybersecurity across the Union
- Link cybersecurity needs with the EU research & innovation agenda in the field of cybersecurity

Link to strategic objective (ENISA strategy)



- Foresight on emerging and future cybersecurity challenges
- Efficient and effective cybersecurity information and knowledge management for Europe
- Empowered and engaged communities across the cybersecurity ecosystem

Results



- Decisions about cybersecurity are future proof and take account of the trends, developments and knowledge across the ecosystem
- Stakeholders receive relevant and timely information for policy and decision-making
- Research and innovation agenda tied to the cybersecurity needs and requirements

Outputs



8.1. Develop and maintain EU cybersecurity index

Outcome



In 2022, ENISA built on the 2021 work concerning the EU cybersecurity index. In collaboration with the ENISA NLO subgroup on the index (21 Member States participating) and under the strategic guidance of the ENISA Management Board (dedicated meeting held in March 2022), ENISA further refined the methodological framework and the list of

indicators for the cybersecurity index. In addition, ENISA developed and deployed a collaboration platform for the collection, management and analysis of the data for different Member States, allowing Member States to review and analyse their own data, and allowing ENISA to process the results concerning the EU cybersecurity index. To test the feasibility of the index framework and the platform, ENISA successfully conducted a pilot exercise of the cybersecurity index, in which 21 Member State actively took part. The results were processed and validated with the NLO subgroup on the index, and lessons learned on the use of the platform, the validation of the data and the presentation of the results were drawn. These lessons learned feed directly into the 2023 SPD work to refine and make the index framework more concrete and operational.

The added value of the EU cybersecurity index is to assess the level of cybersecurity across the EU and the Member States, and in doing so to identify the progress made in various directions. To this end, it was identified that the results of the index may in certain cases assist in assessing the efforts of ENISA to raise the level of cybersecurity across the Union. To this end, KPIs across ENISA activities will be refined in the 2023 SPD to take into account the results of the EU cybersecurity index. Moreover, to further showcase the value of the work on the index, ENISA will focus its efforts on identifying use cases for the effective utilisation of the results of the index by the Member States.

The work delivered under output 8.1 for the cybersecurity index will greatly contribute to the efficient and effective delivery of the NISD2, Article 18, report on the state of cybersecurity in the Union. To this end, further engagement with the Commission, the NISCG and the CSIRTs Network is expected, as is additional work to cater for the requirements set out under Article 18 of NISD2. It is thus expected that additional resources may be required to support the work under output 8.1.

8.2. Collect and analyse information to report on the cyber threat landscapes

In 2022, ENISA continued its year-long efforts in collecting and analysing information to report on the cyber threat landscape. The latest annual report, ENISA Threat Landscape 2022, was published in October 2022, and additionally, dedicated threat landscapes on ransomware (July 2022) and foreign information manipulation and interference (December 2022 in collaboration with EEAS) were also created. A dedicated conference on CTI was held in December 2022, with around 100 participants. In its efforts, ENISA is supported by the dedicated ad hoc working group on cyber threat landscapes.

The output is well defined and directly serves ENISA's statutory task to perform long-term strategic analyses of cyber threats and incidents (Article 9 (2), CSA) and fulfils ENISA strategic objective SO7 on efficient and effective cybersecurity information and knowledge management for Europe. ENISA has been working on an integrated approach and platform for managing information and knowledge on threats and incidents to deliver threat landscapes in a timely, accessible and service-oriented manner. To this end, an open and transparent methodology was published in 2022 to promote the consistency and validity of ENISA's work.

The added value of the output in ensuring that information and knowledge is shared and expanded within the EU cybersecurity ecosystem is undeniable, given the high recognition that ENISA's threat

landscapes receive from the community. However, moving forward, the KPIs to assess the performance of the output, and particularly its outreach, need to be refocused. This is an effort that ENISA will be undertaking as part of the 2023 SPD.

8.3. Analyse and report on incidents as required by Article 5 (6) of the CSA

In 2022, 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 EEC, Article 40. Moreover, ENISA supported the NISCG by analysing and reporting incidents reported under the NISD, Article 10 (3).

ENISA has 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. In doing so, ENISA has built on its previous work on an incident-reporting system, which has been enriched in functionality, thus allowing rapid processing and extraction of trends and patterns. Significant efforts were made in 2022 to prepare NISD2, to address the need to rehaul the incident-reporting regime and relevant tools, and to promote better internal knowledge management (synergies between incident reporting, threat landscapes and situational awareness were identified during the inception and closure of relevant projects).

The work on incident reporting is not only a statutory task of ENISA; it is more importantly an integral piece of work to better support 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 NISD2. Looking ahead to 2024 and NISD2, the consolidation of all three incident-reporting streams under the NISD2 umbrella, the more frequent reporting of incidents to ENISA (every trimester instead of annually) and the increased number of applicable sectors will undoubtedly require additional resources, including an expansion of the capacity of current IT systems. One additional area for improvement involves the better uptake of the recommendations of ENISA's analyses, and to this end refined and targeted KPIs will be introduced in the 2024 SPD.

8.4. Develop and maintain a portal (information hub), a one stop shop to organise and make available to the public information on cybersecurity, and establishment of procedural framework to support knowledge management activities maximising synergies with the European Cybersecurity Atlas

In 2022, ENISA continued its multiannual work on delivery of the infohub by materialising the framework defined in the initial phase within the design of a prototype for testing the approach and the supporting infrastructure. This pilot testing was an opportunity to evaluate how to link knowledge and information from multiple sources, while bringing added value and supporting Member States' efforts in sharing best practices and public information to enhance the level of cybersecurity in the EU.

The functional concept has been tested with the support of experts appointed by 11 Member States. The work done and the prototype were appreciated, with constructive feedback given, which indicated that it could be optimised in the next phase and focus on a specific

audience, and that cybersecurity professionals are best suited to be the initial target group.

For the next stage of development, the lessons learned will be integrated into adjustments and usage optimisation, while introducing alternative ways of content visualisation, thus aiming to support information sharing within the cybersecurity ecosystem and maximise synergies with other projects.

8.5. Foresight on emerging and future cybersecurity challenges and recommendations.

In 2022, ENISA worked on three streams, in line with Article 9 (1) of the CSA. The agency conducted the first ever cybersecurity foresight exercise – with the participation of the ENISA Advisory Group, the ad hoc working group on foresight for emerging and future cybersecurity challenges, and representatives from EU-Cyclone and the CSIRTs Network – to identify cybersecurity threats in 2030. This work identified topic-specific trends and assessed potential threats regarding the expected societal, legal, economic and regulatory impacts of technological innovations on cybersecurity, and in particular the top 10 cybersecurity threats for 2030. The work built on ENISA's methodology, which was defined in 2021. In April 2022, the flagship conference Threathunt 2030 was organised, bringing together the cybersecurity communities to discuss future challenges and to collectively pave the way forward. This work fully delivers on ENISA's strategic objective SO6 on foresight regarding emerging and future cybersecurity challenges.

In addition, the agency conducted targeted analyses of emerging technologies and particularly AI and post-quantum computing. With the support of the ENISA ad hoc working group on artificial intelligence, a report on security and privacy controls for four distinct AI use cases was delivered, identifying the particularities of different applications of use. Acknowledging the potential risks and opportunities of post-quantum computing, the agency published a report on its integration, exploring the necessity to design new cryptographic protocols and integrate post-quantum systems into existing protocols.

The significance and added value of this output in enhancing preparedness for emerging challenges and conducting foresight allows the definition of early mitigation strategies to improve the EU's resilience. Given the vast field of emerging challenge, it is essential for ENISA to have a mechanism in place to prioritise areas where dedicated studies will be conducted. Accordingly, in order to identify the topics for targeted recommendations and analyses, the agency has put forward a methodology to incorporate and take up the results of the regular foresight exercises, also involving the ENISA Advisory Group. This methodology will enhance the scope and focus of the output to better contribute and bring added value to obtaining strategic objective SO6. Moreover, in anticipation of the 2023 SPD, ENISA will further refine relevant KPIs to ensure a better assessment of the impact and uptake of its work.

8.6. Contribute to the Union's strategic research and innovation agenda and programmes in the field of cybersecurity (annual report)

In 2022, ENISA focused on three main themes: securing AI and AI for cybersecurity, improving Europe's cyberdefence (SOCs technology) and promoting a risk management culture through cyberinsurance. ENISA aimed to answer fundamental questions on what needs to be researched and how to create an environment conducive to cybersecurity innovation. The agency examined existing research, identified gaps, and analysed emerging and future trends in technological innovation. From the results, a list of 40+ recommendations and 5 priority areas for cybersecurity research and innovation were identified. ENISA also produced recommendations for building stronger foundations for cybersecurity research and innovation, as a plan to harness the results. The scope and the findings of this work were validated with experts, members of the research and innovation community and representatives of industry during two round table discussions. These recommendations were further detailed and explained in separate reports and summarised in ENISA's annual brief on research and innovation for 2022.

For 2023, within the 2023–2025 SPD, Activity 10, 'advise on research and innovation needs and priorities' was created, and therefore this output was reorganised into outputs 10.1, 'consolidated cybersecurity research and innovation roadmap across the EU', and 10.2, 'collect and analyse information on new and emerging information and communications technologies in order to identify gaps, trends, opportunities and threats (research and innovation observatory)'. The aim is to decouple the identification of emerging and future trends on technology research and development from the process of producing relevant, informed, timely and well-supported advice on research and innovation, and deployment needs and priorities.

8.7. Advise on potential investment priorities (e.g. capacity building and market & industry) and emergent cyber technologies in particular supporting the activities of the Competence Centre and the Network

In 2022, ENISA carried out multiple activities with the ECCC and the NCCs. To better define and plan these activities, ENISA prepared a memorandum of understanding (MoU) with a framework for cooperation and development of synergies with the ECCC. The team also contributed to the preparation of a service-level agreement to assist the ECCC with accounting and data protection officer services. ENISA contributed to the preparation of the ECCC strategic agenda with the 'way forward' report and was an active member of the ECCC Governing Board Working Group 4. ENISA initiated the co-chairing of the ECCC Governing Board Working Group on Skills and also contributed to the preparation of the community guidelines as a member of the Governing Board Working Group 3. The agency also organised several physical meetings with the NCCs to discuss the ECCC SPD and agenda, and hosted five webinars covering the topics of certification, skills, training tools, innovation and community engagement.

In 2023, within the 2023–2024 SPD's Activity 10, 'advise on research and innovation needs and priorities', this output has been renamed as 'provide strategic advice to the EU agenda on cybersecurity research, innovation and deployment'. The aim is to better align the output with Article 11 of the CSA, and thus to focus on advising stakeholders, including the ECCC and NCCs, on research and innovation, and deployment needs and priorities.

Key performance indicators ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge, including contributions to the research and innovation agenda	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
8.1. Number of users and frequency of use of a dedicated portal (observatory)^a					
8.2. Total number of recommendations, analyses and challenges identified and analysed	Number	Annual	ENISA reports and studies	288	357
8.3. Number of requests from Member States and EU research and innovation entities to contribute to, provide advice on or participate in activities	Number	Annual	Internal report	N/A	63
8.4. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research (survey)	%	Biennial	Survey	N/A	91.5 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	94 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	90 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	86 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	94 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	94 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	91 %
Allocated FTEs as per SPD, based on full establishment at 2022 year end	10	Actual used FTEs		10.90	
Planned budget (direct costs only)	EUR 1 051 950	Consumed budget (direct costs only)		EUR 1 043 564	
		Of which carried over to 2023		EUR 81 543	

a Infohub has yet to be implemented.

ACTIVITY 9

Outreach and education



ENISA supported the objective of engaged and empowered stakeholders by designing and implementing cybersecurity awareness campaigns and contributing to bridging the global cybersecurity skills gap through education and capacity building. This activity contributes to achieving behavioural change in operators of essential entities not only through tailor-made campaigns and awareness material but also through promoting good cybersecurity practices.

Achievements

The greatest achievement in 2022 (as reported under Activity 3) was the publication of the ECSF following 2 years of rounds of consultations with the academic and industry community. The ECSF categorises cybersecurity-related professions into 12 profiles and outlines key competences and skills for each profile, offering a common 'language' for professionals so that they can make an informed decision when choosing cybersecurity as career path. The activities on skills are reported under Activity 9 as of the 2023 work programme.

Another great achievement was the publication of the first version of AR-in-a-Box (awareness raising in a box), a set of tools provided widely to the public that enables professionals to design and run their own tailor-made cyberawareness programmes. The level of interest in supporting AR-in-a-Box is already high; numerous operators have recognised the value it offers. On these grounds, ENISA prepared to deliver in 2023 an online course that would be publicly available to the community.

Towards the end of 2022, ENISA published for the first time a report related to cybersecurity in education. This publication stems from requests from the Member States for information to better understand national activities on the topic; however, owing to resource constraints, a platform and mechanism were not developed. In 2023, the work undertaken in this area has been boosted with its own dedicated budget under output 9.6.

Budget constraints also affected the number of activities that were planned as part of the ECSM campaign and other sectoral campaigns. Events were limited to virtual workshops, and physical participation in conferences and stakeholder activities was a low priority. This scaling down did not support the overall objective of promotion and dissemination.

Resources

Budget consumption reached 98.8 % in 2022. The 30 % that was carried over stems from the time frames of certain activities, for example ECSM, which is organised from October, allowing only a few weeks before the end of the year for data collection and analysis. From 2021, the team increased resources for the OES campaigns and AR-in-a-Box and took on communication sector-related tasks. However, the adoption of NISD2, with new additional sectors, will require an increase in resources for output 9.1 and sectoral campaigns.

The recently published European Commission communication on the Cybersecurity Skills Academy (April 2023) requires ENISA to take several actions to reduce the skills gap currently identified in the EU, demanding even more resources (both budgetary and human) to be invested in the cybersecurity skills output (2023 SPD, output 9.5).

To increase outreach to the wider community, including SMEs (which constitute 93 % of the European market), language barriers need to be overcome. Several activities were designed to mitigate this issue, including material translation and dissemination (e.g. presence at national events with material in local languages). However, budget constraints have affected and will further affect this activity, which requires more resources for promotion and dissemination.

As regards FTE resources, the team gladly welcomed new members in September 2022, following an unscheduled call for support due to an unforeseen staff shortage (0.75 FTEs were allocated from September 2022 to the awareness and education team). Nevertheless, Activity 9 outputs are managed by two teams (the

Awareness and Education Team and the International Cooperation Team), which, like all horizontal teams, face the challenge of having no fully dedicated team members but instead team members who contribute in various percentages towards the team and operational unit, meaning that staff allocation can change each year. The upcoming tasks deriving from the European Commission communication on the Cybersecurity Skills Academy will further increase the need for resources (both human and budgetary) under this activity (output 9.5). This demands reprioritisation of resources and tasks, particularly those directed towards largely obsolete projects.

During the course of 2022, the Awareness and Education Team contributed approximately 0.2 FTEs to the support action.

It is estimated that approximately 0.7 FTEs are used by its operational human resources to perform technical/corporate/administrative tasks (secretarial work – minutes etc. – and administrative reporting, event and project management, communication, etc.) within this activity.

This activity (involving both the Awareness and Education Team and the International Cooperation Team) requires an increased missions budget because of the nature of the projects, which build synergies and increase outreach across the EU and internationally.

Overall assessment

Given the resource limitations, this activity delivers the intended result of engaging stakeholder communities in Europe and beyond. Targeting specific stakeholder groups (e.g. SMEs) and empowering them to improve their cybersecurity posture still has a long way to go; however, ENISA has now created the tools to support SMEs in this endeavour. Activities around diversity were redirected and rescope into the #CyberAll concept (which did not exist in 2021) and focused on empowering young girls and women by offering upskilling opportunities (in collaboration with the Capacity Building Unit under the training and exercises service package).

At the same time, the cybersecurity skills shortage became a shared responsibility, and key stakeholders joined forces towards closing the gap through education, proper career development and capacity-building activities. This joint movement will bring more tasks and more responsibilities to ENISA, along with the need for additional resources. To this end, a new objective has been proposed to be introduced in the draft 2024 SPD to align cybersecurity market demands with the supply of skilled professionals.

Responses to the stakeholder survey included positive remarks on the projects managed within Activity 9. The team is managed three ad hoc working groups (on enterprise security, cybersecurity skills and awareness raising) and the ECSM coordinators group, with great success. As regards output 9.4, that KPI was not delivered because of constraints on external sources; it has been proposed that the draft 2024–26 SPD is updated to reflect the requirements of NISD2 Article 18 (1). It needs to be taken into account that the result of this KPI cannot be attributed solely to ENISA's support actions (the level of awareness derives from numerous sources). At the same time, survey responses provided comments on 'duplication of efforts', which mainly stems from the activities surrounding ECSM; on this matter, the agency strongly believes that ECSM should be delivered back to the Member States so that they can tailor their activities to their audience's needs, with ENISA adopting a community coordination role.

In the draft 2024 SPD, output 9.5 has been renamed as 'Support the implementation and uptake of the ECSF' to better reflect the scope of the output, and further links with the European Commission Communication on the Cybersecurity Skills Academy are expected to be included.

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

Link to strategic objective (ENISA strategy)



- Empowered and engaged communities across the cybersecurity ecosystem

Results



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

Outputs



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

Outcome



In an effort to increase cyberawareness in the essential sectors, the agency designed and delivered two cybersecurity awareness-raising campaigns, one dedicated to the healthcare sector and one dedicated to the energy sector. The goal was to enhance the level of awareness of employees in these sectors on trending cybersecurity threats and, as a result, reduce the number of cybersecurity incidents or minimise their impact. Tailor-made material was prepared and promoted through multiple channels.

Moreover, under this output, the agency launched a framework for building cybersecurity culture – AR-in-a-Box – based on experiences from capacity-building and awareness-raising activities and with the input of relevant stakeholders. The goal was to help organisations and private companies to build their own awareness programmes in a low-cost and efficient manner to improve cyber hygiene and their internal cybersecurity culture.

The overall feedback collected was positive, and this is evident from the exponential increase of requests from stakeholders to formalise the content for widespread utilisation. The gamification element was a novelty that was applauded by the stakeholders. The content was reviewed by a wide community of stakeholders, including health and energy (electricity) operators, who validated the content as part of the sectoral cyberawareness campaigns. After all, changing an organisation's culture begins within the organisation itself.

This activity correlates with the activities related to the NISD and capacity building, creating a full cycle of service offerings to stakeholders. The service will be further formalised in the coming year and offered in different settings; this is a priority for the agency.

This output has been renamed in the draft 2024–2026 SPD to reflect NISD2 requirements. This output will require additional resources in 2024 because of the new sectors that are emerging as critical under NISD2 and the high demand for the service. In addition, in the future, AR-in-a-Box could be resourced by a payable services model.

9.2. Promote cybersecurity topics, education and good practices on the basis of the ENISA stakeholders' strategy

Under this output, the agency aims to assist SMEs and the wider community in improving their cybersecurity posture by creating and promoting several kinds of material, for example videos, tools, visuals, physical events and expositions. The goal is to inform the general public, SMEs and cybersecurity professionals about pertinent cybersecurity topics to promote best practices and increase the outreach of Member States and ENISA recommendations.

It was quickly identified that increasing outreach to include SMEs would require building strong synergies at national level (because of language barriers). On these grounds, ENISA participated in events across the EU (e.g. the IT Security Expo and Congress and the International Cybersecurity Forum) to make a strong case for improved cybersecurity. More Member States are supporting the action and organising similar activities with the support of ENISA in 2023.

The concept of #CyberAll was created to increase diversity in cybersecurity, and a combination of capacity-building and awareness-raising activities was organised, with capture the flag for girls, a girls' panel in the Skills Conference, podcasts on role models in ENISA, etc. Insightful discussions between experts in the field on numerous technical topics took place to promote female role models.

On certification, the team designed video material and launched two campaigns to promote and raise awareness of EU cybersecurity certification, and organised and participated in several conferences and talks on IT and the cybersecurity ecosystem, with the aim of building promotional content on cybersecurity certification and initiating dissemination in order to grow the cybersecurity certification community. In this light, promoting cybersecurity certification should be integrated with the actions in Activity 7.

The education aspect of this output was moved in the 2023 work programme under output 9.6 because of high demand and the need for specific resources.

9.3. Implement ENISA's international strategy and outreach

The ENISA Management Board approved the ENISA international strategy in November 2021, which is annexed to the 2022–2024 SPD as a separate document and available on the ENISA website.

The following were the main achievements in 2022.

- An agency-wide process was established to enable international cooperation in accordance with the agency's international strategy policy.
- Through the agency-wide process, ENISA handled five outreach engagements and three assisting engagements, and evaluated 86 requests for limited engagements.
- The agency established internal practices and roles to allow it to respond rapidly to service requests.
- It established points of contact and processes to liaise with key EU stakeholders such as EEAS, DG Connect and DG Neighbourhood and Enlargement Negotiations. This has enabled the agency to appropriately implement the international strategy and to be considered a strategic partner for external actions on behalf of the EU.

- The agency enhanced its efforts to support the EU action in response to the Russian war of aggression against Ukraine, in particular by moving forward a cooperation agreement with selected Ukrainian entities.
- Supported internally with international relations meetings (with Australia, Mauritius, Moldova, Montenegro, Singapore, NATO and the Association of Southeast Asian Nations).
- The process was established for concluding cooperation agreements with international partners. The process has allowed the agency to progress towards the closure of strategic agreements with the NATO Communications and Information Agency, State Special Communications Service of Ukraine, National Coordination Center for Cybersecurity of Ukraine and US Cybersecurity and Infrastructure Security Agency.
- Participated in two cyber dialogues (between the EU and Ukraine and between the EU and the USA).

In this work the agency supported strategic objectives 1–5 and 7.

The high level of interest in the agency's international engagement has led to significant progress in key areas. Regular updates and discussions have taken place at both Executive Board and Management Board levels, and the agency has also worked very closely with both the Commission and EEAS. There has been increased interest from the international community in interacting with the agency, which points to the need to further enhance and prioritise efforts in accordance with the agency's international strategy.

The agency will continue its ongoing cooperation with the USA in accordance with the EU-US cyber dialogue; strive to finalise the working arrangements with Ukraine, the USA and NATO; and cooperate with the Organisation for Economic Co-operation and Development in areas of mutual interest in which cooperation has not already occurred and pursue achievable actions under the identified cooperation areas. It is also intended that new opportunities for regional cooperation will be sought with countries from the western Balkans and the Eastern Partnership, in coordination with the EU Cyber Capacity Building Board.

As an indication of future progress, a key aspect will be to consolidate the different initiatives for formalised international cooperation, which in the coming years could further develop and improve the quality of collaborations, reducing the necessity for limited engagements and maximising impact through assisting and outreach approaches.

9.4. Organise European cybersecurity month (ECSM) and related activities

Users are the first line of defence in the cybersecurity chain, which has made awareness-raising an imperative, and as a response to this the 2022 ECSM campaign focused on two of the most prominent threats:

- phishing, so that users may detect and react to the most common attack against individuals;
- ransomware, so that users become aware of the threat, learn how to identify it and react appropriately to it, and realise its severity by getting to know its consequences.

The target audience of the campaign was employees aged between 45 and 65 years, in an attempt to address the gap that exists between younger and older generations where digitalisation is concerned, and also because ransomware is one of the predominant threats, with great potential to damage corporations.

2022 was the tenth anniversary of the campaign, which was celebrated with – among other things – the production of a ‘crowdsourcing’ video that brought together the testimonies of people from all Member States and organisations that have made ECSM possible over the years.

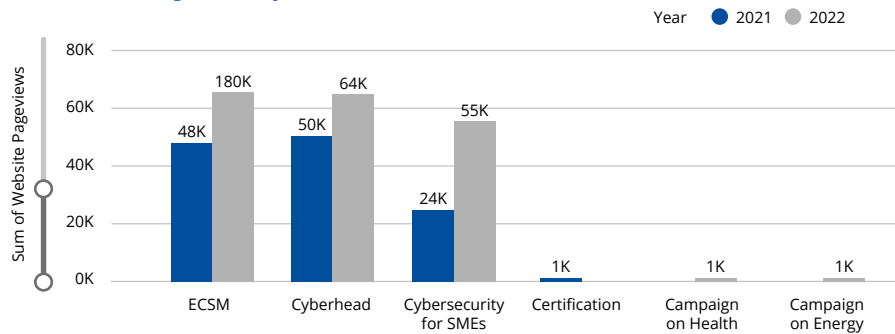
Another novelty in 2022 was the introduction of the ECSM awards. The aim of these is, on the one hand, to increase visibility of the excellent and creative material the Member States have produced in recent years under the ECSM umbrella, and, on the other, to increase engagement and encourage potential synergies. Member States put forward national material to compete in the categories of best video, best infographic and best educational material. Winners were widely promoted by all ECSM partners.

The agency, together with the ECSM national coordinators, agreed on the evolution of ECSM, spreading activities throughout the year, with the number of events peaking in October. Stronger collaboration mechanisms have been set up in the group to enable information sharing, which should result in a greater impact and cause behavioural change. Further reflection on the campaign design and development indicated the need for the agency to outsource the campaigns logistics to a trusted partner and to focus its activities on community building and identifying synergies to increase uptake. This is in line with the feedback on the duplication of efforts received from stakeholders through the ENISA stakeholder satisfaction survey. After 10 years of ECSM, Member States show greater maturity and a better understanding of target audiences.

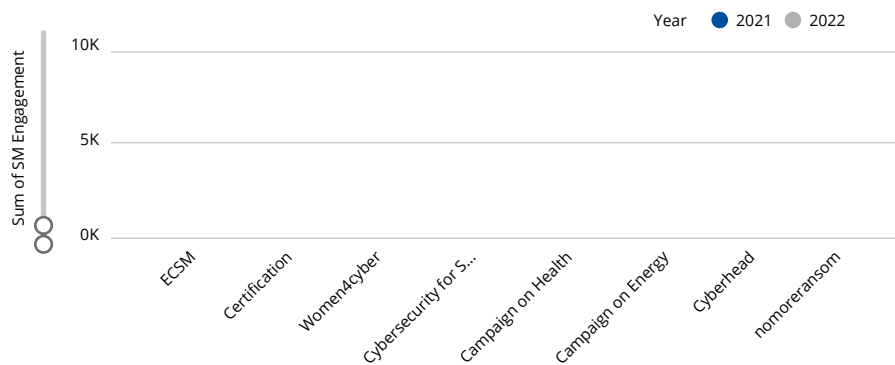
Key performance indicators Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU Level of outreach	Unit (of measurement)	Frequency	Data source	Results 2021	Results 2022
9.1. Number of cybersecurity incidents reported having human error as a root cause	Number	Annual	CIRAS tool	173	153
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	20 756 630	27 278 491
Total social media engagement	Number	Annual	ENISA analytics	117 720	19 301
Total video views	Number	Annual	ENISA analytics	2 021 129	6 602 355
Total website visits	Number	Annual	ENISA analytics	123 504	300 530
Total participation at events	Number	Annual	ENISA analytics	5	40

Results by ENISA activity

Website Pageviews by Area and Year



Social Media Engagement by Area and Year



Key performance indicators	Unit (of measurement)	Frequency	Data source	Results 2021	Results 2022																											
Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU Level of outreach																																
<div><p>Social Media Impressions by Area and Year</p><table><caption>Social Media Impressions by Area and Year</caption><thead><tr><th>Area</th><th>2021 (K)</th><th>2022 (K)</th></tr></thead><tbody><tr><td>ECSM</td><td>204</td><td>200</td></tr><tr><td>Certification</td><td>86</td><td>200</td></tr><tr><td>Women4Cyber</td><td>201</td><td>83</td></tr><tr><td>Cybersecurity for S...</td><td>44</td><td>36</td></tr><tr><td>Campaign on Health</td><td></td><td>58</td></tr><tr><td>Campaign on Energy</td><td></td><td>57</td></tr><tr><td>nomore ransom</td><td>54</td><td></td></tr><tr><td>Cyberhead</td><td>25</td><td>21</td></tr></tbody></table></div>						Area	2021 (K)	2022 (K)	ECSM	204	200	Certification	86	200	Women4Cyber	201	83	Cybersecurity for S...	44	36	Campaign on Health		58	Campaign on Energy		57	nomore ransom	54		Cyberhead	25	21
Area	2021 (K)	2022 (K)																														
ECSM	204	200																														
Certification	86	200																														
Women4Cyber	201	83																														
Cybersecurity for S...	44	36																														
Campaign on Health		58																														
Campaign on Energy		57																														
nomore ransom	54																															
Cyberhead	25	21																														
9.3. Geographical and community coverage of outreach in the EU	Number	Annual	ENISA analytics	N/A	All 27 MS and EFTA countries																											
9.4. Level of awareness of cybersecurity across the EU / general public (e.g. EU barometer and other) ^a	N/A	Biennial	Survey	N/A	N/A																											
9.5. Stakeholder satisfaction with awareness raising and education activities	%	Biennial	Survey	N/A	91 %																											
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	100 %																											
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	80 %																											
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	84 %																											
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	95 %																											
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	86 %																											
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	98 %																											
Allocated FTEs per SPD based on full establishment at 2022 year end	5	Used FTEs		5.22 ^b																												
Planned budget ^c	EUR 439 900	Consumed budget ^c		EUR 415 122																												
		Of which carried over to 2023		EUR 125 341																												

NB: CIRAS, Cybersecurity Incident Reporting and Analysis System.

^a This KPI has been proposed to be updated in the draft 2024–2026 SPD to reflect the requirements of NISD2 Article 18 (1).

^b The FTE count includes resources allocated under output 3.8 of Activity 3.

^c Direct costs only.

ACTIVITY 10

Performance and risk management



Activity 10 seeks to meet requirements set out in Article 4 (1) of the CSA, which sets as an objective for the agency to 'be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks'.

This objective requires an efficient performance and risk management framework, and the development of single administrative practices, including a quality assessment framework, proper and functioning internal controls and compliance checks. In terms of resource management, the Budget Management Committee ensures that the agency adheres to sound financial management, and the Information Technology Management Committee (ITMC) ensures comprehensive and coordinated governance of the agency's IT systems and services.

Achievements

In 2022, ENISA adopted its own enterprise risk management methodology, and it was applied in enterprise and IT security risk assessment. The results are detailed in the corresponding chapter of the 2022 AAR, as it provides input to overall internal control assessment. Moreover, ENISA revamped its internal control framework indicators to better monitor internal control targets and the achievement of objectives. Both the risk framework and the internal control framework are linked to the ENISA corporate strategy.

Preparation for the roll-out of a project management tool was undertaken in 2022, mapping the tool's processes against the SPD implementation guidelines and configuring it in accordance with internal practices for project managers in order to ensure usability and single administrative practices by staff.

In addition, ENISA liaised with the EU Agencies Network in relation to a pilot in preparation for the upcoming regulation on cybersecurity at EUIBAs ^(a), with the aim of establishing a cybersecurity framework for EUIBAs and supporting the overall implementation of the new regulation within the agency's network.

In 2022, the agency carried out the first audit of ENISA's emissions levels that included recommendations. These recommendations feed into the corporate strategy for achieving climate neutrality by 2030.

Progress was achieved by the ITMC with regard to IT policies. The ITMC developed a number of key policies throughout the year, including the IT security policy.

During the course of 2022, a number of projects were postponed by the Management Team, in particular (1) the roll-out of Advanced Record System (ARES), the agency's document management policy and system, (2) the business continuity strategy and related implementation plans, and (3) the migration of the ENISA website and associated portals to Commission services. The second and third projects could not be implemented because of lack of adequate resourcing (human and budgetary), despite being actions with the potential to significantly reduce the enterprise risk level according to the internal control assessment. In 2022, the risk management framework was prioritised over the completion of the business continuity strategy.

The communications stepped up its monthly reporting during the year at the Management Team meetings, presenting the results of the previous month's activities and presenting the ENISA events planned for the coming months, with more accurate projections to improve support for publications and communications.

Resources

Outputs 10.2, 10.3 and 10.5 were implemented with reduced scopes, as follows.

- The migration of the website and associated portals to Commission services as per the IT strategy was postponed. They were outlined in the internal risks assessment as high risk due to dependency on a single external contractor. The implementation of the project requires approximately EUR 350 000 as per assessment from Commission services. This should be deemed a priority in the coming years, as the current solution poses a risk to the agency.

- Development of the business continuity strategy and related implementation plans was postponed to 2023 due to lack of human resources and capacity within the unit to address several projects simultaneously. Preparatory work was carried out in 2022 with the support of an external contractor, but finalisation was not completed because risk assessment framework revision was prioritised.
- The major updates to the agency's document management policy and system, and the change of tool, were postponed to 2023 because of workload and the limited capacity within ENISA to address the migration needs because of the agency's prioritisation of the introduction of the Mission Information Processing Tool (MIPS). Due to this postponement, a commitment of approximately EUR 23 000 was cancelled.

In addition, the audit of ENISA's emissions levels was carried out as an additional workload and on a best-effort basis, with the help of volunteers from the staff greening committee because of the departure of a senior staff member and no availability for resourcing this gap.

In addition, this activity supported the cybersecurity support action under Activity 5 by providing visual material, translation coordination and legal advice amounting to 0.05 FTE in total.

Overall assessment

Some outputs had reduced scope owing to reduced FTE availability and were implemented on a best-effort basis, which in the long term is not sustainable because of the statutory nature of these outputs.

Activity 10 met its objectives for 2022. The results for this KPI show that expected compliance levels were met. At the time of writing, the agency is developing its corporate strategy to assess how this objective will be met in the future. Concrete steps have been taken in this direction and relevant KPIs have been introduced for the 2024 SPD. Although substantial steps have been taken under this activity towards achieving this strategic objective, reaching the level of single administration in practice is yet to be achieved, as are the business continuity strategy and the website and portals migration. Looking ahead at the challenges and requirements posed overall, and associated compliance and risk mitigation measures, additional human and financial resources should be allocated to the relevant activity by at least filling the gap between the planned FTEs and the actual FTEs. With 2022 being the year when ENISA's first ever enterprise risk assessment was conducted, complementing the overall assessment of internal controls, it is recommended to streamline relevant efforts and commence the integration of ex post and ex ante evaluation with ENISA's outputs related to Activity 8 on foresight.

On the basis of the corporate strategy, this activity will be restructured. A proposal has been made for the draft 2024–2026 SPD to consolidate a number of the outputs and to create a new output specifically for providing support services in the EU Agencies Network and in key areas of the agency's mandate.

Objectives



- Increase effectiveness and efficiency in achieving Agency objectives.
- Fully comply with legal and financial frameworks in performance (i.e. build a culture of compliance).
- Protect the Agency's assets and reputation, while reducing risks.
- Achieve full climate neutrality of all operations by 2030.

Link to corporate objective



- Sound resource and risk management

Results



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

Outputs



10.1. Implementation of performance management framework

Outcome



The implementation of the performance management roadmap continued throughout 2022 with the following achievements.

- External stakeholder dimension. An administrative note on the implementation of the stakeholder strategy was produced, containing definitions and the procedures for its practical implementation.
- People and capabilities domain. This was addressed within Activity 11.
- Organisational culture dimension. The communications sector provided a continuous information flow through weekly question and answer sessions and intranet notifications, among other things.
- Internal processes dimension. The configuration of a new project management tool was initiated during the course of 2022 and configured in accordance with the agency's SPD implementation guidelines.

With the introduction of the corporate strategy in 2023, the performance management framework will be addressed through several outputs. In this way, synergies and interconnections between relevant activities are strengthened.

10.2. Implementation of communications strategy

The communications sector supports both the corporate and operational communication needs of the agency, liaising with actors from across the activities to align communications efforts with the communications strategy.

An administrative note on events guidelines was drafted, and staff received training on the new guidance, with recurring training for newcomers.

To implement the communications strategy, an action plan, of which 85 % was completed, and 22 individual communications plans (to prioritise the actions) were created with operational colleagues.

The communications sector published 53 press releases and news items throughout 2022. The activities around outreach resulted in 1 150 media mentions of ENISA in 2022, compared with 673 in 2021. During 2022, ENISA's work was downloaded 1.76 million unique times from our website, compared with 1.54 million in 2021.

10.3. Develop and implement risk management plans (including IT systems cybersecurity risk assessment, quality management framework and relevant policies and processes)

An enterprise risk management framework and an IT security risk management framework were developed and adopted.

An enterprise and security risk assessment was conducted and adopted in 2022.

Action plans for risk mitigation are under development.

It has been proposed that this output is merged with performance management output in the draft 2024–2026 SPD.

10.4. Develop and monitor the implementation of agency-wide budgetary and IT management processes

The ITMC developed a number of key policies throughout the year. A total of 17 policies (including IT security policies) were produced and 5 were approved, with 12 policies queued for approval in early 2023.

The ITMC reviewed and approved the IT budget for 2022 and monitored budget execution, using the global IT plan and the request process for new or modified systems. In this context, a total of 30 requests were handled, of which 17 were accepted, 8 were postponed, 2 were rejected and 3 were points of information.

The ITMC also reviewed the 2023 budget proposal and submitted a positive opinion to the Budget Management Committee. IT management processes were examined as part of the drive to renew the IT policy framework, and implementation of procedures and technology to mitigate known risk was tracked throughout the year.

In 2022, to actively monitor the implementation and the execution of the budget, the Budget Management Committee produced three interim budgetary reports and a final budgetary report at year end.

Key conclusions and lesson learned from 2022

- The main budgetary objectives of the agency were achieved.
- Except for the payment rate, the budgetary KPIs have improved compared with 2021.
- The implementation of the pilot support action fund was possible thanks to the additional workloads taken on by project managers, financial and budget actors, and the procurement team.
- The total budget increased by 72 % compared with 2021 (from EUR 22 833 000 to EUR 39 208 000).
- Budgetary execution slightly improved (99.93 % in 2022 v 99.51 % in 2021 v 97.35 % in 2020).
- Payment rate decreased (52.02 % in 2022 v 77.40 % in 2021 v 68.62 % in 2020).
- Transfers by Executive Director Decision decreased in number (three in 2022 v five in 2021 v seven in 2020).

Lessons to be drawn from 2022 will be internally analysed

- Strictly respect set deadlines to ensure timely implementation of projects.
- Increase the quality review of amounts carried forward.

It is proposed that this output is merged with the performance management and risk assessment output in the draft 2024–2026 SPD.

10.5. Implement single administrative practices across the agency

The principles for implementation of single administrative practices are addressed in the administrative note, which specifies the roles and responsibilities of ENISA's structural entities, putting in place organisational measures to ensure efficient performance of the agency's tasks and functions. The administrative support is centralised under the Executive Director's Office within a sector of administrative assistants seconded to the units, teams and committees.

With a view to establish a single administration at ENISA, it is necessary to introduce a document management policy and system (ARES), which is planned for implementation in 2023, with administrative assistants acting as focal points for units and teams.

The transparency calendar on ENISA's website is maintained by the administrative assistants as per the ENISA transparency policy.

A transition period to centralise the financial initiation function at ENISA started in 2021 and continued in the course of 2022.

10.5. Carry out an overarching audit on the CO₂ impact of all operations of the agency and develop and implement a targeted action plan

In 2022, the agency undertook an exercise to map its current climate footprint. Based on an audit of past ENISA emissions, for which 2019 and 2021 were used as reference years, it was established that ENISA creates 584 485 tCO₂e of greenhouse gas (GHG) emissions annually, with indirect emissions from purchased electricity (50.33 %) and air travel (36.80 %) being the main sources of impact on climate. Based on these results, an action plan was developed, particularly in relation to the main sources of ENISA's emissions: purchased electricity and air travel. The action plan is further detailed in ENISA's corporate strategy.

It has been proposed that this output is merged with performance management and risk assessment outputs in the draft 2024–2026 SPD.

Key performance indicators: Organisational performance culture Trust in ENISA brand	Unit (of measurement)	Frequency		Results 2021	Results 2022
10.1. Proportion of KPIs reaching targets	Number	Annual		N/A	Targets established as of 2023; however, compared with the base year (2021), 13 metrics were unchanged, 21 underperformed and 58 outperformed
10.2. Individual staff contribution to achieving the objectives of the agency through clear link to KPIs	%	Annual		53 %	64 % ^b
10.3. Exceptions in the risk register	Number	Annual		16	27
Deviation from financial regulations	Number	Annual		14	26
Deviation from staff regulations	Number	Annual		2	1

Key performance indicators: Organisational performance culture Trust in ENISA brand	Unit (of measure- ment)	Frequency		Results 2021	Results 2022
10.4. Number of complaints filed against ENISA, including inquiries/complaints to the European Ombudsman	Number	Annual		19	3
To the European Ombudsman	Number	Annual		3	0 ^c
Under Article 90	Number	Annual		15	3
Under Article 24	Number	Annual		0	0
To European Data Protection Supervisor	Number	Annual		1	0
10.5. Number of complaints addressed in a timely manner and in accordance with relevant procedures	Number	Annual		N/A	3 (complaints to the European Ombudsman under Article 90 (2) closed successfully in accordance with the relevant procedures and addressed in a timely manner)
10.6. Results of the annual risk assessment exercise – see Part III on the internal control framework					
10.7. 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		4	0
IAS	Number	Annual		Three important recommendations	The three important recommendations have been closed in 2023
ECA	Number	Annual		One critical observation	Four non-critical observations were issued by the ECA in its 2021 report. All observations prior to 2021 have been completed
10.8. Level of trust in ENISA ^d	%	Biennial		N/A	95 %
Allocated FTEs as per SPD based on full establishment at 2022 year end	19		Used FTEs	16.5	
Planned budget ^e	EUR 830 685		Consumed budget ^e	EUR 829 614	
			Of which carried over to 2023:	EUR 174 087	

AAR, annual activity report; ECA, European Court of Auditors; IAS, Internal Audit Service; N/A, not applicable.

a Proposal for a regulation laying down measures on cybersecurity at EUIBAs.

b Source of results taken from staff satisfaction survey question 'My contribution and annual objectives at ENISA have a clear link to the objectives and KPIs of the activity(ies) I contribute to'.

c Complaints submitted in late 2021 were closed in Q3 of 2022.

d Source of results taken from stakeholder satisfaction survey: 'agree' and 'somewhat agree' with the statement 'I am confident in ENISA's ability to achieve its mandate'.

e Direct costs only: consultancy, website and missions linked to Activity 10.

ACTIVITY 11

Staff development and working environment



This activity supported ENISA aspirations stipulated in Article 3(4), 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.

Achievements

In 2022, the Corporate Support Services unit managed to achieve day-to-day business continuity of critical services with resources being over extended, thus requiring use of overtime and surplus hours to fulfil activities.

In 2022, the Management Team found that there was a need to implement MIPS, the Public Procurement Management Tool, and an online tool to manage calls for expressions of interest from experts, digitalise recruitment and offer related online services, as well as to introduce ServiceNow as a corporate IT ticketing tool. However, the implementation and deployment of these projects were postponed to 2023, mainly because of the extra activities arising from the additional resource of EUR 15 million, which affected the Finance and Procurement Team.

In 2022, the unit started to revise its competency framework, appraisal process, learning and development process and strategic workforce review as first steps in forward planning. Some efforts were made in this regard, however, the overall competency framework revision was delayed to 2023, while some aspects were introduced in the appraisal and learning and development process in 2022 cycle. In terms of recruitment, the competency framework was included in the recruitment procedures.

In 2022, the unit also made some minor progress in the area of IT facility and security management. The IT budget was clarified, with a clear picture on budget allocation and the decision to outsource facility management services. Key findings and recommendations by ISO were implemented and continue to be implemented in 2023. Progress was made regarding SOPs, clarity of security procedures and the agency's preparations for the new European Union classified information (EUCI) requirements; however, a lot of activities were postponed because of constraints on resources (both human and budgetary).

Resources

The unit faced significant implementation delays, relying heavily on an external workforce to implement core functions. The number of ENISA premises (ENISA Athens Office, ENISA Heraklion Office, ENISA Brussels Office and the disaster recovery site in Alicante, Spain) and the breadth of corporate activities and projects for which the unit offers services and maintains business continuity are not always compatible with the resources assigned to the unit. In 2022, the Corporate Support Services unit reorganised its activities and, as a first streamlined step, created two main domains for its services: a resources sector (HR, host state matters, finance and procurement) and a security and infrastructure sector (facility management, security and IT). Overall, the unit faced significant challenges in 2022 due to a lack of human resources (FTEs) and financial resources as a result of resignations, reallocations of posts and the ongoing business service transformation.

The unit aims to start reversing its planning (financial, resources and procurement) in the upcoming cycle and integrating resource planning as a result of further streamlining and re-engineering of corporate services.

To meet its statutory obligations, the unit will need to review and scrutinise its current *modus operandi*, define a revised procurement strategy, integrate planning and resourcing and streamline using end-to-end user solutions, and invest in a different business model. In addition, to maintain business continuity across dispersed

locations, the unit needs to be equipped with an increased missions budget to be able to flexibly allocate and maintain standard services in all its locations, as its staff need to regularly visit other locations or split their time between the place of assignment and the place of business interest. Part of the stringent mission budget allocated to the Corporate Support Services unit prevented certain visits from occurring in 2022, such as visiting disaster recovery services in Alicante, performing continuation of business continuity services in Athens during summer and holiday periods, and advancing the implementation of specific actions, while also limiting training options for its staff. Preparing the agency for EUCI accreditation and Information Security Regulation parameters were among the key activities the unit had to deprioritise due to budgetary constraints.

This is the challenge the unit will still face in 2023. Resorting to external service providers (intro muros and interim agents) to increase the capacity of the unit. Besides that, the unit, in order to continue path to reform, would need to be supported financially, as a majority of IT and other initiatives that aimed to improve the agency's performance and compliance had to be postponed due to lack of funds. The stringent Title I and Title II budgets limit the opportunities for existing staff to engage in more challenging and in-depth duties and duties of a more qualitative nature, and performing administrative duties of a certain nature remains an obligation, which needs to be further explored and reviewed.

Overall assessment

In 2022, efforts were made to focus on clarifying budgetary obligations while reviewing IT services. In addition, significant attention was given to defining and redesigning the scope of services with a project- / needs-based mindset. The unit focus was bringing ENISA back to basics while clarifying rules and procedures and thoroughly examining how things have been applied in the past; this required a lot of time, dedication and effort in order to map and identify areas with shortcoming in terms of people, processes, systems, policies and overall competencies that would assist the unit in increasing its maturity. The unit's structure was designed to allow it to provide small, agile teams that can absorb work and act fast. The service provision was also explored, and areas where the silo approach was applied were identified. In the course of 2023 and beyond, the unit will need to explore more flexible ways of working with end-to-end solutions, with the user at the centre. In 2023, the unit needs to finalise and implement a sound business continuity plan and review its IT structure and communication model to ensure that essential services are provided during absences or when otherwise requested.

Although a breadth of activities and services were delivered, many activities had to be deprioritised and put on hold owing to limited resources, additional workloads, aggregated sick leave, and absences that affected business continuity. The main gaps that hindered the implementation of the activities were outdated tools and procedures, limited technical know-how, and the need for competency development in policy analysis, communication and networking, data analytics, synthesis and problem-solving, project management and change management.

Overall, should resources not be assigned to the unit, the agency will face severe risks in terms of output delivery. First, regarding human resource management, the increase in sickness and absenteeism due to increased workloads was a serious red flag; historically, the team has not been properly allocated workforce time to deliver its services. The lack of budget to support the additional peak of work with intra muros services or maintain statutory obligations while a series of digital transformations are undergoing is a critical indicator that may jeopardise operational and overall agency expenditures. The lack of knowledge of its staff resulted in limited development options and prevented direct access to specialised legal, financial and staff regulation know-how, causing the agency to be at high risk overall, as the opportunities and solutions offered cannot adequately meet the agency's compliance and service needs. Limitations in the budget for training or consultancy, or access to networks, conferences or other forums of knowledge, also represent a risk to the agency and could slow down its growth.

In the draft 2024–2026 SPD, it is proposed that the five current outputs are consolidated into three distinct outputs and integrated in the corporate strategy: an output related specifically to the day-to-day management of horizontal services in the areas of resources and infrastructure; an output related to the implementation of the corporate strategy, including the HR strategy; and an output focused on enhancing operational excellence and secure ways of working.

Objectives



- Engaged staff who are committed and motivated to deliver and who are empowered to use fully their talents, skills and competences
- Digitally enabled workplace and environment (including home workspace) that cultivates and nourishes performance and enhances social and environmental responsibility

Link to strategic objective



- Build an agile organisation focused on people

Results



- ENISA as an employer of choice

Outputs



- 11.1.** Maintain and implement the competency framework in all HR processes (including in the training strategy, career development report, internal competitions and exit interviews)

Outcome



ENISA's competency framework has been in place since 2020. During the past 2 years, ENISA's HR unit has striven to embed the framework in all HR processes. Therefore, the 2022 appraisals exercise (reference year 2021) comprised of references to the competency framework. Even though the team did not manage to achieve the implementation and launch of the new simplified competency framework, a transitional step occurred in 2023.

As a result of an extensive consultation of the Management Team during the Management Team seminar on 5 December, consultations undertaken during various weekly Management Team meetings, and staff engagement and input through the Staff Strategy Day, five main competencies from the existing ENISA competency framework, which have been deemed crucial and as per one of the agency's aspirations to become a talent factory, have been identified and formalised in Administrative Notice 2023-01. They are also embedded in the 'ability' section of the appraisals that took place in 2022. ENISA's learning and development policy has been revamped to highlight a clear link between staff members' learning and development needs, as identified in their appraisals, staff members' competency levels and gaps to be filled in, thus allowing for targeted staff development, using the competencies as a basis. In terms of recruitment, ENISA's vacancy notices have been redrafted to consistently reference the required competencies to be demonstrated by potential candidates. During interviews with eligible candidates, one of the main components pertaining to behavioural questions, which are competency based, is embedded in the selection procedure. In addition, field assignments or practical tests are increasingly forming an integral part of the selection procedure. Limited efforts were made to apply competency-based selection procedures.

The unit also faced challenges in handling learning and development in line with the defined SPD priorities and competencies, and reflecting on the feedback received from the staff satisfaction survey and included in a revised learning and development framework. The relevant indicators in this activity clearly portray the gap between

the learning and development practices and the needs/expectations of staff (43 % mismatch between needs and expectations, as well as linkage with the career development report).

ENISA aims to complete the holistic integration of its competency framework during the course of the next SPD cycle through introducing job complexity criteria, linking competencies to grades and further refining technical versus transversal behavioural competencies. Unfortunately, during 2022, the Corporate Support Services unit managed to tackle this exercise only in a very limited way, mainly owing to overlapping priorities, lack of resources and limited technical know-how on the subject. In addition, all internal procedures need to be reviewed and redesigned with the end user in mind to reduce duplication of effort.

Some small efforts were made on recruitment, learning and development and appraisal processes, but the content-based results could have been better to foster faster implementation and an integrated plan of action. The lack of integration between financial data and activity-planning or staff-planning data also prevented faster progress, and considerable effort was made to clarify data and validate different sources of information rather than emphasising building the new way ahead.

Findings from exit interviews need to be further reviewed. The exit interview process needs to be reviewed with an eye to the added value it gives back to ENISA, since it needs to add qualitative value rather than the quantitative values currently obtained. The quantitative results do not add any value to the process, and they have not been used to improve any of the HR processes, mainly due to lack of time. Reflecting on the feedback received from the exit interviews, process improvement was handled procedurally, and significant work needs to be done on the onboarding and exit processes across the agency. While many difficulties regarding this process centre around the internal systems and procedures, more technical know-how needs to be applied, and the onboarding and exit process thoroughly revised.

The HR-related gaps concern technical know-how and subject expertise (specialised knowledge in talent management and development and modern HR practices), lack of resources in terms of budget (in order to obtain direct access to subject matter experts who could provide specialised advice on legal matters, compliance and technical HR practices reflecting a modern administration, consultancy and access to platforms to enrich knowledge sharing) and lack of integrated digital tools (in order to be able to synthesise, automate and extract data with greater efficiency). To reduce the burden of tedious, technical administrative work, the agency could budget for outsourcing such repetitive tasks, while maintaining and strengthening its internal workforce's capabilities for work of a more senior and qualitative nature. Currently, the team uses an interim workforce to ensure business continuity, which is a high risk strategy for the agency, as it outsources basic, core activities.

In the future, the team needs to further invest in upskilling and reskilling, not only in terms of its technical know-how but also in terms of the competency development areas of policy advice, analysis and synthesis, networking and communication, project management, change management and problem-solving skills, in order to meet the challenges of the future. As of 2023, work included in this output will need to be recalibrated, discontinued or redesigned with a different

goal in mind, as the day-to-day administrative services are not reflected in this output. Recalibration of work includes restructuring of roles and functions, continuously improving skills/competencies and developing expertise in line with the desired competencies. The agency is placing great strategic importance on the areas of HR management, integrated workforce analytics and talent development, in order to meet business challenges of the future.

11.2. Develop the HR strategy, with emphasis on talent development, growth and innovation

In 2022, some initial efforts were made to prepare the HR strategy and implement some fundamentals that are the cornerstone of sound administration. HR policies, their application and related know-how seem to be a struggle for HR staff, including managers; deeper knowledge in these fields of expertise is required. Thus policy analysis, developing HR policies and implementing provisions among actors meant that triggering and implementing changes proved to be a considerable challenge in 2022, and caused stress for staff assigned to these tasks. In addition, there seems to be a corporate overdependency on the administrative functions to perform tasks that are the responsibility of users and managers, which further strains the resources allocated to the unit. Thus, significant effort in educating others in the area of HR policies and practices, and the legal framework, needs to be made in the coming years.

The unit also faced challenges in integrating the SPD's priorities with the legal framework and general HR framework to its competency framework; and linking its reclassification and other HR processes (probation, contract renewal) to the new way ahead. In 2022, the unit aimed to revamp its corporate SWP process and conducted internal sessions to generate feedback from staff. The emphasis was placed on clarifying the legal framework and the framework of the staff regulation, the need for and purpose of continuous improvement, and the overall regime.

In terms of HR services, the model applied is quite outdated and is not fit to support ENISA's future challenges. The service-level agreement with the Paymaster Office (PMO) needs to be further explored and capitalised on, in addition to the modernisation of HR services, in order to alleviate the administrative burden further, simplify the nature of tasks and provide growth opportunities. The dependency of HR services on old financial practices brings risk, and efforts in 2023 need to further streamline HR and financial processes.

The team needs to invest further in improving and updating its technical know-how, but also in the competency development area of policy advice, analysis and synthesis, data analytics, networking and communication, project management and change management, and in problem-solving skills, in order to meet the challenges of the future. Besides that, integration of staff and financial data with data analytics and forecasting is crucial for the future and efforts need to be made by allocated staff to further their know-how in this area but also for the agency to align, integrate and build its planning, forecasting and data-driven decision-making by using modern and state-of-the-art technological solutions. To fulfil its objectives, the unit would benefit from specialised FTEs at relatively high grades, with specialised expertise in policy advice, law, talent acquisition and development, and general strategic HR skills, in order to drive its future corporate strategy and HR strategy.

In addition, significant work needs to be done on sickness and absence management as well as maximising advisory services to staff and managers in the unit's area of expertise. The agency did not take mitigating steps in 2022 to improve the welfare of its staff via dedicated medical service provision in the host state or complementary insurance, or by providing quality advice in this area to managers and staff. The agency tackled this issue purely from a procedural and transactional perspective while facing significant shortcomings in using the relevant digital tools, policy application and improvements. Therefore, the HR work performed in this area needs to be further reflected on and restructured in order to meet the challenges of the future and modernise the welfare provision of the agency.

With the introduction of the corporate strategy in 2023, the HR activities will be addressed via several outputs. In this way, synergies and interconnection between relevant activities are strengthened.

The strategy will focus on the main objectives and pillars of the overall corporate strategy of a 'human-centric organisation'. By placing the human at the centre of its operations and HR approach, the agency will steer activities around three main objectives:

- effective workforce planning and management,
- efficient talent acquisition, development and retention,
- caring and inclusive modern organisation.

This strategy aims to provide a clear understanding of the policy framework within which ENISA strives to implement sustainable and consistent HR management practices, and to acquire, develop and retain the best staff. The strategy is intended to serve as a central reference for all managers and employees, and complements the ENISA corporate strategy.

The overall corporate strategy also aims to introduce a corporate costing model in order to obtain the necessary support for providing the services to the operational activities. As the agency's operational activities increased, the corporate domain resources remained unchanged, creating significant strain for the people performing the tasks. Increased absenteeism rates, long working hours and increased stress levels, as pointed out in the results of the staff satisfaction survey, highlight the necessity to add more resources in the corporate area when increasing operational needs arise, in order to balance better staff well-being and business requirements.

Besides that, the strategy places significant importance on integrating financial, HR and corporate planning (including procurement planning). ENISA has identified shortages in this area and inefficiency in current practice. Besides the lack of integrated systems, relevant staff require reskilling and upskilling in the areas of financial management, project management, planning and forecasting. Significant emphasis on talent development and growth, competency analysis, and planning of learning and development needs and talents are needed, as well as an emphasis on succession planning and leadership needs; hence, greater emphasis needs to be placed on transferable competencies, policy analysis and advisory skills, tools, and integrating HR planning with planning and forecasting competencies and activities, and with budgeting. Therefore, in order to better support the agency's growing needs in the area of forecasting, planning, data analytics and reporting, the unit needs financial resources to invest in an integrated digital solution for financial

and HR management, financial and activity planning tools, and digital solutions for talent management.

The unit lacks resources and skills in the areas of talent development and growth, forecasting and planning, and uses a lot of temporary staff to ensure business continuity; this presents a risk to the agency, as the external workforce performs core activities in the absence of integrated systems and digital solutions. Considering the emphasis the agency will place in the future on strategic planning, forecasting and HR matters, the growing demand and its business requirements, additional resources in terms of both finance and FTEs are needed, while the existing efforts to upskill staff need to continue in order to meet the need for skills.

To do so, this output should be reviewed and redesigned. The whole operating model of the unit needs to be reviewed. Recalibration of its work includes restructuring of roles and functions, as well as continuously improving skills/competencies and developing expertise in line with the desired competencies required, since the agency is placing a great strategic demand on this area of HR management, integrated workforce analytics and talent development, in order to meet business challenges of the future.

11.3. Undertake actions to develop and nourish talent and conduct necessary management development activities

The actions undertaken to develop and nourish talent were twofold: firstly, ENISA invested heavily in developing and upgrading its staff's skills through its learning and development policy. It sponsored SANS training, as well as other relevant niche training, as defined in the respective staff members' appraisal reports. Thus, ENISA has ensured that it provides cutting-edge training options to its staff, to keep it abreast of new developments in the domain.

Secondly, a management seminar took place each quarter in terms of management development activities. During this instance, the goal was to provide the organisation's leaders with the opportunity to enhance their skills and knowledge on various topics, such as strategic workforce planning, performance management and recruitment.

While these indicate a move towards management development in 2022, the agency did not manage to make significant efforts to invest in management development, due to a lack of resources and know-how in this field, limited available budget to engage and develop all-round management development programmes, and a lack of data and know-how on this field of knowledge. While coaching has been widely offered to all ENISA management, limited focused management development sessions have occurred. The agency needs to steer its direction towards investing further in management development, increasing know-how, and evolving its learning and development strategy towards a more all-inclusive, holistic, collaborative, trust-based management practice.

To do so, this output should be discontinued, and its activities need to be further reviewed and redesigned and included within the overall HR strategy and the way ahead for learning and development. Overall, the unit should allocate more effort (resources) to this specific output due to increased demand and strategic focus.

11.4. Develop and maintain a user-friendly and service-oriented teleworking and office environment (including digital tools and services)

In the course of 2022, ENISA adopted the European Commission decision on hybrid ways of working with effect from 1 January 2023, by analogy, and reviewed its service approach to its staff since the new way of working has evolved. In addition, ENISA continues to improve its digitalisation path, introducing modules or digital solutions that aim to reduce staff administrative burden and increase service orientation.

Regarding facility management, the growth of ENISA and the return to the office created a lot of additional work that was being carried out. The unit focused on fully outsourcing and centralising facility management services to support this area. The agency still has a lot to undertake in the area of facility management and modernising its workplace, and needs to allocate a certain budget amount to this end. Physical upgrades to the overall office environment (furniture, etc.) have been small, particularly due to budgetary constraints, mainly financial resources.

In relation to the office environment, limited solutions were identified to improve the physical meeting rooms and update the audiovisual set-up, particularly due to the staff's lack of competency and skills.

In terms of IT and digital solutions, the unit has achieved the following milestones:

- comprehensive Zero Trust analysis: a first analysis to improve the current security posture and identify the necessary basic steps for implementing a Zero Trust framework,
- FortiVPN solution implementation: deployment of FortiVPN solution, enhancing the security and performance of our remote access capabilities,
- seamless transition to Windows 11,
- addressing the vulnerabilities identified by the Red Team exercise to improve ENISA's security posture.

Besides that, the IT domain was restructured and reorganised in order to meet the resourcing challenges and develop a more effective IT governance model. In this effort, particular emphasis was placed on streamlining the IT budget and optimising resources allocated while clarifying recurrent versus one-off project expenditure. The unit faced challenges in providing support to the IT operational systems, particularly due to a lack of resources (both human and financial) as well as a lack of dedicated skill set and specialised know-how among existing staff. The decentralised IT support applied at ENISA, which is spread among the different entities, is starting to impact business continuity and increasing costs; thus, efforts need to be made to identify synergies and efficiencies in this area corporately. The situation in the IT field remains critical in terms of both FTE allocation and technical know-how, while efforts are being made to upskill and reskill staff. In addition, the breadth and scope of the IT activities and the business requirements provide a different maturity and service level increase. While the Market, Certification and Standardisation unit and the Capacity Building unit transferred some resources for short periods to support it, the need proved to be permanent and, with the upcoming legislative changes and business priorities, even greater, while the transfer had an impact on these two operational entities. The quality of know-how of existing IT staff and the digital solutions applied to manage IT service are not those required for a sustainable team that is able to scale up quickly in order

to meet changing or all-inclusive user demands. Thus, even though efforts were made to increase service orientation, this is done with an overdependency on external consultants and reduced service provision towards operational units.

The unit has started scrutinising its costs and expenditure and has differentiated Title II IT costs into recurrent expenses, on the one hand, and ad hoc expenses and external workforce needs, on the other. The fact that many IT services are also held on the premises, rather than in the cloud, impacts the Title II budget, and the unit faces critical resource constraints in continuing to maintain its current essential IT services. Besides that, the unit's services are at the centre of all operational services, rendering its planning mainly demand driven to a large extent. The tools and procedures in place for financial and resource planning are inadequate and not automated, and thus prone to human error.

The geographical dispersal among four locations (Athens, Brussels, Heraklion and Alicante) demands the allocation of resources, which exceeds current capacity. Besides the overall costs required to ensure business continuity, staff will also need to be retrained to reflect the needs of the agency and increase know-how on EU-related aspects of IT at the parent DGs. The agency's overdependency on a sole individual in the area of IT (e.g. a datacentre) creates a significant critical risk in the form of a single point of failure, and needs to be minimised.

The need to allocate additional resources coincides with the agency's efforts to set up its EUCI accreditation path, which is under way. The geographically dispersed locations and the requirements for EUCI accreditation in terms of resources and budget need to be further considered, as possible delays would impact ENISA's operational capacity and strategic operational goals. In relation to IT and security services, the unit and the agency overall need to reflect on its business operating model and explore synergies and efficiencies corporately in anticipation of the upcoming cybersecurity regulation and common binding rules, its revised political priorities and internal challenges.

In the areas of security and safety, the agency has allocated 0.25 of a security officer to handling and manoeuvring a range of corporate security activities among three locations. While the local security officers support their role remotely, there is a demand to train, educate and upskill in this domain.

Although efforts were made to manage security services, this approach still stretched operational and corporate activities in the timely implementation of the required/desired needs. Lack of resources in terms of FTEs (since the relevant legislation requires specialist function roles), and lack of budget to improve the physical security posture of the agency is of paramount importance in order to meet the business objectives of the future. With the upcoming legislation on information security and the consolidated actions in the areas of facility management, physical security and IT infrastructure, the agency needs to achieve a greater balance in this area in order to progress towards the desired results. However, areas such as business continuity, completing the work for the secure rooms in the Athens and Brussels offices, and proceeding with investments in physical security have not materialised due to lack of dedicated resources and specialised resources allocated in this domain.

Overall, in 2022 the unit:

- has achieved a satisfying baseline of physical security for its new headquarters in Athens by upgrading security systems to meet the business requirements of the agency;
- has completed the development of safety procedures for staff for its premises in Athens and Heraklion and conducted safety drills;
- has drafted SOPs for security and has conducted security drills.

ENISA has initiated preparations for handling EUCI information.

ENISA has started developing relevant policies and is in the process of producing relevant internal implementation documentation and required organisational changes.

Through a dedicated security portal:

- staff can be informed on security-related topics;
- staff can request security-related services via a ticketing system;
- security staff can monitor the agency's security posture;
- a warning system can inform staff of security-related risks/hazards in Athens, Brussels and Heraklion.

This activity will need to be reviewed, restructured and redesigned in the SPD for 2024 onwards. Thus, the unit and the agency overall are facing serious to critical resource constraints in this area, in terms of allocation of FTEs, quality of know-how and expertise, and financial resources to maintain business continuity, professionalise its posture, increase its maturity level and maximise its service provision to its operational units and external stakeholders. Thus, this activity would justify allocating even more human and financial resources to this output due to the greater demand, while upskilling/reskilling is critical.

In the future, the team needs to invest further in improving and updating its technical know-how, but also in the competency development areas of policy advice, analysis and synthesis, networking and communication, project management and change management, and in problem-solving skills, in order to meet the challenges of the future. Recalibration of work includes restructuring of roles and functions, as well as continuously improving skills/competencies and developing expertise in line with the desired competencies, since the agency is placing a great strategic demand in this area of corporate IT and security.

11.5. Set up service provision standards and provide quality support and services for ENISA staff, employees, corporate partners and visitors

ENISA continued to introduce digital solutions that will increase its service provision. In Sysper; the time management module was launched in 2022. The need to proceed further with digital solutions via Sysper, to reduce administrative burden, has increased. Naturally, there is a significant delay in administrative services and module implementation due to shortage of human and financial resources.

ENISA advanced further with the aim of starting to use MIPS as the mission management tool, while delays occurred in the planning and preparation phases. While the launch of MIPS has been postponed to 2023, cooperation with the new travel agency started in 2022, and the online booking tool was successfully introduced. The aim was to transition to PMO MIPS and mission management with the service provider that is exclusively used by PMO in order to benefit from the

scale-of-economies and the know-how that is established via the long relationship between PMO and the service provider and the direct access to the online booking tools, which is a pre-requisite in the Guide to missions and authorised travel.

In the area of finance and procurement, the unit faced significant critical risks, as there is an overdependence on the external workforce in implementing core, critical and related sensitive tasks. Planning of budget, resources, procurement and operational activities is not integrated; that affects corporate support services, strains its resources and impacts operational activity managers. There is a significant FTE deficit in this area, and a heightened critical risk, as this team has an ageing workforce and also carries out some of the most impactful and sensitive/core functions (procurement and financial verification). The specialised know-how in procurement is stretched, and the outputs were achieved via increased working hours, even during weekends, while the administrative support was implemented relying on an external workforce. The overall resource situation in the area of finance and procurement remains critical, since the growth of operational activities has not been reflected in resources in the area of procurement and financial support (both planning and execution).

the situation in the area of finance and procurement remains critical, since the growth of operational activities has not been reflected in resources in the area of procurement and financial support (both planning and execution).

This activity will need to be reviewed and redesigned in the SPD for 2024 onwards. Thus, this activity would justify even more human and financial resources to be allocated to this output due to the greater demand, while upskilling/reskilling in both technical expertise and identified competency development remains critical. The same applies to the members of staff and the levels of responsibilities assigned to them, and in some areas the outputs performed and the grading of the allocated FTEs. The financial, compliance and legal responsibilities in the area of finance and procurement are performed by FTEs in assistant roles, which does not necessarily reflect the specialisation, job complexity and level of responsibility that are involved.

Overall, the service provision in the area of the unit, and consequently the agency, is seriously impacted by the fact that integrated digital solutions are non-existent, while there is a growing need for reskilling to increase technical know-how and maximise the use of the European Commission's existing digital solutions to obtain efficiency gains.

Key performance indicators: Staff commitment, motivation and satisfaction	Unit (of measurement)	Frequency	Data source	Results 2020	Results 2021	Results 2022
11.1. 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)						
% of staff satisfied with their work	%	Annual	Staff satisfaction survey	68 %	76 %	76 %
% of staff seeing a positive atmosphere within ENISA since the reorganisation	%	Annual	Staff satisfaction survey	70 %	58 %	N/A
% of staff feeling confident working within the new organisational culture	%	Annual	Staff satisfaction survey	61 %	68 %	N/A
% of staff indicating their line manager provides sufficient feedback on their performance	%	Annual	Staff satisfaction survey	68 %	76 %	60 %
% of staff indicating their line manager sets clear objectives	%	Annual	Staff satisfaction survey	66 %	76 %	71 %
% of staff feeling well informed by ENISA leadership regarding important matters	%	Annual	Staff satisfaction survey	80 %	73 %	36 %
11.2. Quality of ENISA training and career development activities organised for staff						
% of staff trusting that ENISA will support them in acquiring the necessary skills and capabilities to successfully manage the reorganisation	%	Annual	Staff satisfaction survey	69 %	49 %	N/A
% of staff indicating that courses match their training and development needs	%	Annual	Staff satisfaction survey	N/A	58 %	43 %
% of staff finding that their line manager dedicates enough time during the career development report (CDR) dialogue to mapping training and development needs	%	Annual	Staff satisfaction survey	N/A	55 %	36 %

Key performance indicators: Staff commitment, motivation and satisfaction	Unit (of measurement)	Frequency	Data source	Results 2020	Results 2021	Results 2022
% of staff finding that their line manager ensures a proper follow-up of the training and development needs from the CDR	%	Annual	Staff satisfaction survey	N/A	47 %	55 %
% of staff finding that they have had the opportunity to grow in their career at ENISA since the reorganisation	%	Annual	Staff satisfaction survey	N/A	35 %	38 %
11.3. Reasons for staff departure (exit interviews) ^a						
On a scale of 1 to 10, did the job you were employed for meet your expectations?	Scale 1–10	As required	HR files	N/A	7.5	8.5
On a scale of 1 to 10, did you have all the tools and resources you needed to effectively perform your job?	Scale 1–10	As required	HR files	N/A	6.6	7.5
On a scale of 1 to 10, how would you describe the tasks assigned and workload (tasks too demanding / not demanding; too much workload / not enough tasks)?	Scale 1–10	As required	HR files	N/A	7.75	7
On a scale of 1 to 10, how would you rate the management style of your immediate supervisor?	Scale 1–10	As required	HR files	N/A	6.5	7.5
On a scale of 1 to 10, what was your working relationship with your manager like?	Scale 1–10	As required	HR files	N/A	7.25	8.5
On a scale of 1 to 10, how would you describe your relationship and communication with your colleagues?	Scale 1–10	As required	HR files	N/A	8.4	9
On a scale of 1 to 10, did you have clear performance objectives in your job (10 being crystal clear and 0 being not clear at all)?	Scale 1–10	As required	HR files	N/A	6.8	8
On a scale of 1 to 10, how competitive would you say the compensation and benefits were for your position?	Scale 1–10	As required	HR files	N/A	6.6	8.5
On a scale of 1 to 10, how would you rate your employee experience in the agency?	Scale 1–10	As required	HR files	N/A	6.6	7
11.4. Staff retention / turnover rate	%	Annual	HR files	2 %	3 %	4 %
11.5. Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services and tools)						
Critical systems downtime	%	Annual	Uptime report of FortiMail	N/A	99.38 %	100 %
% of central IT infrastructure assessments with few (< 5) critical findings	%	Annual	Intranet repository	N/A	100 %	100 %

Key performance indicators: Staff commitment, motivation and satisfaction	Unit (of measurement)	Frequency	Data source	Results 2020	Results 2021	Results 2022
% of central infrastructure patched to the last formal versioning of 1 year	%	Annual	Yearly IT maintenance plan in PDF	N/A	95 %	97.33 %
% of major IT helpdesk requests resolved in a satisfactory way within 2 business days	%	Annual	IT ticket repository	N/A	80 %	79.28 %
% of staff satisfied with resolution	%	Annual	Staff survey	N/A	N/A	84 %
% of staff rating ENISA's out-of-hours support service a 4 or a 5	%	Annual	Staff survey	N/A	N/A	38 %
% of staff indicating that the IT help desk responds within a reasonable time	%	Annual	Staff survey	N/A	75 %	83 %
% of staff rating DMSs favourably	%	Annual	Staff survey	N/A	N/A	44 %
% of staff who can find information on intranet easily	%	Annual	Staff survey	N/A	N/A	41 %
% of staff satisfied with the meeting rooms' audiovisual equipment	%	Annual	Staff survey	N/A	N/A	53 %
% of staff satisfied with the Webex services' performance	%	Annual	Staff survey	N/A	N/A	82 %
% of staff not aware of the online service catalogue	%	Annual	Staff survey	N/A	N/A	72 %
Allocated FTEs as per SPD based on full establishment at 2022 year end	19		Used FTEs	15		
Planned budget ^b	EUR 1 234 934		Consumed budget ^b	EUR 1 229 738		
			Of which carried over to 2023	EUR 444 812		

a The greater the number the better the performance and vice versa.

b Direct costs only: staff learning and development, staff welfare, books and newspapers, consultancy and travel expenditures linked to Activity 11.

PART II (A)

MANAGEMENT

2.1. MANAGEMENT BOARD

In 2022, the Management Board met for two ordinary meetings and one extraordinary meeting. The extraordinary meeting was organised to exchange views among the members on strategic issues for ENISA and the direction that the agency should follow in some key areas, namely its exercises and training strategy, the EU cybersecurity index and the concept of joint technical situational reports. The discussion aimed to build a conceptual vision and anticipate necessary changes. The Management Board strategy meeting was combined with the official inauguration of new ENISA premises and the visit of the Vice-President of the European Commission, Margaritis Schinas, who opened a discussion with the Management Board on building a common situational awareness.

In total, the Management Board made 14 decisions during the year, such as decisions on the establishment and operation of ad hoc working groups, on ENISA's internal control framework and on the conditions for working time and hybrid working. In accordance with the EU Cybersecurity Act and the Management Board rules of procedure, the Management Board decisions were prepared by the Executive Board and adopted by the Management Board.

As one of its functions, the Management Board reviewed and evaluated ENISA's achievements in the context of implementation of its strategic objectives, as outlined in the ENISA strategy

published on 17 July 2020. The 2021 annual activity report was adopted. The Management Board also expressed its opinion on the final annual accounts for the 2021 financial year and adopted the *ENISA Single Programming Document 2023–2025*, including the 2023 budget and establishment plan.

As part of regular information sharing with the Management Board, ENISA reported on its work programme, budget implementation, audit and evaluation activities (e.g. by the ECA and the IAS), and engagements with international partners in line with the ENISA international strategy.

In addition, the Management Board provided strategic guidance in terms of the certification strategy and the challenges resulting from NIS2.

Following the request from the Commission for ENISA's involvement in the implementation of the new Emergency Response Fund for Cybersecurity, the Management Board supported the implementation of the pilot ENISA cybersecurity support action 2022 mechanism, mainly by adopting a decision on amending ENISA's budget for the 2022 financial year.

In 2022, the elections to two Executive Board alternate vacant member posts were concluded.

Four formal Executive Board meetings were held (one meeting per quarter).

2.2. MAJOR DEVELOPMENTS

2.2.1. ENISA cybersecurity support services action

During the course of 2022 the European Commission allocated to ENISA a one-off payment of EUR 15 million so that the agency could massively scale up and expand its *ex ante* and *ex post* services to the Member States. In 2022, the agency worked closely with the Member States and Commission to set up the framework contracts in each Member State to be able to scale up the services offered to beneficiaries indicated by the Member States. This short-term support aimed to complement, not duplicate, efforts by Member States and those at EU level to increase the level of protection against and resilience to cyber threats, by providing ENISA with additional means to support preparedness for (*ex ante*) and response to (*ex post*) large-scale cybersecurity incidents.

The agency managed the cybersecurity support action by reallocating staff from across the work programme and particularly from Activities 4 and 5 – to achieve the goal of having framework contracts in place in 27 Member States and a pan-European lot by year end; however, this came at the expense of other work programme outputs, as detailed in the activities above.

2.2.2. Identification of negative priorities for forthcoming years

During the development of the 2023 work programme the agency identified a resource shortfall amounting to EUR 734 000 and two FTEs in operations, and EUR 2.5 million in corporate services. To address the resource shortfall, each activity manager assessed what could and could not be delivered with the available resources, and what the impact of the shortfall was on the activity, by describing reduced scope, postponed projects and suppressed outputs.

The Agency undertook a thorough assessment of its internal human resourcing needs for the programming period of 2023-2025, taking into account the near-term foreseen legislative and political developments, as well as the heightened level of threats of the cybersecurity landscape. The assessment points out a significant human resource gap with approx. half of this gap linked to highly critical or critical activities needed to fulfil the tasks for 2023-2025.

2.2.3. New legislative proposals

During the course of 2022 legislative proposals were put forward to develop cybersecurity across the EU. ENISA worked to that end together with Member States to identify best EU practices in line with the provisions of the NISD and to share them among its stakeholders. The agency supported Member States with the implementation of the revised rules under NISD2 and a new range of rules, including those of the DORA, those of the future Electricity Network Code for Cybersecurity and those that will be introduced with the CRA.

NISD2 assigned to ENISA a number of significant new tasks such as the development and maintenance of a European vulnerability registry, acting as the secretariat of EU-Cyclone, the publication of an annual report on the state of cybersecurity in the EU, supporting the organisation of peer reviews between Member States, and the creation and maintenance of a registry for entities providing cross-border services, for example domain name system service providers, top-level domain name registries, entities providing domain name registration services, cloud computing service providers and data centre service providers. ENISA is expected to support the implementation of the NISD as part of its mandate and its work programme.

In parallel with NISD2, the European Parliament and the Council adopted in December 2022 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). The regulation aims to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyberattacks and other risks. ENISA actively supported the preparation of new legislation on cybersecurity in the financial sector and worked closely with the European Commission and relevant EU bodies on cybersecurity aspects of DORA including crisis management, incident reporting and information sharing.

A new proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, was put forward by the European Commission in 2022 to bolster cybersecurity rules to ensure more secure hardware and software products. The CRA foresees a role for ENISA in the implementation of the regulation. ENISA's role includes receiving notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, and

of incidents that have an impact on the security of those products; preparing a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements; and submitting information relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level to EU-Cyclone.

In March 2022, the European Commission proposed a new regulation with rules to increase cybersecurity in all EU institutions by establishing a governance framework for all EUIBAs. A proposed regulation² on information security in the institutions, bodies, offices and agencies of the EU was also put forward earlier in 2022 to create a minimum set of information security rules and standards for all EU institutions, bodies, offices and agencies to ensure enhanced and consistent protection against the evolving threats to their information.

2.2.4. Service catalogue

In 2022, the agency introduced the concept of the service catalogue during the preparation of the 2023 work programme, to allow management to focus efforts and resources in a highly structured and more efficient manner for obtaining specific objectives. The ENISA service catalogues are organised into individual service packages. A service package is a collection of cybersecurity products and services that span a number of activities and contribute to the objectives of a discrete service package; a service package is a means of centralising all services that are important to the stakeholders that use it.

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

- NISD
- training and exercises
- situational awareness
- certification
- cybersecurity index.

2.2.5. Skills framework

The development and publication of the ECSF marks a major milestone for the agency, following 2 years of rounds of consultations with the academic and industry community. The ECSF categorises cybersecurity-related professions into 12 profiles and outlines key competences and skills for each profile,

offering a common 'language' for professionals so that they can make an informed decision when choosing cybersecurity as a career path. The ECSF was presented during the first Cybersecurity Skills conference, and was followed by the declaration by the President of the European Commission that 2023 would be the European Year for Skills.

2.2.6. Internal control framework

With a view to further strengthening its internal control framework, ENISA adopted in 2022 a comprehensive methodology for enterprise risk management (ERM) based on the relevant guidelines of the European Commission. In this context, the agency also formalised its IT security risk management methodology, which is interlinked with the ERM framework. On the basis of the adopted methodologies and related internal procedures, ENISA performed its enterprise and IT security risk assessments in 2022, which will feed into ENISA's activities in the years to come.

2.2.7. Other developments

In 2022, the existing Advisory Group's term drew to a close and a public call for expressions of interest from experts to become members of the Advisory Group was launched on 1 September 2022. The call closed on 30 September 2022. The call text, which included eligibility and selection criteria, was adopted by Management Board Decision No MB/2022/6. In accordance with the rules laid down by the previously mentioned documents, the Executive Director established a dedicated Selection Committee by Executive Director decision to assess the applications received. The Selection Committee preselected a list of applicants and submitted this preselection to the Executive Director, who drew a proposal for the Management Board for the appointment of members of the Advisory Group, ensuring appropriate gender and geographical balance as well as balance between the different stakeholder groups. The Management Board established the new Advisory Group term and composition by Management Board Decision No MB/2023/02.

An MoU was signed between ENISA and the European Data Protection Supervisor during the course of 2022 to establish a strategic cooperation framework. The MoU includes a strategic plan to promote awareness of cyber hygiene, privacy and data protection among EUIBAs. The plan also aims to promote a joint approach to cybersecurity aspects of data protection, to adopt privacy-enhancing technologies, and to strengthen the capacities and skills of EUIBAs.

² Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union.

During the course of 2022 ENISA established a task force to achieve accreditation for handling EUCI.

A number of key steps towards this goal were taken in 2022. Following a detailed mapping of the relevant Commission decisions to the existing ENISA documentation set, a complete business analysis was conducted. In parallel, the existing policy framework was adapted to accommodate the needs of EUCI, and all key policies were produced. In particular, the security core operational procedures were finalised following discussions with experts in the Commission and other EU agencies. The associated IT procedures were developed using the existing framework and have been integrated into the policy planning and implementation cycle defined and managed by the Information Technology Management Committee (ITMC). Where physical security is concerned, works to complete the installation of a 'strong room' were completed in April. The agency is currently adapting its governance system to meet the identified requirements and foresees accreditation in 2023.

EU Cybersecurity Act to improve the prevention, detection and analysis of cyber threats and incidents, and the capability to respond to these, by providing Member States with knowledge and expertise. A further EUR 610 000 was granted to ENISA in late November 2022 with the adoption of NISD2³.

In 2022, in addition to the 197 low-value contracts with direct award (less than EUR 15 000), ENISA concluded 74 public procurement procedures:

- 44 were done using the open procedure (59.5 %);
- 20 were done through reopening of competitions under framework contracts (27 %);
- 9 were done through negotiated procedures for medium- and low-value contracts (12 %);
- 1 was done using the restricted procedure (1.5 %).

No interest for late payments was charged by suppliers in 2022.

The table below shows ENISA's budget implementation targets and achievements in 2022, which were improved further compared with 2021.

2.3. BUDGETARY AND FINANCIAL MANAGEMENT

2.3.1. Financial management

During 2022, ENISA has been operating with a budget of EUR 39.2 million, a 67 % increase compared with the 2021 budget of EUR 23.5 million. Amending budget 1/2022 was adopted by the Management Board by written procedure on 5 August 2022 for the pilot implementation of a cybersecurity support action granting ENISA an additional budget of EUR 15 million. This cybersecurity support action aims at reinforcing ENISA's response capabilities in supporting Member States in accordance with its mandate, in particular under Articles 6 and 7 of the

2.3.2. Budget execution of EU subsidy (C1 funds of current year 2022)

From 1 January to 31 December 2022, ENISA executed EUR 39 179 405.95 in commitment appropriations, representing 99.93 % of the total budget of the year, and EUR 20 396 780.25 in payment appropriations, amounting to 52.02 % of the total budget. A majority of the commitments under the cybersecurity support action were signed late in the year, which explains the relatively low payment rate (and the subsequent large carry-forward).

³ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Area	Objective	Target 2022	Level of completion 2022
Budget implementation (appropriations committed through the year)	Efficiency and sound financial management	95 %	99.93 %
Budget implementation without support action (appropriations committed through the year)	Efficiency and sound financial management	95 %	99.91 %
Payments against appropriations of the year (C1 funds)	Efficiency and sound financial management	80 %	52.02 %
Payments against appropriations of the year without support action (C1 funds)	Efficiency and sound financial management	80 %	84.11 %
Payments against appropriations carried over from previous year (C8 funds)	Efficiency and sound financial management	95 %	95.07 %

Omitting the implementation of cybersecurity support action funds, ENISA executed EUR 24 184 884.73 in commitment appropriations, representing 99.91 % of the budget of the year, and EUR 20 361 678.03 in payment appropriations, amounting to 84.11 % of the budget.

Compared with 2021, there has been a slight increase in commitment execution – 99.93 % in 2022, compared with 99.51 % in 2021 (97.35 % in 2020). Overall payment execution has decreased owing to cybersecurity support action funds and reached 52.02 %, compared with 77.40 % in 2021 (68.62 % in 2020). However, comparing only the initial budget

allocated to ENISA, payment execution increased to 84.11 %, which is a noticeable achievement.

The target of 95 % for 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 2022 were carried forward to 2023.

The tables below summarise the execution of the budget in 2022, by title, for the full budget 2022, for cybersecurity support action implementation and for ENISA funds without support action.

2022 full budget (C1)						
Area of budget allocation	Appropriation amount (EUR)	Commitment amount (EUR)	Percentage committed	Payment amount (EUR)	Percentage paid	Amount carried forward to 2023 (EUR)
	(1)	(2)	(2)/(1)	(3)	(3)/(1)	(2)-(3)
Title I	12 024 668.92	12 024 177.67	100.00 %	11 348 571.92	94.38 %	675 605.75
Title II	3 896 915.42	3 896 259.17	99.98 %	2 012 371.87	51.64 %	1 883 887.30
Title III	23 286 040.66	23 258 969.11	99.88 %	7 035 836.46	30.21 %	16 223 132.65
TOTAL	39 207 625.00	39 179 405.95	99.93 %	20 396 780.25	52.02 %	18 782 625.70

2022 Cybersecurity Support Action funds only (C1)						
Area of budget allocation	Appropriation amount (EUR)	Commitment amount (EUR)	Percentage committed	Payment amount (EUR)	Percentage paid	Amount carried forward to 2023 (EUR)
	(1)	(2)	(2)/(1)	(3)	(3)/(1)	(2)-(3)
Title I	150 021.22	150 021.22	100.00 %	35 102.22	23.40 %	114 919.00
Title II	494 500.00	494 500.00	100.00 %	–	0.00 %	494 500.00
Title III	14 355 478.78	14 350 000.00	99.96 %	–	0.00 %	14 350 000.00
TOTAL	15 000 000.00	14 994 521.22	99.96 %	35 102.22	0.23 %	14 959 419.00

2022 Cybersecurity Support Action funds only (C1)						
Area of budget allocation	Appropriation amount (EUR)	Commitment amount (EUR)	Percentage committed	Payment amount (EUR)	Percentage paid	Amount carried forward to 2023 (EUR)
	(1)	(2)	(2)/(1)	(3)	(3)/(1)	(2)-(3)
Title I	11 874 647.70	11 874 156.45	100.00 %	11 313 469.70	95.27 %	560 686.75
Title II	3 402 415.42	3 401 759.17	99.98 %	2 012 371.87	59.15 %	1 389 387.30
Title III	8 930 561.88	8 908 969.11	99.76 %	7 035 836.46	78.78 %	1 873 132.65
TOTAL	24 207 625.00	24 184 884.73	99.91 %	20 361 678.03	84.11 %	3 823 206.70

2.3.3. 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 to 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 2 weeks, the proposed transfers are deemed to be adopted.

During 2022, the agency made one transfer by Executive Director's decision on the initial budget and three transfers by Executive Director's decision on the amended budget (in comparison, the Executive Director made four transfers on the initial budget and one transfer on the amended budget in 2021). Transfers on the initial budget and on the amended budget included transfers of funds within title and between titles. Funds were moved from Title I to Title II and Title III to finance corporate ICT-related projects and cover operational commitments related to the cybersecurity support action. Savings under Title I were effected by the late adoption of NISD2 granting funds for salaries of 5 FTEs.

2.3.4. Carry-forward of commitment appropriations

The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not fully paid at the end of 2021 were carried forward to 2022 (C8 appropriations).

Compared with 2021, there was a decrease in payment execution (95.07 % in 2022 compared with 96.55 % in 2021). A large proportion of cancellations were due to consultancy and corporate ICT budget lines for which the actual amount of services provided was lower than planned.

2.4. DELEGATION AND SUBDELEGATION

At the end of 2020, in line with the reorganisation, the Executive Director reviewed the delegation of authorising authority powers and on 22 December 2020 adopted a new decision on a framework for the financial delegation of the authorising officer.

This decision confirmed the financial delegations applicable to heads of unit and permanent team leaders with respective limits of EUR 400 000 and EUR 200 000 per financial transaction for the budget lines relevant for the performance of their duties and assigned activities or outputs of the Single Programming Document.

The table below summarises the changes to the budget in 2022.

2022 Budget (C1) (EUR)	Initial budget	Amending budget	Transfers approved by the Executive Director	Final budget
Title 1	12 494 335.00	250 000.00	-719 666.00	12 024 669.00
Title 2	2 824 300.00	800 000.00	272 615.00	3 896 915.00
Title 3	8 888 990.00	13 950 000.00	447 051.00	23 286 041.00
TOTAL	24 207 625.00	15 000 000.00	-	39 207 625.00

2022 Budget (C8) (EUR)	Appropriations carried forward from 2021 to 2022 (EUR)	Payment amount (EUR)	Percentage paid	Amount cancelled (EUR)
Title 1	708 557.72	662 622.37	93.52 %	45 935.35
Title 2	2 164 072.99	1 986 995.40	91.82 %	177 077.59
Title 3	2 176 174.22	2 150 441.78	98.82 %	25 732.44
TOTAL	5 048 804.93	4 800 059.55	95.07 %	248 745.38

On 5 August 2022 the Management Board adopted Decision No MB/2022/8 granting ENISA an additional EUR 15 million for the pilot implementation of a cybersecurity support action, and specifying that:

- financial delegation should take into account ENISA's size and organisational structure and the financial resources allocated to pursue specific activities under ENISA's mandate;
- the Operational Cooperation Unit will play a central role in implementing the cybersecurity support action.

The Executive Director consequently increased the limit of his delegation to the Head of the Operational Cooperation Unit to EUR 1 million per financial transaction.

Controls on these delegation rights are carried out through a periodical review of the access rights granted to the accrual-based accounting system within the main financial system, and are shared on an annual basis with the Commission (Directorate-General for Budget).

2.5. HUMAN RESOURCES MANAGEMENT

In 2022, ENISA continued with the new organisational structure established by the Management Board in 2020. Guidelines for the proportional allocation of resources between its 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 human resources (HR) sector continued to support the operational and administrative goals of the agency in terms of staff acquisition and development. In 2022, ENISA's HR unit welcomed 16 new staff members

(7 temporary agents, 4 contract agents, 4 seconded national experts and 1 trainee).

A review of ENISA's strategic workforce planning started in 2022, with the aim of adjusting and improving the first strategic workforce planning decision, adopted in 2021, to enable the agency to proactively estimate needs, engage and develop staff, and align its HR operations with the evolving strategic focus of its activities and objectives as directed by its single programming documents (SPDs), the Management Board and EU legislation.

In 2022, 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 the Executive Director's 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 2022, four 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 sector in 2022.

Area	Objective	2022 performance	2022 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 from the deadline specified in the vacancy notice for candidates to submit applications to the signing of the reserve list by the Executive Director)	≤ 5 months	≤ 5 months
Turnover of staff	Reduced turnover rate of statutory staff (temporary agents and contract agents)	4 %	< 15 %
Staff performance management	Implementation and monitoring of the appraisal and reclassification exercises (launching and completion of the exercises)	100 %	100 %

ENISA's code of conduct includes the following principles.

- **Independence.** Staff members should always serve the interest of the agency and never act on behalf of any other interest, whether private or otherwise, or as a result, for example, of political pressure.
- **Impartiality.** Staff members should always be unbiased in any advice or decision they are asked to give or make.
- **Objectivity.** Staff members' opinions, conclusions and advice should be balanced and based on a thorough analysis of the facts and the legal background.
- **Loyalty.** Staff members should always be loyal to the agency in order to safeguard its independence and contribute to achieving its mission. Staff members should be committed to the agency's mission and support its growth and goals.
- **Circumspection.** In the exercise of their duties, staff members should always reflect on the possible consequences and implications of potential actions, showing a proper degree of moderation and conducting themselves with a due sense of proportion at all times.
- **Transparency and accountability.** Staff members should act in a transparent manner and be ready to explain and justify the reasons for particular actions taken on behalf of the agency and the context in which they were taken.
- **Mutual respect between all colleagues.** Staff members should treat their colleagues the same way they want to be treated by them. Respect means valuing others, acting with care and kindness, and respecting diversity and different opinions, cultures and backgrounds. Staff members should also act with respect in their interactions with external stakeholders. A culture of mutual respect positively affects the outcome of work.
- **Integrity.** Staff should behave in an honest, ethical and fair manner at all times and uphold ENISA principles through the consistent application of the decision-making process.
- **Lawfulness.** Staff's conduct and decision-making must be in accordance with the applicable legal framework and guided by evidence.

The code of conduct provides further details on the following elements:

- compliance with the law
- respect in the workplace
- protection of ENISA's property
- professionalism
- ENISA's code of good administrative behaviour
- creating a healthy working environment
- disciplinary actions.

2.5.1. Implementing rules adopted in 2022

Management Board Decision No MB/2022/13 on working time and hybrid working was adopted, providing guidance to staff, including line managers, on hybrid ways of working, working time and teleworking.

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

In 2022, 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 and neutral. 'Administrative support and coordination' remained at the level of 21 %. An increase can be observed in the posts under the 'operational' area, which were at the level of 71 %. 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 Corporate Support Services unit does not exceed the average number of staff members assigned to operational units. 8 % of the posts are 'neutral' posts.

2.6. STRATEGY FOR EFFICIENCY GAINS

The agency initiated the development of its corporate strategy in 2022, which is to be discussed by the Management Board at its meetings in March and June 2023. The strategy for achieving efficiency gains will be formalised as part of the corporate strategy, which will also encompass ENISA's HR strategy, greening and digital strategy, and service model.

The corporate strategy (including the HR strategy) presents a vision for modern, flexible and values-driven planning of all the agency's resources in service of an organisation that ensures its staff deliver outstanding results for all stakeholders across the EU.

The aim is to further improve ENISA's organisational efficiency and flexibility to meet operational needs. To this end, the agency aims to include in its HR strategy an efficiency strategy component, with specific initiatives and a cross-unit perspective.

In 2022, ENISA took steps to move from a traditional headcount methodology to strategic workforce planning. This will enable a forward-looking, proactive, flexible and integrated approach to anticipating and addressing staffing gaps in order to build an agile workforce and allocate resources to priority areas. To achieve this, ENISA revamped its internal strategic workforce planning framework, with the aim of combining 'hard' workforce data with 'soft' competency aspects and adopting a new staffing strategy aligned with organisational priorities.

ENISA continued to review and explore options for re-engineering its processes, with a view to optimising service quality and cost-effectiveness, for instance by:

- exploring and piloting changes in service levels and modalities to increase added value and cost efficiency, such as shifting from owned to leased solutions and from manual data entry to centrally managed solutions;
- identifying activities and services that could be downsized or discontinued if necessary;
- continuously streamlining and automating administrative workflows to improve staff productivity by removing redundant steps and capitalising on new technologies, for example by making use of services and tools provided by the Directorate-General for Informatics;
- reviewing ICT infrastructure and related technologies to reduce duplication of components and to optimise maintenance and capital replacement, for instance by moving to cloud-based solutions for storage.

In line with the call for agencies to promote the use of shared services, ENISA sought efficiency gains through initiatives such as the following.

- ENISA sought to increase its use of services shared with other agencies and/or the Commission, including, for example, through interagency and interinstitutional procurement processes, and sharing services with Cedefop and the ECCC. In 2022, the agency signed a service-level agreement with the newly established European Cybersecurity Industrial, Technology and Research Competence Centre, for the provision by ENISA to the centre of data protection officer and accountant services, to be implemented in 2023.
- The agency contributed to further promotion of shared services among agencies through various networks, particularly in the areas

of procurement, HR, ICT, risk management, performance management, data protection, information security and accounting.

- In addition, the agency announced a pilot exercise within the EU Agencies Network intended to support EU agencies to increase their preparedness for the upcoming new cybersecurity regulation. The pilot was launched in 2023, with agencies expressing interest and with the support of CERT-EU.

ENISA has already started its efficiency gains journey and intends in the forthcoming period to connect the separate actions through a corporate plan in order to meet the challenges of the future.

2.7. ASSESSMENT OF AUDIT AND EX POST EVALUATION RESULTS DURING THE REPORTING YEAR

2.7.1. Internal Audit Service

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.

ENISA welcomed and agreed with these three audit observations and has already taken the necessary steps to address these concerns.

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 closed.

2.7.2. European Court of Auditors

In 2022, the ECA issued its report on the 2021 annual accounts of the agency⁴. In the ECA's opinion, the accounts of the agency for the year ended 31 December 2021 present fairly, in all material respects, the financial position of the agency at 31 December 2021, 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 2021 are legal and regular in all material respects.

⁴ <https://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-2021-annual-report-eca-report.pdf>.

Nevertheless, the ECA issued in 2022 four observations on management and control systems, which are currently being addressed by the agency.

2.7.3. Ex post control evaluation results

In 2022, ENISA performed *ex post* controls of financial transactions made during 2021 financial year as per Article 45(8) and (9) of the ENISA financial regulation .

A total of 355 financial transactions were scrutinised, representing 20.08 % of the agency's financial transactions and 83.30 % of the agency's budget (excluding salaries and related staff expenditure as per the *ex post* control methodology).

Three weaknesses were identified, leading to three recommendations on financial transactions, none of which was deemed critical. To address the main weakness, weekly monitoring of time to payment was introduced in 2022 to alert the relevant financial staff to urgent transactions remaining to be processed, to comply with the legal framework on payment time limits.

More details are available in Part III 'Assessment of the effectiveness of the internal control systems'.

2.8. (a) FOLLOW-UP OF RECOMMENDATIONS AND ACTION PLANS FOR AUDITS AND EVALUATIONS

2.8.1.(a) Internal Audit Service

The IAS 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 the corrective actions implemented by ENISA, one very important recommendation remained open at the end of 2022, not having been fully implemented within the set time frame⁵.

This open recommendation has, however, been partially addressed, resulting in its being downgraded after an IAS follow-up audit in 2021 from 'very important' to 'important'. The part of the recommendation that remains open is related to the formal endorsement of the HR strategy by the Management Board to ensure its alignment with the programming documents to enable effective and

efficient planning and allocation of human resources to achieve the agency's objectives⁶.

2.8.2.(a) European Court of Auditors

The ECA has deemed all previous years' observations (i.e. up to 2021) completed, as ENISA has implemented the necessary corrective actions to address the identified weaknesses.

The agency took the necessary steps to mitigate the weaknesses identified by the auditors by strengthening its internal controls and updating its internal processes for procurement procedures.

2.8. (b) FOLLOW-UP OF RECOMMENDATIONS ISSUED FOLLOWING INVESTIGATIONS BY THE EUROPEAN ANTI-FRAUD OFFICE

Following the receipt of the investigation report of the European Anti-Fraud Office of 17 December 2020, which found that a staff member had breached the provisions of Articles 11, 12 and 21 of the Staff Regulations, the Executive Director referred the case to the Disciplinary Board. The board's reasoned opinion was made known to the agency in January 2022. The Executive Director issued a related decision. Finally, the forms of candidacy for vacancies were revised to include circumstances that are not aligned with staff members' obligations under the Staff Regulations.

⁵ This recommendation is considered significantly delayed (i.e. still open more than 6 months after the original expected date of implementation).

⁶ ENISA's HR strategy will be submitted for adoption by the Management Board in June 2023.

2.9. FOLLOW-UP OF OBSERVATIONS FROM THE DISCHARGE AUTHORITY

In relation to the 2021 discharge, as decided by the European Parliament, the Executive Director of the agency was granted discharge regarding the implementation of the agency's budget for the 2021 financial year. The closure of the agency's accounts for the 2021 financial year was also approved by the discharge authority. In reply to observations and comments made by the European Parliament in its discharge of 2021, 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 necessary steps 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 balance and recruitment, and with a view to limiting its need to rely on interim agents, ENISA is continuously fine-tuning its HR policy.

2.10. ENVIRONMENTAL MANAGEMENT

The agency undertook an evaluation of its climate footprint in 2022. Based on an audit of past ENISA emissions, for which 2019 and 2021 were used as reference years, it was established that the agency creates GHG emissions of 584.485 tonnes of carbon dioxide equivalent annually, with indirect emissions from purchased electricity (50.33 %) and air travel (36.80 %) being the main sources of climate impact. Based on these results, an action plan was developed, in particular in relation to the main sources of ENISA's emissions: purchased electricity and air travel. The action plan will be further detailed in the ENISA corporate strategy, to be discussed at the Management Board meeting in June 2023.

2.11. ASSESSMENT BY MANAGEMENT

The agency's operational and corporate activities were implemented in accordance with the 2022 work programme, including the unplanned work on the cybersecurity support action, which was carried out using an additional EUR 15 million that was provided to the agency to support Member States with expanded *ex ante* and *ex post* services. The cybersecurity support action was initiated in the second half of the year and implemented by having framework contracts in place in 27 Member States and a pan-European lot by year end. This additional work required the agency to mobilise resources from across operational and corporate activities to deliver support services to Member States, which came at the expense of a number of outputs in terms of both objectives not being achieved in the two operational cooperation activities (Activities 4 and 5) and delays to and the lower quality of one of the outputs in the work programme, as detailed in the overall assessments of the activities in this report.

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.

PART II (B)

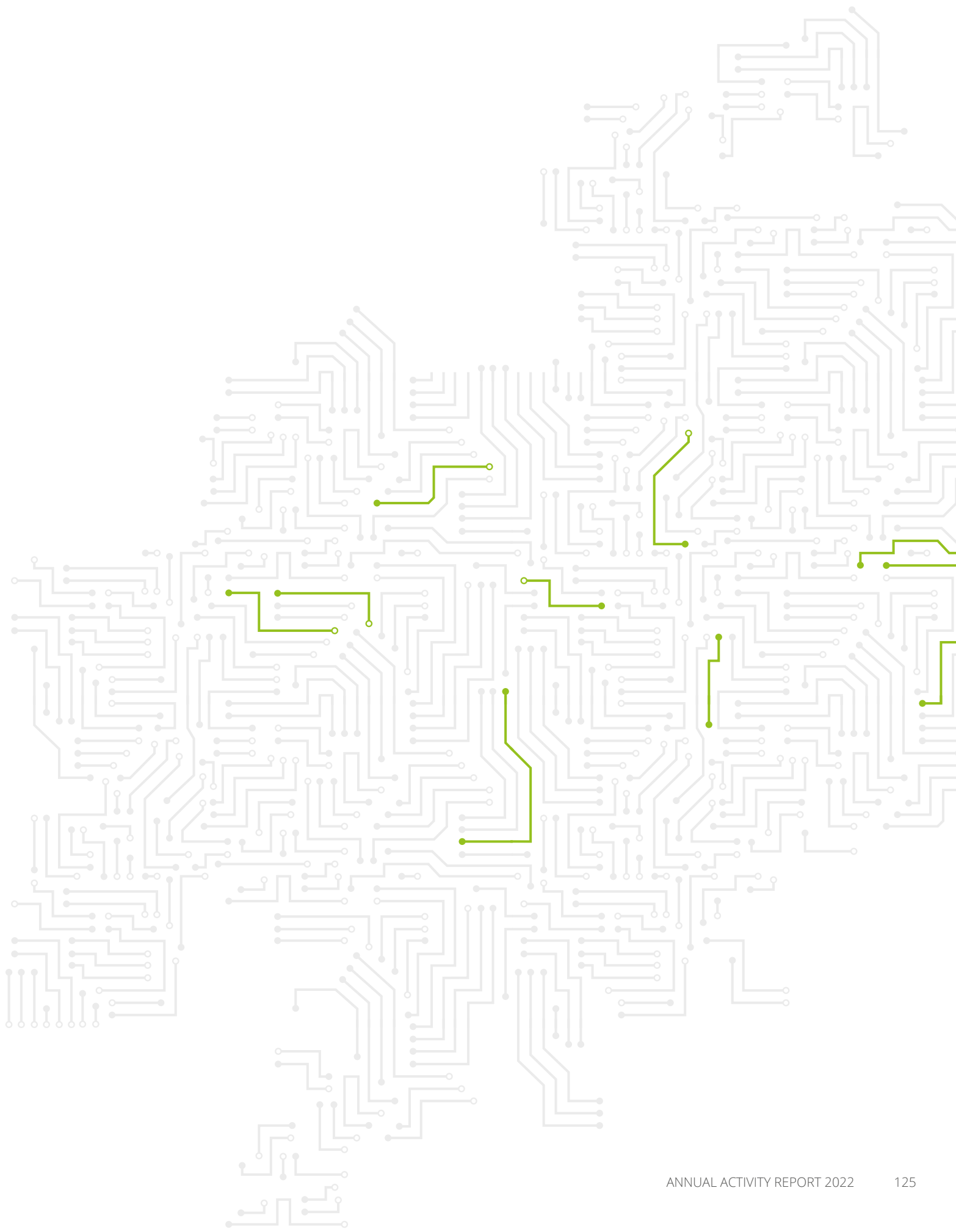
EXTERNAL EVALUATIONS

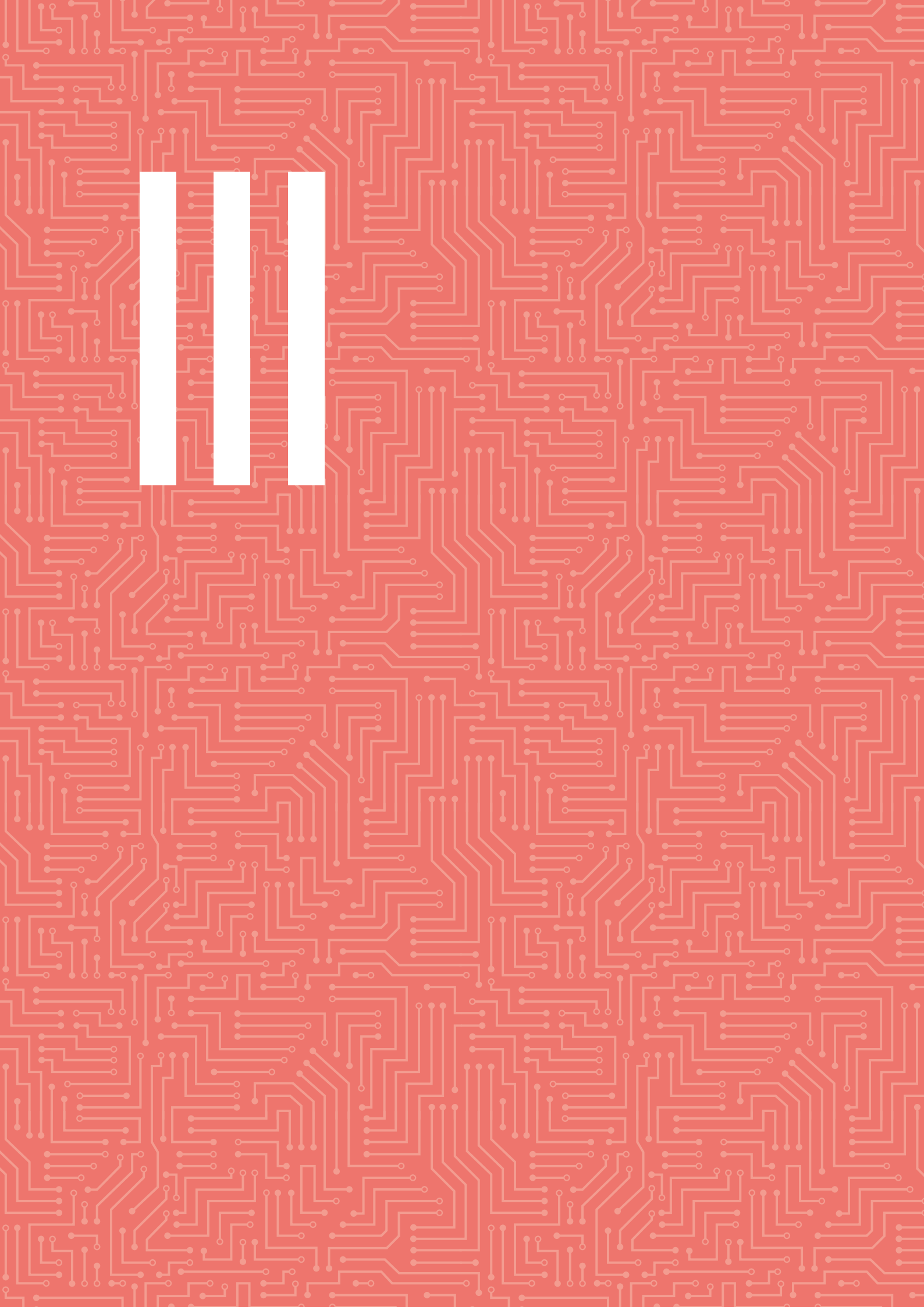
In 2022, the agency developed a stakeholder satisfaction survey to gather feedback on the outcomes/results of ENISA work over the past two reporting periods (2021 and 2022). In addition, the survey sought to assess the satisfaction levels of stakeholders in relation to the way the agency implements its projects, specifically how work is organised and managed and how the feedback from external stakeholders is taken into account. The survey was launched in Q1 of 2023 and the results of the survey are among the KPI results reported in the assessments of the operational activities in Part I. In addition, the agency ran two surveys among its key statutory bodies, namely the NLOs and the Advisory Group, to help it to assess whether its activities enable the agency to achieve its strategic objectives, and to enable it to further develop its annual work programme and SPD in line with its strategic objectives.

These strategic objectives are:

- empowered and engaged communities across the cybersecurity ecosystem;
- cybersecurity as an integral part of EU policies;
- effective cooperation among operational actors within the EU in the event of a massive cyber incident;
- cutting-edge competences and capabilities in cybersecurity across the EU;
- a high level of trust in secure digital solutions;
- foresight on emerging and future cybersecurity challenges;
- efficient and effective cybersecurity information and knowledge management for Europe.

With regard to *ex ante* evaluation, the agency consults on its outputs with external stakeholders during the planning stages. The scope of the outputs is decided on after gathering feedback from external stakeholders to ensure that the outcomes/results of the work are geared towards stakeholder needs. In addition, ENISA's work on foresight under Activity 8 provides insights into future challenges and topics that are used in the development of ENISA's work programmes.





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 Decision No MB/2022/11 amending it. 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 seventeen 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. Working with 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 Decision No MB/2022/11). The indicators are assessed individually and supported by relevant evidence. The assessment of the internal controls is an important part of ENISA's internal control framework, and it is conducted on an annual basis. For 2022, this assessment was based on the indicators of the framework, and also additional information from specific (risk) assessment reports, audit findings and other relevant sources. The assessment also followed the related guidance and templates developed through the EU Agencies Performance Development Network.

3.1.1. Assessment of the control environment component

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

Principle 1. ENISA demonstrates commitment to integrity and ethical values.

The assessment concluded that this principle is present and functioning, but some improvements are needed in the area of mandatory staff training.

In particular, to increase rates of participation in such training, the agency should consider a diversity of training plans/programmes to address different levels of staff knowledge/maturity.

Further to that, 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 the Executive Director's 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, but some improvements are needed.

In particular, it was noted that ENISA does not sufficiently follow up on relevant conclusions and deficiencies identified by internal control processes, and corrective action is to be implemented in 2023 to mitigate the underlying risks.

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 the 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 a minor improvement is needed with regard to staff's perception of their level of participation in the agency's decision-making.

On a regular basis, the agency publishes on its intranet the adopted and updated organisational charts. The Executive Director's Decision No EDD/2020/146 on delegation of authority, which entered into force on 1 January 2021, describes the financial circuits and all financial delegations,

ensuring a clear segregation of duties. This specific decision limits the number of authorising officers, covering all delegations of financial transactions, streamlining the profiles, and enhancing efficiency and effectiveness. Importantly, it includes a sunset clause to end all subdelegated authority automatically 3 months after a change in the person of the Executive Director, unless the new Executive Director explicitly confirms the delegations in place.

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, and only a minor improvement is needed in the area of learning opportunities for ENISA's staff, which should be more comprehensive. This point has been 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 a minor improvement is needed: staff members' feeling that they are recognised for their contributions within the agency should be increased.

The agency reviews its annual objectives during the year. While mid-term reviews are planned, significant efforts are 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, 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 annual objectives throughout the year. To ensure that amended or new objectives can be achieved, job descriptions can be reviewed if necessary.

Staff efficiency, abilities and conduct are assessed annually against the expected standards of conduct and set objectives. Promotions for staff are decided on after considering the comparative merits of the eligible staff, taking into account their appraisal reports.

3.1.2. Assessment of the risk assessment component

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

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

The assessment concluded that this principle is present and functioning well.

On the basis of ENISA's strategy, adopted in 2020, the Executive Director's 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 amended by Decision No EDD/3/2022 to reflect the latest organisational 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 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.

In 2022, a centralised risk management approach was implemented at agency-wide level. An 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 was conducted for 2022 (entailing an enterprise risk assessment and an IT security risk assessment). The cross-cutting risks were presented in a corporate risk register, and specific risks per unit/team were also identified.

As regards the enterprise risk assessment, no critical risks were identified.

However, the following high risks were pointed out:

- dependence on external providers (systems, services, people),
- lack of comprehensive IT strategy implementation across the agency,

- lack of resources and talent / insufficient HR management.

In addition, certain medium-level risks were highlighted:

- dependency from ENISA stakeholders and need to manage trust and requirements,
- lack of comprehensive integration of risk management into internal (SPD) processes,
- complex organisational structure and need for activity-based management for pool of resources,
- complex internal processes and procedures, and need for simplification.

The results of the risk assessment were presented to and endorsed by the ENISA Management Team in 2023 and will form the basis of an action plan during the year. The risk assessment results were also integrated into ENISA's corporate strategy.

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

The assessment concluded that this principle is present and functioning well.

The agency's anti-fraud strategy was updated in 2021 and formally adopted by Management Board Decision No MB/2021/5. All objectives and actions for 2022 were delivered. A dedicated web page was created on ENISA's intranet, where all relevant regulations, documents and training materials, and a toolbox, are available to all staff; training in fraud prevention, which forms part of training in ethics and integrity, is delivered regularly.

Principle 9. ENISA identifies and analyses significant change.

The assessment concluded that this principle is present and functioning well.

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 significant change (thus enabling further reflection of this change in internal activities). The establishment of dedicated committees (the ITMC, Budget Management Committee, Intellectual Property Rights Management Committee) further supports change management at corporate level. In 2022, change and arising risks from it were adequately managed, as illustrated by, among other things, the efficient implementation of ENISA's

support to the EU action in response to the Russian war of aggression against Ukraine.

3.1.3. Assessment of the control activities component

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

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

The assessment concluded that this principle is partially present and functioning but that improvements are needed to ensure that the results of controls are sufficiently monitored and addressed. In addition, further development of the agency's business continuity plan is needed.

To resolve these issues, the agency is to implement a system of consolidated monitoring of weaknesses and subsequent corrective actions identified through all possible sources, including internal control assessments, the IAS, the ECA, *ex post* controls and risk assessments. The system will serve as a continuous management status update and will cover all areas across the agency, including information security. Moreover, actions to put in place the agency's business continuity strategy and plan have already been undertaken in 2023.

In addition, a number of other controls in this field are already in place and effective. In line with the financial circuits to be followed, all financial transactions are subject to *ex ante* verification. In terms of *ex post* controls, 5 % of all transactions, amounting to a value of EUR 1 973 266, have been validated, out of a total value for all transactions of EUR 15 479 992 (this excludes salary payments to ENISA staff, which are processed by the European Commission Office for the Administration and Payment of Individual Entitlements), in line with the methodology selected, which requires 13 % of transactions by value to undergo *ex post* controls. The percentage of the total EU budget (C1 funds) committed was at the level of 99.93 % according to ENISA's final accounts. Access rights to the accrual-based accounting system were validated by a neutral verifier and the results shared with the European Commission's Directorate-General for Budget. A policy on sensitive positions is in place and assessed on a regular basis. Moreover, a risk assessment on sensitive positions was performed in 2022 and endorsed by ENISA's Management Team.

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, but certain identified high security risks were not fully mitigated within 2022 in a timely manner. Immediate action on the pending issues was undertaken in 2023.

However, the performance of the corporate IT systems during 2022 was assessed as high (99 %) on the basis of specific indicators adopted by the ITMC.

In addition, an IT security risk management framework was adopted and an IT security risk assessment was performed at the end of 2022 (as part of the broader ERM framework). When the results were presented to ENISA's Management Team, specific mitigation actions were endorsed that will be followed up (under a specific action plan).

There was no high-risk security incident or any incident requiring reporting to CERT-EU in 2022.

The total percentage of the IT budget allocated to information security in 2022 amounted to approximately 15 %.

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 as ENISA's internal policies and procedures are not adequately documented or communicated to staff.


Moreover, out of 27 exceptions identified and registered in 2022, none was assessed as high risk (23 were assessed as low risk and four as medium risk). The four medium-risk exceptions were related to transactions between EUR 10 000 and EUR 20 000, of which three concerned *a posteriori* commitments (i.e. the budgetary commitments were signed after the legal commitments, breaching ENISA's applicable financial rules intended to ensure that ENISA has sufficient budget to honour its financial obligations stemming from legal commitments) and one was 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.

3.1.4. Assessment of the information and communication component

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

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

The assessment concluded that this principle is present and functioning, but some improvements are needed, as internal information sharing and mapping



Frequent question-and-answer sessions for all staff on various relevant topics were organised throughout 2022.

of information could be improved and the need-to-know principle (to access internal information) needs further assessment.

The agency registers and archives all its official documents (outgoing and incoming) in a dedicated registration system. In 2021, the agency started its migration to ARES, the European Commission's registration system. The completion of this project is expected in 2023. This new development supports the principle of single administration within ENISA (the same tools and processes are used by staff internally). ENISA uses various tools for internal communications; the most common are ENISA's intranet, email, Skype for Business and WebEx.

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. The weekly Management Team meeting minutes are made available by email to all staff. In addition, frequent question-and-answer sessions for all staff on various relevant topics were organised throughout 2022. 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 whistleblowing policy.

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. The agency communicates about its internal controls essentially through the annual activity report.

3.1.5. Assessment of the monitoring activities component

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

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

The assessment concluded that this principle is present and functioning, but some improvements are needed; for example, recommendations and risks identified in *ex ante* and *ex post* controls and other financial evaluations are not followed up in a timely manner.

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 some improvements are needed; for example, mitigation measures are only partially addressed in a timely manner.

3.2. CONCLUSIONS OF ASSESSMENT OF INTERNAL CONTROL SYSTEMS

The overall assessment shows that the internal controls at ENISA provide reasonable assurance that policies, processes, tasks and behaviours at the agency, taken together, facilitate its effective and efficient operation, help to ensure the quality of internal and external reporting and help to ensure compliance with its regulations. That being said, some improvements are needed in relation to certain principles to increase effectiveness and ensure proper implementation of the internal controls. The follow-up on these improvements will be assessed during the next mid-term review of the agency.

3.3. STATEMENT OF THE INTERNAL CONTROL COORDINATOR IN CHARGE OF RISK MANAGEMENT AND INTERNAL CONTROL

I, the undersigned,

The manager in charge of risk management and internal control within the European Union Agency for Cybersecurity (ENISA),

In my capacity as Head of the Executive Director's Office, in charge of risk management and internal control, declare that, in accordance with the ENISA internal control framework, I have reported my advice and recommendations on the overall state of internal control in the agency to the Executive Director.

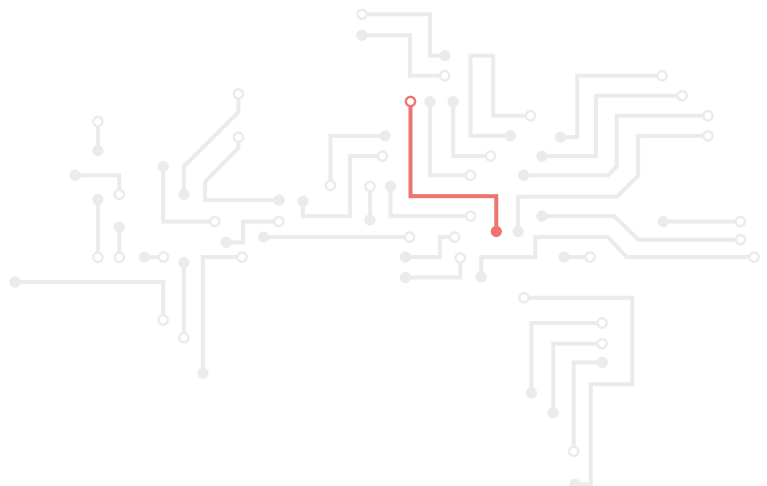
I hereby certify that the information provided in the present consolidated annual activity report and in its annexes is, to the best of my knowledge, accurate, reliable and complete.

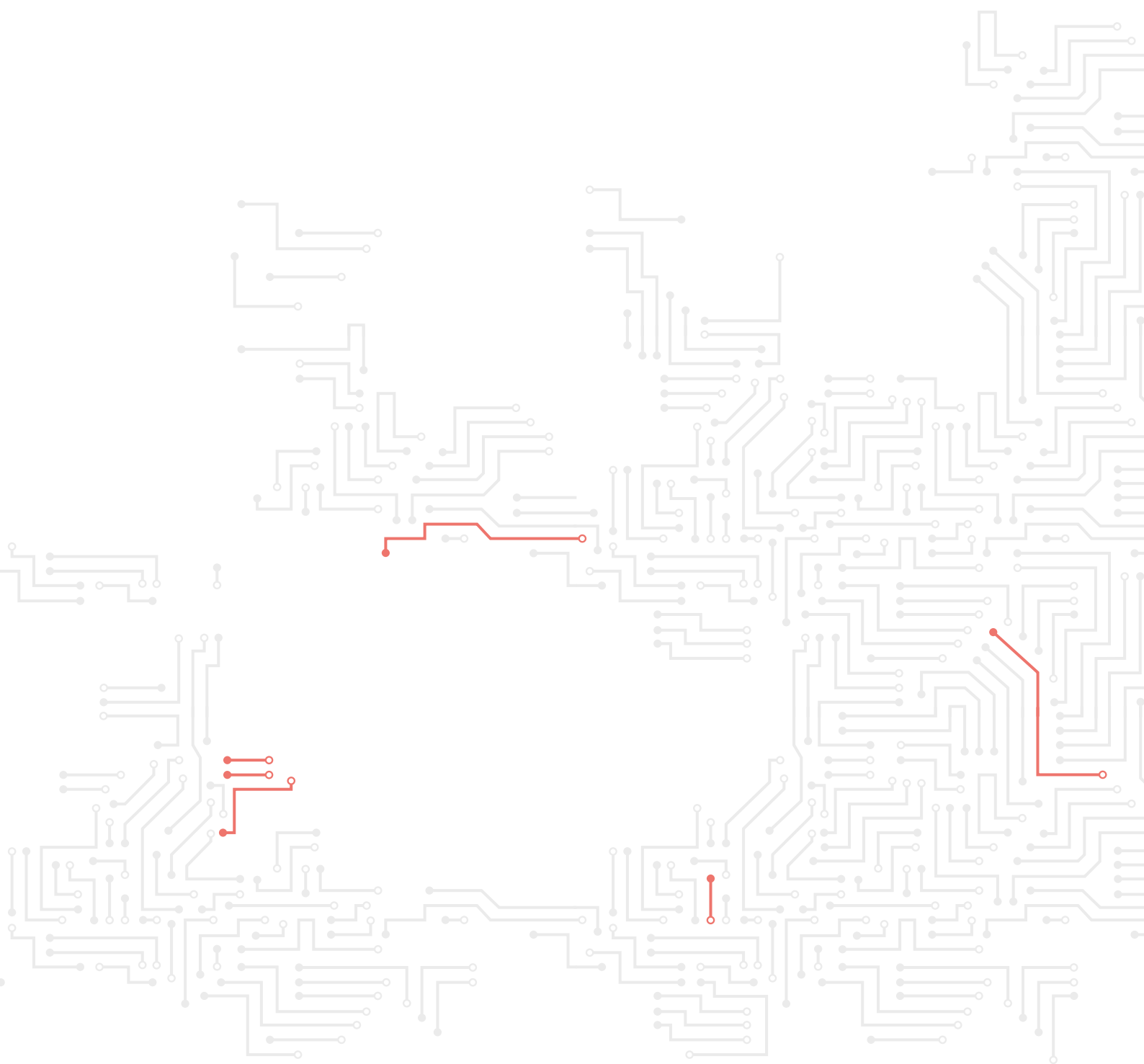
A handwritten signature in blue ink, appearing to read "Ingrida Taurina".

Ingrida Taurina

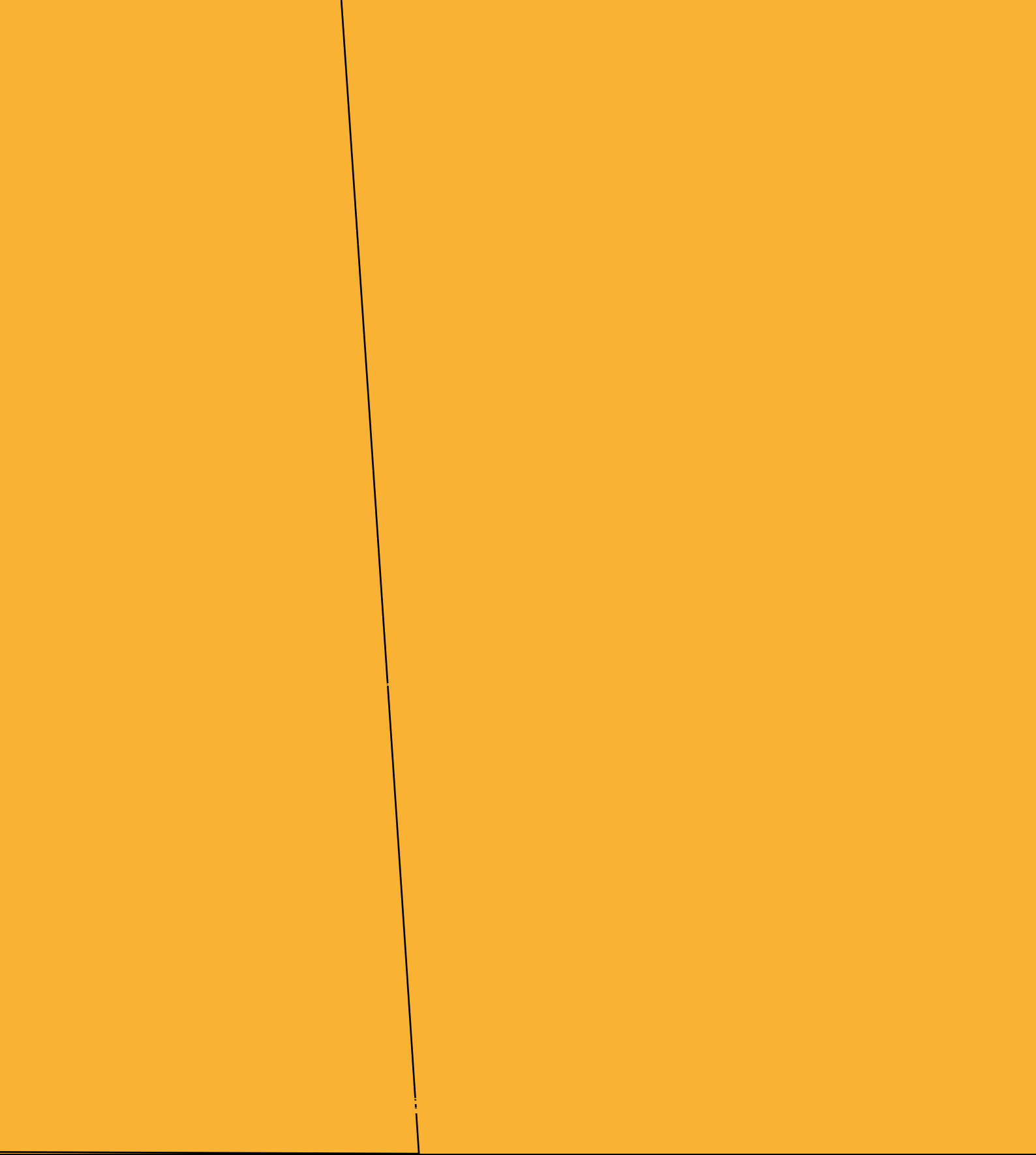
Head of the Executive Director's Office

Athens, 6th June 2023





V



KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (<i>ex ante</i>)					
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	95 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	91 %

N/A, not applicable.

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
Contribution to policy implementation and implementation monitoring at EU and national levels (<i>ex post</i>)					
2.1. Number of EU policies and regulations implemented at national level supported by ENISA	Number	Annual	Manual collection from staff members	5	5
2.2. Number of ENISA reports, analyses and/or studies referred to at EU and national levels	Number	Biennial	Survey	N/A	65
2.3. Satisfaction with ENISA added value of support	%	Biennial	Survey	N/A	94 %
% of stakeholders rating outcome/ result of ENISA work as high or some added value	%	Biennial	Survey	N/A	93 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	87 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	90 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	97 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	93 %

N/A, not applicable.

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents					
3.1. Increase/decrease in maturity indicators ^a					
Maturity of NCSSs					
Number of Member States that rate the overall maturity of their cybersecurity strategy					
High maturity	Number	Annual	Survey	3	6
Medium maturity	Number	Annual	Survey	4	5
Low maturity	Number	Annual	Survey	3	0
Number of Member States planning to use ENISA framework to measure the maturity of their national cybersecurity capabilities					
Already using	Number	Annual	Survey	1	2
Not using but planning to use	Number	Annual	Survey	5	9
Don't know or will not use in the foreseeable future	Number	Annual	Survey	4	2
Number of Member States that have set KPIs to measure the progress and effectiveness of the implementation of their strategic objectives when drafting their NCSS					
Already using	Number	Annual	Survey	3	9
Not set but planning to use	Number	Annual	Survey	4	5
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	3	0
The frequency in which Member States update their strategy to adapt to technological advancements and new threats					
Every 2–3 years	Number	Annual	Survey	2	1
Every 4–5 years	Number	Annual	Survey	6	12
More than 6 years or don't know	Number	Annual	Survey	2	1
Sectorial ISACs coverage					
Percentage of NISD2 sectors having an EU ISAC	%	Annual	Report	—	60 %
3.2. Outreach, uptake and application of lessons learned from capability-building activities					
C2021 cyber standard operating practice exercise (number of improvements proposed by participants)	Number	Per exercise	—	5	5
3.3. Number of cybersecurity programmes (courses) and participation rates ^b					
Total number of students enrolled in the first year of the academic programmes (2020)	Number	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	4 843	5 205
Student gender distribution (% female to % male)	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	20 % to 80 %	19 % to 81 %

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents					
Total number of cybersecurity programmes (2020)	Number	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	119	122
Percentage of postgraduate programmes	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	6 %	5 %
Percentage of master's degree programmes	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	77 %	80 %
Percentage of bachelor's degree programmes	%	Annual	https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education	17 %	15 %
3.4. Number of exercises executed annually					
Number of exercises executed annually	Number	Annual	Report	5	5
3.5. Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey)					
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	97 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	77 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	80 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	96 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	97 %
Standard operating practice exercise (SOPex) series					
Usefulness low	%	Per exercise	Survey	9 %	6 %
Usefulness medium	%	Per exercise	Survey	71 %	54 %
Usefulness high	%	Per exercise	Survey	20 %	40 %

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents					
Relevance low	%	Per exercise	Survey	4 %	7 %
Relevance medium	%	Per exercise	Survey	53 %	53 %
Relevance high	%	Per exercise	Survey	43 %	40 %
Cyber Europe exercise series (biannual)					
Usefulness low	%	Per exercise	Survey	—	6 %
Usefulness medium	%	Per exercise	Survey	—	54 %
Usefulness high	%	Per exercise	Survey	—	40 %
Relevance low	%	Per exercise	Survey	—	7 %
Relevance medium	%	Per exercise	Survey	—	53 %
Relevance high	%	Per exercise	Survey	—	40 %
Jasper series					
Data to be made available from 2023	%	Per exercise	Survey	—	—

N/A, not applicable.

- a This KPI should be viewed over a period of a number of years. The 2021 KPI establishes the 'baseline' that allows us to gauge the evolution of the corresponding maturity indicator in the coming years.
- b This KPI should be viewed over a period of a number of years. The 2021 KPI establishes the 'baseline' that allows us to gauge the evolution of the corresponding maturity indicator in the coming years. As of 2023, this KPI will be moved under Activity 9.

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
Effective use of ENISA's tools and platforms and take-up of SOPs in operational cooperation					
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	115 %	19 %
Number of exchanges/interactions increase year on year	%	Annual	Platform	291 %	104 %
EU-Cyclone increase year on year					
Active users increase year on year	%	Annual	Platform	143 %	2 %
Number of exchanges/interactions increase year on year	%	Annual	Platform	1 011 %	548 %
4.2. Uptake of platforms/tools/SOPs during massive cyberincidents	—	—	—	N/A	N/A ^a
4.3. Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs provided by ENISA (survey)	%	Biennial	Survey	N/A	89 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	94 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	84 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	83 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	94 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	87 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	94 %

N/A, not applicable.

^a Although the networks were in escalated mode, this situation was not deemed a large-scale cybersecurity incident as defined by NISD2, Article 6(7).

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
ENISA's ability to support the response to massive cyberincidents					
5.1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents that ENISA contributes to mitigation efforts	—	Biennial	—	N/A	Postponed ^a
5.2. Stakeholder satisfaction with ENISA's ability to provide operational support (survey)	%	Biennial	Survey	N/A	84 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	82 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	73 %
% of stakeholders likely to take up results of ENISA's work immediately or in medium term	%	Biennial	Survey	N/A	86 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	82 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	82 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	100 %
5.3. Number of relevant incident responses ENISA contributed to as per the CSA, Article 7	Number	Annual	ENISA	N/A	2

N/A, not applicable.

a The survey was postponed owing to the reprioritisation of resources for the cybersecurity support action.

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
Effectiveness of ENISA's supporting role for participants in the European cybersecurity market					
7.1. Number of market analyses, guidelines and good practices issued by ENISA					
Cybersecurity market analysis framework	Number	Annual	Reports	Two	Five in different stages (two reports pending publication, two internal reports, one report published)
7.2. Uptake of lessons learned / recommendations from ENISA reports					
% of respondents interested in using ENISA's good practice on market analyses	%	Annual	Survey	87 % (fully and partially interested)	85 % (high and medium interest)
% of respondents interested in using ENISA's standards mapping related to digital identities	%	Annual	Survey	N/A	89 % (high and medium interest)
% of respondents interested in using ENISA's standards mapping related the internet of things	%	Annual	Survey	88 % (high and medium interest)	89 % (high and medium interest)
% of respondents interested in using ENISA's standards mapping related to AI	%	Annual	Survey	N/A	82 % (high and medium interest)
% of respondents interested in using ENISA's risk-based approach for their cybersecurity certification activities	%	Annual	Survey	72 % (high and medium interest)	86 % (high and medium interest)
% of respondents interested in using ENISA's consolidated certification labelling process	%	Annual	Survey	84 % (high and medium interest)	93 % (high and medium interest)
% of respondents interested in using ENISA's vulnerability management process for certified products, services and processes	%	Annual	Survey	82 % (high and medium interest)	89 % (high and medium interest)
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work (survey)	%	Biennial	Survey	N/A	88 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	88 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	84 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	72 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	100 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	93 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	94 %

N/A, not applicable.

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge, including contributions to the research and innovation agenda					
8.1. Number of users and frequency of use of a dedicated portal (observatory) ^a					
8.2. Total number of recommendations, analyses and challenges identified and analysed	Number	Annual	ENISA reports and studies	288	357
8.3. Number of requests from Member States and EU research and innovation entities to contribute to, provide advice on or participate in activities	Number	Annual	Internal report	N/A	63
8.4. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research (survey)	%	Biennial	Survey	N/A	91.5 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	94 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	90 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	86 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	94 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	94 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	91 %

N/A, not applicable.

^a Infohub has yet to be implemented.

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
1. Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU					
2. Level of outreach					
9.1. Number of cybersecurity incidents reported having human error as a root cause	Number	Annual	CIRAS tool	173	153
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	20 756 630	27 278 491
Total social media engagement	Number	Annual	ENISA analytics	117 720	19 301
Total video views	Number	Annual	ENISA analytics	2 021 129	6 602 355
Total website visits	Number	Annual	ENISA analytics	123 504	300 530
Total participation in events	Number	Annual	ENISA analytics	5	40

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
1. Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU					
2. Level of outreach					
CyberAll (formerly Women4Cyber campaign)					
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	201 188	82 900
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	3 865	1 286
Video views	Number	Annual	YouTube	1 283	2 285
Cybersecurity for SMEs campaign					
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	44 497	35 900
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	957	1 200
Video views	Number	Annual	YouTube	736	6 113
Website visits	Number	Annual	ENISA website	24 362	55 082
References	Number	Annual	Media monitoring	~ 40	N/A
Participation in events	Number	Annual	Websites announcements	5	6
NoMoreRansom campaign					
Social media impressions	Number	Annual	Social media (Twitter)	54 022	N/A
Social media engagement	Number	Annual	Social media (Twitter)	465	N/A
Campaign on health					
Social media impressions	Number	Annual	ENISA analytics	N/A	58 200
Social media engagement	Number	Annual	ENISA analytics	—	1 100
Video views	Number	Annual	ENISA analytics	—	197
Website visits	Number	annual	ENISA analytics	—	1 008
Campaign on energy					
Social media impressions	Number	Annual	ENISA analytics	N/A	56 900
Social media engagement	Number	annual	ENISA analytics	—	703
Video views	Number	annual	ENISA analytics	—	224
Website visits	Number	annual	ENISA analytics	—	586
ECSM campaign					
Social media impressions	Number	Annual	ENISA analytics	20 400 000	26 823 591
Social media engagement	Number	Annual	ENISA analytics	110 266	9 000
Video views	Number	Annual	ENISA analytics	2 018 441	6 589 457
Website visits	Number	Annual	ENISA analytics	47 939	179 571

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
1. Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU					
2. Level of outreach					
Certification campaign					
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	85 599	200 000
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	1 701	5 900
Video views	Number	Annual	YouTube	669	4500
Website visits	Number	Annual	ENISA website	1 239	N/A
Cyberhead campaign					
Social media impressions	Number	Annual	Social media	25 292	21 000
Social media engagement	Number	Annual	Social media	466	112
Website visits	Number	Annual	ENISA website	49 964	64 283
9.3. Geographical and community coverage of outreach in the EU	Number	Annual	ENISA analytics	N/A	All 27 Member States and EFTA countries
9.4. Level of awareness of cybersecurity across the EU / general public (e.g. Eurobarometer and other surveys) ^a	—	Biennial	—	—	N/A
9.5. Stakeholder satisfaction with awareness raising and education activities	%	Biennial	Survey	N/A	91 %
% of stakeholders rating outcome/result of ENISA work as high or some added value	%	Biennial	Survey	N/A	100 %
% of stakeholders rating extent of ENISA content that does not duplicate or to some extent duplicates Member States' activities	%	Biennial	Survey	N/A	80 %
% of stakeholders likely to take up results of ENISA work immediately or in medium term	%	Biennial	Survey	N/A	84 %
% of stakeholders satisfied with the way ENISA organised and managed processes for planning and implementing work	%	Biennial	Survey	N/A	95 %
% of stakeholders satisfied that their comments, advice or expertise have been taken into consideration by ENISA	%	Biennial	Survey	N/A	86 %
% of stakeholders satisfied with ENISA's community-building actions	%	Biennial	Survey	N/A	98 %

NB: CIRAS, Cybersecurity Incident Reporting and Analysis System; N/A, not applicable.

a It has been proposed that this KPI be updated in the draft 2024–2026 SPD to reflect the requirements of NISD2, Article 18(1).

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
1. Organisational performance culture					
2. Trust in ENISA brand					
10.1. Proportion of KPIs reaching targets	Number	Annual	AAR	N/A	Targets established as of 2023; however, compared with the base year (2021), 13 metrics were unchanged, 21 underperformed and 58 outperformed
10.2. Individual staff contribution to achieving the objectives of the agency through clear link to KPIs	%	Annual	Staff survey	53 %	64 % ^a
10.3. Exceptions in the risk register	Number	Annual	Internal control	16	27
Deviation from financial regulations	Number	Annual	Internal control	14	26
Deviation from staff regulations	Number	Annual	Internal control	2	1
10.4. Number of complaints filed against ENISA, including number of inquiries/complaints to the European Ombudsman	Number	Annual	—	19	3
To the European Ombudsman	Number	Annual	ENISA functional mailbox	3	0 ^(b)
Under Article 90	Number	Annual	Internal control files	15	3
Under Article 24	Number	Annual	Internal control files	0	0
To European Data Protection Supervisor	Number	Annual	Internal control files	1	0
10.5. Number of complaints addressed in a timely manner and in accordance with relevant procedures	Number	Annual	Internal files	N/A	3 (complaints to the European Ombudsman under Article 90(2) closed successfully in accordance with relevant procedures and addressed in a timely manner)
10.6. Results of the annual risk assessment exercise – see Part III on the internal control framework					
10.7. 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	—	4	0
IAS	Number	Annual	IAS Section 2.7.1	Three important recommendations	The three important recommendations have been closed in 2023

KPI Metric	Unit (of measurement)	Frequency	Data source	2021 results	2022 results
1. Organisational performance culture					
2. Trust in ENISA brand					
ECA	Number	Annual	ECA Section 2.7.2	One critical observation	Four non-critical observations were issued by the ECA in its 2021 report. All observations prior to 2021 have been closed.
10.8. Level of trust in ENISA ^(c) (survey)	%	Biennial	—	—	95 %

NB: AAR, annual activity report; N/A, not applicable.

- a Source of results taken from staff satisfaction survey question 'My contribution and annual objectives at ENISA have a clear link to the objectives and KPIs of the activity(ies) I contribute to'.
- b Complaints submitted in late 2021 were closed in Q3 of 2022.
- c Source of results taken from stakeholder satisfaction survey 'agree' and 'somewhat agree' to the statement 'I am confident in ENISA's ability to achieve its mandate'.

KPI Metric	Unit (of measurement)	Frequency	Data source	2020 results	2021 results	2022 results
Staff commitment, motivation and satisfaction						
11.1. 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)						
% of staff satisfied with their work	%	Annual	Staff satisfaction survey	68 %	76 %	76 %
% of staff seeing a positive atmosphere within ENISA since the reorganisation	%	Annual	Staff satisfaction survey	70 %	58 %	N/A
% of staff feeling confident working within the new organisational culture	%	Annual	Staff satisfaction survey	61 %	68 %	N/A
% of staff indicating their line manager provides sufficient feedback on their performance	%	Annual	Staff satisfaction survey	68 %	76 %	60 %
% of staff indicating their line manager sets clear objectives	%	Annual	Staff satisfaction survey	66 %	76 %	71 %
% of staff feeling well informed by ENISA leadership regarding important matters	%	Annual	Staff satisfaction survey	80 %	73 %	36 %
11.2. Quality of ENISA training and career development activities organised for staff						
% of staff trusting that ENISA will support them in acquiring the necessary skills and capabilities to successfully manage the reorganisation	%	Annual	Staff satisfaction survey	69 %	49 %	N/A
% of staff indicating that courses match their training and development needs	%	Annual	Staff satisfaction survey	N/A	58 %	43 %
% of staff finding that their line manager dedicates enough time during the CDR dialogue for mapping training and development needs	%	Annual	Staff satisfaction survey	N/A	55 %	36 %

KPI Metric	Unit (of measurement)	Frequency	Data source	2020 results	2021 results	2022 results
Staff commitment, motivation and satisfaction						
% of staff finding that their line manager ensures proper follow-up of the training and development needs from the CDR report	%	Annual	Staff satisfaction survey	N/A	47 %	55 %
% of staff finding that they had the opportunity to grow in their career at ENISA since the reorganisation	%	Annual	Staff satisfaction survey	N/A	35 %	38 %
11.3. Reasons for staff departure (exit interviews) ^a						
On a scale of 1 to 10, did the job you were employed for meet your expectations?	Scale 1–10	As required	HR files	N/A	7.5	8.5
On a scale of 1 to 10, did you have all the tools and resources you needed to effectively perform your job?	Scale 1–10	As required	HR files	N/A	6.6	7.5
On a scale of 1 to 10, how would you describe the tasks assigned and workload (tasks too demanding/not demanding; too much workload/not enough tasks)?	Scale 1–10	As required	HR files	N/A	7.75	7
On a scale of 1 to 10, how would you rate the management style of your immediate supervisor?	Scale 1–10	As required	HR files	N/A	6.5	7.5
On a scale of 1 to 10, what was your working relationship with your manager like?	Scale 1–10	As required	HR files	N/A	7.25	8.5
On a scale of 1 to 10, how would you describe your relationship and communication with your colleagues?	Scale 1–10	As required	HR files	N/A	8.4	9
On a scale of 1 to 10, did you have clear performance objectives in your job (10 being crystal clear and 0 being not clear at all)?	Scale 1–10	As required	HR files	N/A	6.8	8
On a scale of 1 to 10, how competitive would you say the compensation and benefits were for your position?	Scale 1–10	As required	HR files	N/A	6.6	8.5
On a scale of 1 to 10, how would you rate your employee experience in the agency?	Scale 1–10	As required	HR files	N/A	6.6	7
11.4. Staff retention / turnover rate	%	Annual	HR files	2 %	3 %	4 %
11.5. Resilience and quality of ENISA IT systems and services (including ability to consistently increase satisfaction with IT services and tools)						
Critical systems downtime	%	Annual	Uptime report of FortiMail	N/A	99.38 %	100 %
% of central IT infrastructure assessments with few (< 5) critical findings	%	Annual	Intranet repository	N/A	100 %	100 %
% of central infrastructure patched to the last formal versioning of 1 year	%	Annual	Yearly IT maintenance plan in PDF	N/A	95 %	97.33 %
% of major IT help desk requests resolved in a satisfactory way within 2 business days	%	Annual	IT ticket repository	N/A	80 %	79.28 %

KPI Metric	Unit (of measurement)	Frequency	Data source	2020 results	2021 results	2022 results
Staff commitment, motivation and satisfaction						
% of staff satisfied with resolution	%	Annual	Staff survey	N/A	N/A	84 %
% of staff rating ENISA's out-of-hours support service a 4 or a 5	%	Annual	Staff survey	N/A	N/A	38 %
% of staff indicating that the IT help desk responds within a reasonable time	%	Annual	Staff survey	N/A	75 %	83 %
% of staff rating DMSs favourably	%	Annual	Staff survey	N/A	N/A	44 %
% of staff that can easily find information on intranet easily	%	Annual	Staff survey	N/A	N/A	41 %
% of staff satisfied with the meeting rooms' audiovisual equipment	%	Annual	Staff survey	N/A	N/A	53 %
% of staff satisfied with the Webex services' performance	%	Annual	Staff survey	N/A	N/A	82 %
% of staff not aware of the online service catalogue	%	Annual	Staff survey	N/A	N/A	72 %

NB: DMS, document management system; N/A, not applicable.
a The greater the number the better the performance and vice versa.

ANNEX 2

STATISTICS ON FINANCIAL MANAGEMENT

Budget out-turn and cancellation of appropriations (in EUR)

Budget out-turn	2020	2021	2022
Reserve from the previous years' surplus (+)			
Revenue actually received (+)	21 801 460	23 058 211	39 227 392
Payments made (-)	- 15 050 421	- 17 989 374	- 20 396 780
Carry-over of appropriations (-)	- 6 200 614	- 5 082 548	- 18 836 095
Cancellation of appropriations carried over (+)	180 023	209 385	248 745
Adjustment for carry-over of assigned revenue appropriation from previous year (+)	10 403	125 622	33 743
Exchange rate differences (+/-)	- 1 291	- 428	- 17
Adjustment for negative balance from previous year (-)			
Total	739 560	320 868	276 988

Execution of commitment appropriations in 2022

In EUR	Chapter	Commitment appropriations authorised ^a	Commitments made	% Commitment rate
A-11	Staff in active employment	9 859 760	9 859 760	100.00 %
A-12	Recruitment/Departure Expenditure	287 409	287 409	100.00 %
A-13	Sociomedical Services and Training	1 182 072	1 181 581	99.96 %
A-14	Temporary Assistance	6 95 428	695 428	100.00 %
	Title I	12 024 669	12 024 178	100.00 %
A-20	Buildings and Associated Costs	1 044 795	1 028 295	98.42 %
A-21	Movable Property and Associated Costs	64 137	64 137	100.00 %
A-22	Current Administrative Expenditure	952 915	952 259	99.93 %
A-23	ICT	1 873 073	1 851 568	98.85 %
	Title II	3 934 920	3 896 259	99.02 %
B-30	Activities Related to Outreach and Meetings	563 440	542 365	96.26 %
B-37	CSA Core Operational Activities	8 384 397	8 366 604	99.79 %
B-38	Core Operational Activities – Assistance Funds	14 353 668	14 350 000	99.97 %
	Title III	23 301 505	23 258 969	99.82 %
	Total	39 261 094	39 179 406	99.79 %

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

Execution of payment appropriations in 2022

In EUR	Chapter	Payment appropriations authorised ^a	Payments made %	Payment rate
A-11	Staff in Active Employment	9 859 760	9 859 760	100.00 %
A-12	Recruitment/Departure Expenditure	287 409	252 896	87.99 %
A-13	Sociomedical Services and Training	1 182 072	862 918	73.00 %
A-14	Temporary Assistance	695 428	372 998	53.64 %
	Title I	12 024 669	11 348 572	94.38 %
A-20	Buildings and Associated Costs	1 044 795	726 652	69.55 %
A-21	Movable Property and Associated Costs	64 137	15 290	23.84 %
A-22	Current Administrative Expenditure	952 915	214 614	22.52 %
A-23	ICT	1 873 073	1 055 815	56.37 %
	Title II	3 934 920	2 012 372	51.14 %
B-30	Activities Related to Outreach and Meetings	563 440	481 631	85.48 %
B-37	CSA Core Operational Activities	8 384 397	6 554 205	78.17 %
B-38	Core Operational Activities – Assistance Funds	14 353 668	–	0.00 %
	Title III	23 301 505	7 035 836	30.19 %
	Total	39 261 094	20 396 780	51.95 %

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

Carry-forward to 2023 (open amounts as of 31 December 2022)

In EUR	Chapter	Commitments made	Payments made %	Amount to be paid in 2023	% Amount to be paid
A-11	Staff in active employment	9 859 760	9 859 760	–	0.0 %
A-12	Recruitment/departure expenditure	287 409	252 896	34 513	12.0 %
A-13	Sociomedical services and training	1 181 581	862 918	318 663	27.0 %
A-14	Temporary assistance	695 428	372 998	322 430	46.4 %
	Title I	12 024 178	11 348 572	675 606	5,6 %
A-20	Buildings and associated costs	1 028 295	726 652	301 643	29.3 %
A-21	Movable property and associated costs	64 137	15 290	48 847	76.2 %
A-22	Current administrative expenditure	952 259	214 614	737 644	77.5 %
A-23	Information and communication technologies	1 851 568	1 055 815	795 753	43.0 %
	Title II	3 896 259	2 012 372	1 883 887	48.4 %
B-30	Activities related to outreach and meetings	542 365	481 631	60 734	11.2 %
B-36	CSA Core operational activities	8 366 604	6 554 205	1 812 398	21.7 %
B-38	Core Operational Activities – Assistance Funds	14 350 000	–	14 350 000	100.0 %
	Title III	23 258 969	7 035 836	16 223 133	69.8 %

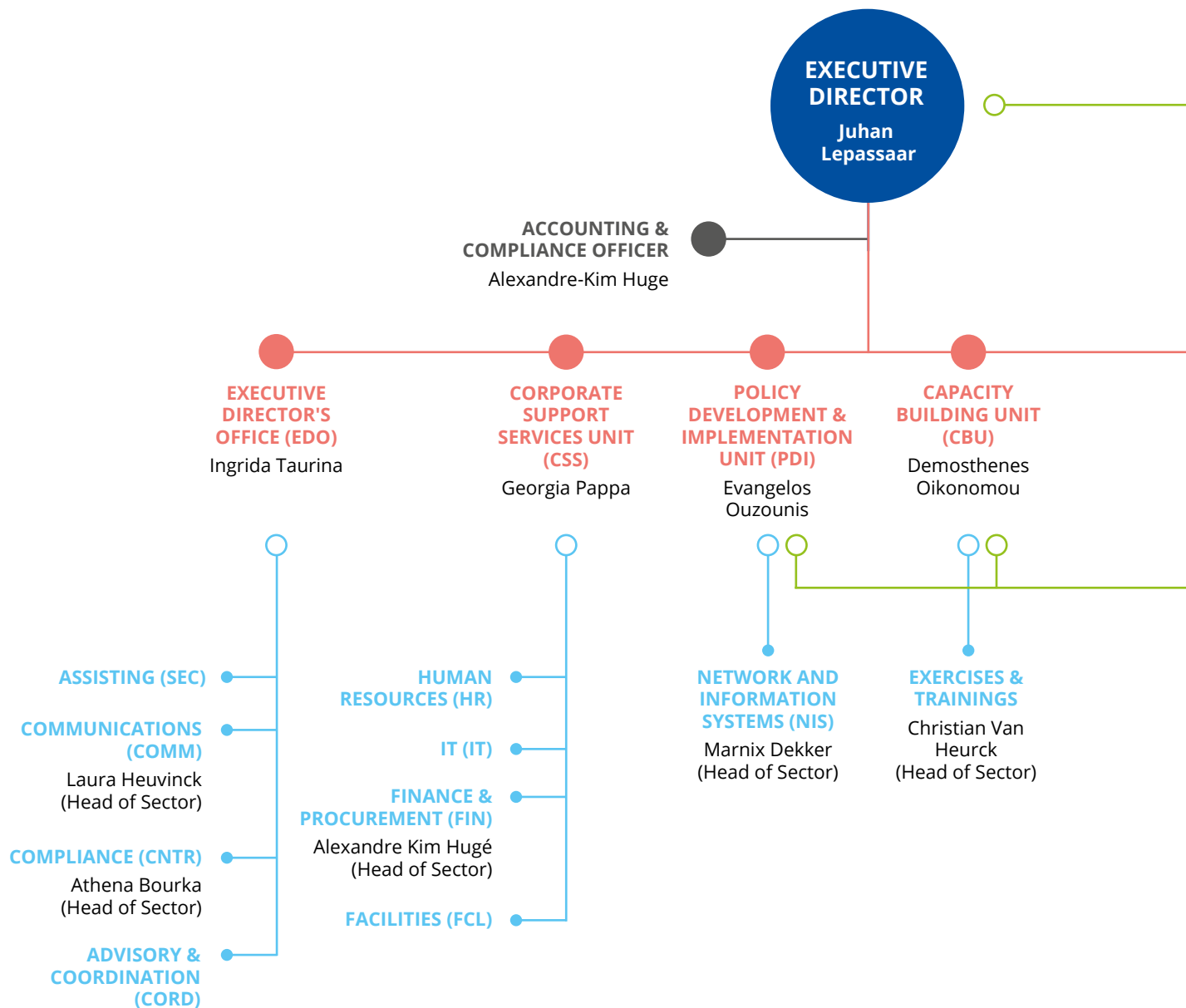
Revenue and income during 2022 (in EUR)

Type of revenue	Entitlements established	Revenue received	Outstanding at the end of the year
Subsidy from the EU Budget	39 207 625.00	39 207 625.00	–
Subsidy from Hellenic Authorities	–	–	–
Revenue from Administrative Operations	25 366.76	19 766.76	5 600
Total	39 232 992	39 227 392	5 600

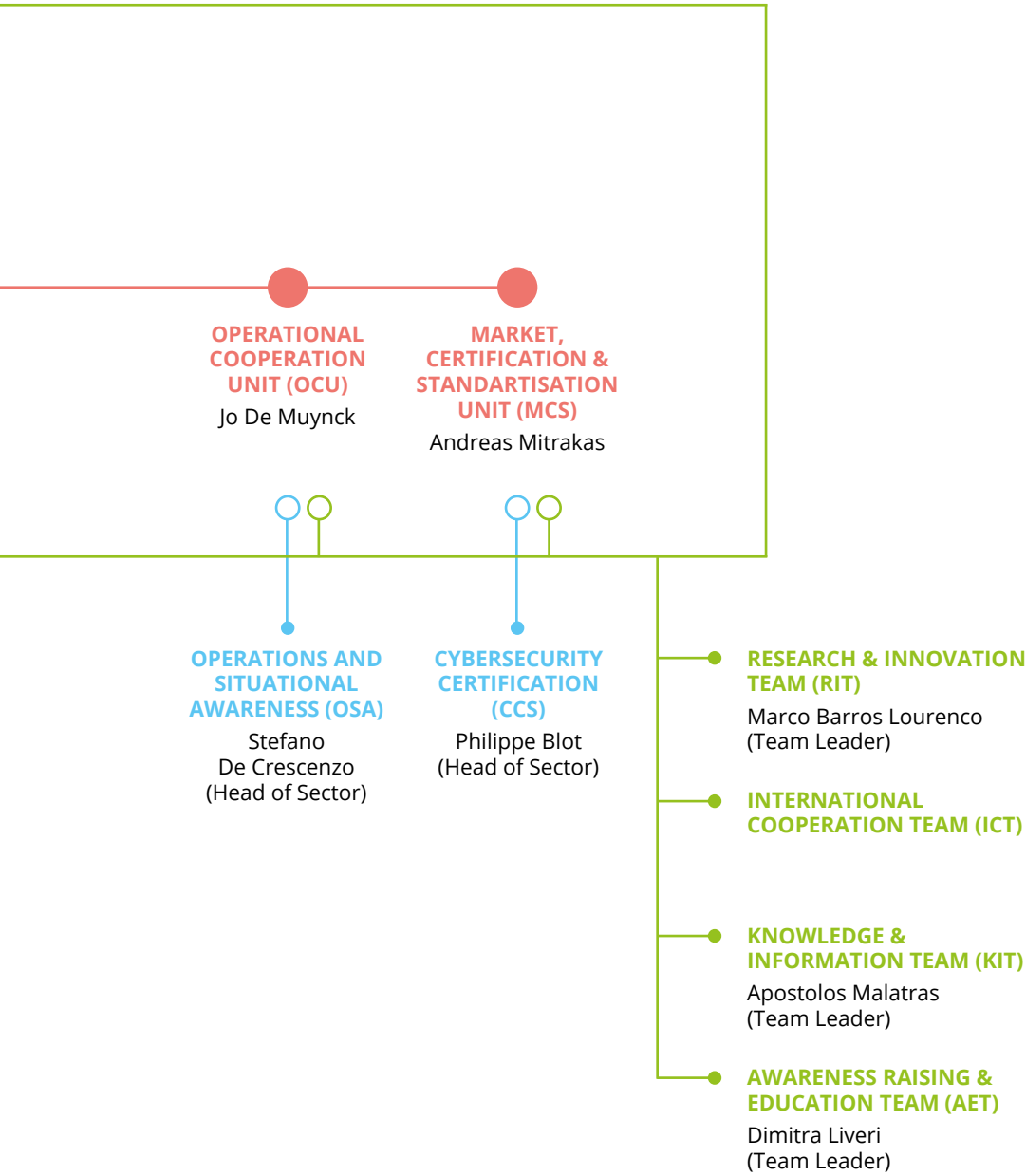
Total revenue may differ from commitment appropriations authorised as total revenue is based on actual income whereas commitment appropriations may use estimates for other, minor administrative revenue

ANNEX 3

ORGANISATIONAL CHART



- UNITS (incl. Head of Unit)
- SECTORS (incl. Head of sector, where relevant)
- TRANSVERSAL TEAMS (incl. Team Leader)



ANNEX 4

2022 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT

2022 establishment plan

Function group and grade	Establishment plan in 2022 voted EU budget		Positions filled as of 31 December 2022	
	Officials	Temporary agents	Officials	Temporary agents
AD 16				
AD 15		1		
AD 14				1
AD 13		2		1
AD 12		4		4
AD 11		2		2
AD 10		4		1
AD 9		11		12
AD 8		22		8
AD 7		8		11
AD 6		9		15
AD 5				
Total number of ADs		63		55
AST 11				
AST 10				
AST 9				
AST 8		2		2
AST 7		3		1
AST 6		8		5
AST 5		5		4
AST 4		1		4
AST 3				1
AST 2				1
AST 1				
Total number of ASTs		19		18
AST/SC 6				
AST/SC 5				
AST/SC 4				

Function group and grade	Establishment plan in 2022 voted EU budget		Positions filled as of 31 December 2022	
	Officials	Temporary agents	Officials	Temporary agents
AST/SC 3				
AST/SC 2				
AST/SC 1				
Total number of AST/SCs				
Total		82		73

NB: AD, administrator; AST, assistant; AST/SC, assistant-secretary.

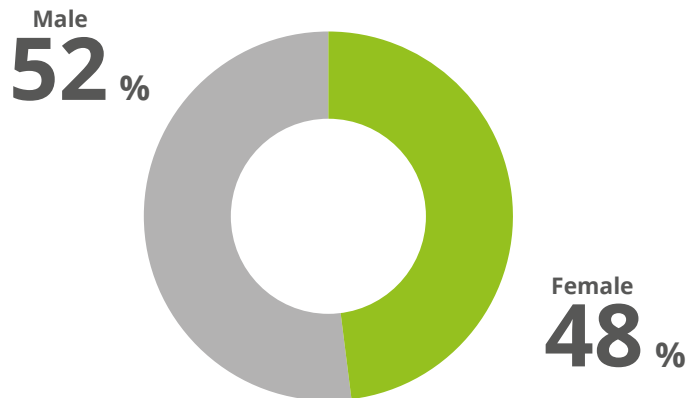
Information on entry level for each type of post

Job title	Type of contract (official, temporary agent, contract agent or seconded national expert)	FG / grade of recruitment	Function (administrative support or operations)
Executive Director	Temporary agent	AD 14	Top operations
Adviser	Temporary agent	AD 12	Administrative
Head of unit	Temporary agent	AD 9	Administrative/operations
Head of sector	Temporary agent	AD 6	Administrative/operations
Team leader	Temporary agent	AD 7	Operations
Senior cybersecurity expert	Temporary agent	AD 9	Operations
Cybersecurity expert	Temporary agent	AD 6	Operations
Cybersecurity officer	Contract agent	FG III	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	Operations
Spokesperson	Temporary agent	AD 6	Administrative
Legal adviser	Temporary agent	AD 7	Administrative
Data protection officer	Temporary agent	AD 7	Administrative
Information security officer	Temporary agent	AD 7	Administrative
Administrator	Temporary agent	AD 8	Administrative
Accounting	Temporary agent	AD 8	Administrative
Seconded national expert	Seconded national expert	N/A	Operations

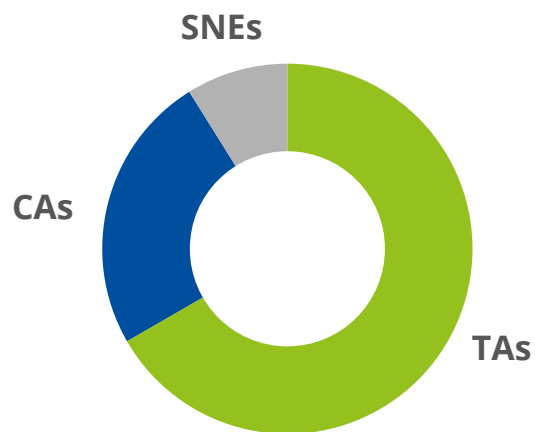
NB: AD, administrator; AST, assistant; FG, function group; N/A, not applicable.

Information on benchmarking exercise

Gender distribution, statutory staf, as of 31/12/2022



Gender distributed by contract type, as of 31/12/2022



Management	2021		2022	
	Number ^(a)	%	Number ^a	%
Female managers	5	30	5	30
Male managers	12	70	12	70

a The managers are the Executive Director (1), heads of unit (6), team leaders (3) and heads of sector (7).

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

Grades	2018 (ref. year 2017)	2019 (ref. year 2018)	2020 (ref. year 2019)	2021 (ref. year 2020)	2022 (ref. year 2021)	Actual average over 5 years	Average over 5 years according to Decision C(2015) 9563
AD 5	—	—	—	—	—	—	2.8
AD 6	2	3	0	1	1	3.8	2.8
AD 7	0	0	1	0	2	3	2.8
AD 8	1	1	2	1	3	4.1	3
AD 9	1	0	0	0	0	10	4
AD 10	0	0	0	0	2	10	4
AD 11	0	0	0	0	0	0	4
AD 12	0	0	0	1	0	10	6.7
AD 13	0	0	1	0	10	10	6.7
AST 1	—	—	—	—	—	—	3
AST 2	—	—	—	—	—	—	3
AST 3	1	1	0	0	1	5.1	3
AST 4	1	1	1	0	0	4.33	3
AST 5	1	0	0	1	0	5.5	4
AST 6	0	0	1	1	0	3.5	4
AST 7	0	0	0	1	1	4	4
AST 8	—	—	—	—	—	—	4
AST 9	—	—	—	—	—	—	N/A
AST 10 (senior assistant)	—	—	—	—	—	—	5

NB: AD, administrator; AST, assistant; N/A, not applicable; ref., reference.

Reclassification of contract agents

Contract agents	Grade	Staff members reclassified in 2022 (ref. year 2021)	Average number of years in grade of reclassified staff members	Average number of years in grade of reclassified staff members according to Decision C(2015) 9561
Function group IV	17	—	—	Between 6 and 10 years
	16	—	—	Between 5 and 7 years
	15	1	4	Between 4 and 6 years
	14	1	5.8	Between 3 and 5 years
	13	—	—	Between 3 and 5 years
Function group III	11	—	—	Between 6 and 10 years
	10	1	3	Between 5 and 7 years
	9	1	3	Between 4 and 6 years
	8	—	—	Between 3 and 5 years
Function group II	6	—	—	Between 6 and 10 years
	5	—	—	Between 5 and 7 years
	4	—	—	Between 3 and 5 years
Function group I	3	—	—	N/A
	2	—	—	Between 6 and 10 years
	1	—	—	Between 3 and 5 years

NB: ref., reference.

Schooling

Agreement in place with the School of European Education of Heraklion	
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	Executive Director Decision No EDD/2021/41 on financial support for the staff of ENISA in relation to the cost of schooling remains in place

Human resources by activity

The allocation of financial and human resources for 2022 for the operational and corporate activities described in Part I of this consolidated annual activity report is presented in the table below. The allocation was determined according to the direct budget and number of full-time equivalents (FTEs) reported for each activity, with the indirect budget being assigned based on drivers such as direct FTEs.

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

- The direct budget is the actual cost for each of the nine operational activities described in Part I of this consolidated annual activity report in terms of services, goods and missions.
- The indirect budget is the actual cost for salaries and allowances, buildings, IT, equipment and miscellaneous operating costs attributable to each activity. The indirect budget was allocated to activities based on drivers. The main driver for cost allocation was the number of direct FTEs spent for each operational activity in 2022.
- Cybersecurity support action funds (EUR 15 million) have been included under Activity 5, including the reallocated 10.5 FTEs.
- For the purpose of the allocation of human and financial resources, an Executive Director's Office activity (Activity 10 as described in Part I) (budget and FTEs), which includes coordination, compliance, communication and administration, was allocated for all of the agency's operational activities.
- For the purpose of the allocation of human and financial resources, Corporate Support Service activity (Activity 11 as described in Part I), including HR, IT services, procurement and finance, facilities and logistics, was allocated for all of the agency's operational activities.

Allocation of human and financial resources - all funds including Cybersecurity Support Action funds	Budget allocation (in EUR)	FTE allocation
Activity 1 - Providing assistance on policy development	1 504 130,01	7,09
Activity 2 - Supporting implementation of Union policy and law	2 996 538,66	13,66
Activity 3 - Building capacity		

ANNEX 6

GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENT

ENISA does not receive any form of grant.

Active service-level agreements with other EU agencies in 2022:

- with Cedefop for the purposes of increasing cooperation and sharing services between the two agencies;
- with BEREC for provision of electronic data backup services;
- with the European Union Intellectual Property Office for disaster recovery services;
- with the EDA for the establishment of a structured cooperation;
- with the EDA, EC3 and CERT-EU for cooperation supported by all the parties' respective mandates;
- with the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) for a working arrangement;
- with eu-LISA for a 2021–2023 cooperation plan;
- with Europol for co-operative relations to support the Member States;
- with Europol for the EC3 working group on security and safety online;
- with the European Union Aviation Safety Agency for a permanent secretariat;
- with the European Food Safety Authority for the Shared Support Office under the EU Agencies Network;
- with the European Data Protection Supervisor for increasing cooperation.

ANNEX 7

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.

In 2021, the Management Board of ENISA established in the agency's 2022–2024 SPD the goal for the agency to achieve climate neutrality (defined as zero CO₂, CH₄ and N₂O emissions) across all its operations by 2030. As a first step, the agency undertook in 2022 an exercise to map its current climate footprint. Based on an audit of past ENISA emissions for which 2019 and 2021 were used as reference years, it was established that ENISA creates 584 485 tCO₂e of GHG emissions annually, with indirect emissions from purchased electricity (50.33 %) and air travel (36.80 %) being the main sources of impact on the climate.

Furthermore, the audit established that the level of energy emissions per employee in Athens is 1 435 tCO₂ per employee and in Heraklion is 10 times greater (14 217 tCO₂ per employee). Although ENISA staff used air travel 770 times (missions of ENISA staff) in 2019, ENISA also organised 79 in-person meetings in 2019 (and 125 in-person or hybrid/online meetings in 2022). ENISA operated almost entirely online from March 2020 to May 2022.

In its quest to achieve climate neutrality, ENISA anticipates a 41 % 'automatic' reduction of GHG emissions in comparison with base year transitional emissions (2019, 2021) due to external factors (reforms undertaken by the host country – Greece). The remaining 59 % or 413 tCO₂e needs to be tackled by ENISA itself, either through changing its business practices to lessen their impact on the climate (less in-person participation in meetings/ events) or by offsetting emissions if activities cannot be moved online without undermining the objectives of ENISA's operational mandate. However, to be true to the goals set by the Management Board, offsetting should be used only when other options are exhausted. The draft corporate strategy that is scheduled to be discussed at the June 2023 Management Board meeting outlines objectives and KPIs in relation to developing ENISA into a sustainable organisation.

ANNEX 8

ANNUAL ACCOUNTS

Statement of financial position (EUR)

	31 December 2021	31 December 2022
I. Non-current assets	1 994 449	2 073 836
Intangible fixed assets	0	0
Tangible fixed assets	1 994 449	2 073 836
II. Current assets	5 772 118	4 661 489
Short-term receivables	378 897	4 661 489
Cash and cash equivalents	5 393 221	0
Total assets (I. + II.)	7 766 567	6 735 325
III. Non-current liabilities	0	0
Long-term provision for risk and charges	0	0
IV. Current liabilities	1 418 889	1 406 595
EC pre-financing received	320 867	0
Accounts payable	67 797	74 662
Accrued liabilities	1 030 225	1 331 933
Total liabilities (III. + IV.)	1 418 889	1 406 595
V. Net assets	6 347 678	5 328 730
Accumulated result	7 313 389	6 347 678
Surplus/(deficit) for the year	- 965 711	- 1 018 948
Total liabilities and net assets (III. + IV. + V.)	7 766 567	6 735 325

Statement of financial performance (EUR)

	2021	2022
Revenue from the EU subsidy	22 512 193	24 207 625
Revenue from administrative operations	228 252	16 666
Total operating revenue	22 740 445	24 224 291
Administrative expenses	- 14 821 111	- 16 817 269
Staff expenses	- 10 252 970	- 11 354 679
Fixed asset-related expenses	- 836 573	- 765 737
Other administrative expenses	- 3 731 568	- 4 696 853
Operational expenses	- 8 883 259	- 8 425 808
Total operating expenses	- 23 704 370	- 25 243 077
Surplus/(deficit) from operating activities	- 963 925	- 1 018 786
Financial revenue	0	68
Financial expenses	-1 358	- 212
Exchange rate loss	- 428	- 18
Surplus/(deficit) from non-operating activities	- 1 786	- 162
Surplus/(deficit) from ordinary activities	- 965 711	- 1 018 948
Surplus/(deficit) for the year	- 965 711	- 1 018 948

ANNEX 9

LIST OF ACRONYMS, INITIALS
AND ABBREVIATIONS

ACER	European Union Agency for the Cooperation of Energy Regulators
AI	artificial intelligence
AIA	Artificial Intelligence Act
APF	Annual Privacy Forum
AR-in-a-Box	awareness raising in a box
ARES	Advanced Record System
BlueOLEx	blueprint operational level exercise
CA	contract agenda
CDR	career development report
Cedefop	European Centre for the Development of Vocational Training
CEN	European Committee for Standardisation
Cenelec	European Committee for Electrotechnical Standardisation
CESICAT	Centre de Seguretat de la Informació de Catalunya
CEF	Connecting Europe Facility
CERT-EU	Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CIIP	critical information infrastructure protection
CISO	chief information security officer
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	computer security incident response team
CTI	cyber threat intelligence
CTF	capture the flag
CVD	coordinated vulnerability disclosure
CyLEE	cyber law enforcement exercise
DG	Directorate-General
DG Connect	Directorate-General for Communications Networks, Content and Technology
DORA	Digital Operational Resilience Act
DSP	digital service provider
EASA	European Union Aviation Safety Agency
EC3	Europol's European Cybercrime Centre
ECA	European Court of Auditors
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECSC	European Cyber Security Challenge
ECISO	European Cyber Security Organisation
ECSF	European Cybersecurity Skills Framework
ECSM	European Cyber Security Month
EDA	European Defence Agency
EEA	European Economic Area
EEAS	European External Action Service
EECC	European Electronic Communications Code
EFTA	European Free Trade Association
eIDAS	electronic identification and trust services
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cybersecurity
ERA	European Union Agency for Railways

ERM	enterprise risk management
ETIS	the community for Telecom professionals
ETSI	European Telecommunications Standards Institute
EUCC	European Union common criteria scheme
EUCI	European Union classified information
EUCS	European Union cloud services scheme
EU5G	European Union certification scheme for 5G networks
EUIBAs	European Union institutions, bodies and agencies
EU Cycles	EU cybercrisis-linking exercise on solidarity
EU-Cyclone	European Cyber Crisis Liaison Organisation Network
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	full-time equivalent
GDPR	general data protection regulation
GHG	greenhouse gas
HoD	head of department
HoU	head of unit
HR	human resources
IAS	Internal Audit Service
ICC	International Cybersecurity Challenge
ICT	information and communications technology
infohub	information hub
ISAC	Information Sharing and Analysis Centre
IT	information technology
ITMC	Information Technology Management Committee
JCAR	joint cyber assessment report
JCU	Joint Cyber Unit
KPI	key performance indicator
LE	law enforcement
MFF	multi-annual financial framework
MIPS	Mission Information Processing Tool
MoU	memorandum of understanding
NCCA	national cybersecurity certification authority
NCCs	Network of National Coordination Centres
NCSS	national cybersecurity strategy
NIS	network and information security
NISD	network and information security directive
NISD2	second network and information security directive
NISCG	Network and Information Security Cooperation Group
NLO	national liaison officer
OES	operator of essential services
OOTS	once and only technical solution
OpenCSAM	Open Cyber Situational Awareness Machine
SCCG	Stakeholder Cybersecurity Certification Group
SMEs	small and medium-sized enterprises
SNE	seconded national expert
SOCs	security operation centres
SOP	standard operating procedure
SPD	single programming document
UICC	universal integrated circuit card
WEBEx	western Balkans tabletop exercise



ABOUT ENISA

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

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14
Chalandri 15231, Attiki, Greece

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 978-92-9204-639-2