



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONSOLIDATED ANNUAL ACTIVITY REPORT



2021

ISSN 2314-9434

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 2021. The report is based on the 2021 work programme as approved by the Management Board of ENISA in Decision No MB/2020/20 and the amended budget approved by the Management Board of ENISA in **Decision No. MB/2021/18**

The *ENISA Programming Document 2021–2023* was adopted as set out in Annex 1 to that decision.

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

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity, 2022

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 978-92-9204-578-4	ISSN 1830-981X	doi:10.2824/851293	TP-AB-22-001-EN-C
PDF	ISBN 978-92-9204-577-7	ISSN 2314-9434	doi:10.2824/072581	TP-AB-22-001-EN-N



CONSOLIDATED ANNUAL ACTIVITY REPORT 2021

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

FOREWORD	6
ENISA MANAGEMENT BOARD ASSESSMENT	11
EXECUTIVE SUMMARY	15
Implementation of the agency's annual work programme and highlights of the year	15
PART I	
ACHIEVEMENTS OF THE YEAR	19
ACTIVITY 1: PROVIDING ASSISTANCE ON POLICY DEVELOPMENT	20
ACTIVITY 2: SUPPORTING IMPLEMENTATION OF UNION POLICY AND LAW	24
ACTIVITY 3: BUILDING CAPACITY	30
ACTIVITY 4: ENABLING OPERATIONAL COOPERATION	38
ACTIVITY 5: CONTRIBUTE TO COOPERATIVE RESPONSE AT UNION AND MEMBER STATE LEVELS	44
ACTIVITY 6: DEVELOPMENT AND MAINTENANCE OF EU CYBERSECURITY CERTIFICATION FRAMEWORK	48
ACTIVITY 7: SUPPORTING THE EUROPEAN CYBERSECURITY MARKET AND INDUSTRY	54
ACTIVITY 8: KNOWLEDGE ON EMERGING CYBERSECURITY CHALLENGES AND OPPORTUNITIES	60
ACTIVITY 9: OUTREACH AND EDUCATION	66
ACTIVITY 10: PERFORMANCE AND RISK MANAGEMENT	72
ACTIVITY 11: STAFF DEVELOPMENT AND WORKING ENVIRONMENT	76
PART II (A)	
MANAGEMENT	87
1 MANAGEMENT BOARD	87
2 MAJOR DEVELOPMENTS	87
3 BUDGETARY AND FINANCIAL MANAGEMENT	89
4 DELEGATION AND SUB DELEGATION	91
5 HUMAN RESOURCES MANAGEMENT	91
6 STRATEGY FOR GAINS IN EFFICIENCY	92
7 ASSESSMENT OF AUDIT AND EX-POST EVALUATION RESULTS DURING THE REPORTING YEAR	92
8 FOLLOW UP OF RECOMMENDATIONS AND ACTION PLANS FOR AUDITS AND EVALUATIONS	94
9 FOLLOW-UP OF RECOMMENDATIONS ISSUED FOLLOWING INVESTIGATIONS BY THE EUROPEAN ANTI-FRAUD OFFICE	94
10 FOLLOW-UP OF OBSERVATIONS FROM THE DISCHARGE AUTHORITY	94
11 ENVIRONMENTAL MANAGEMENT	94
12 ASSESSMENT BY MANAGEMENT	95

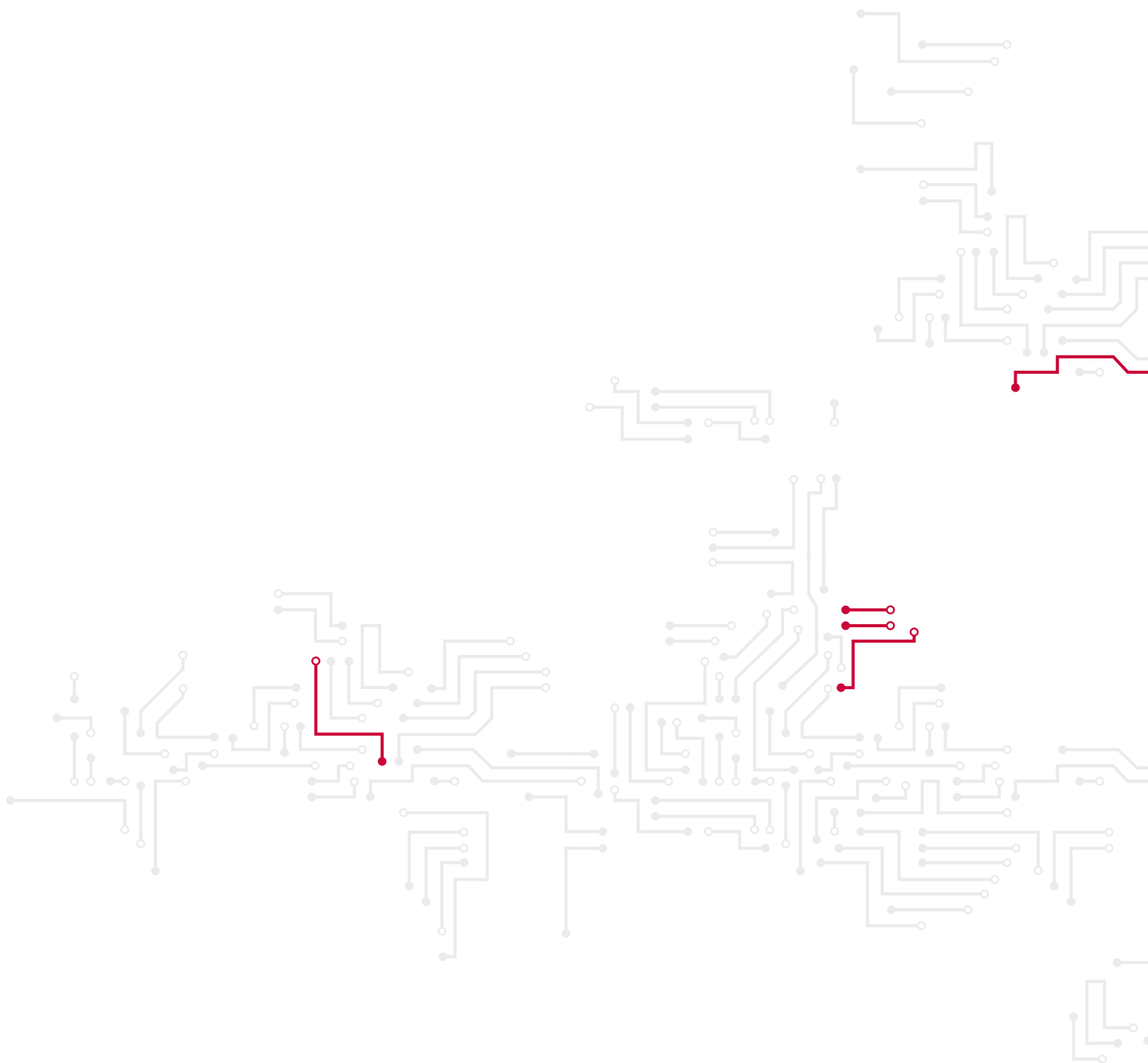
PART II (B)	
EXTERNAL EVALUATIONS	95
PART III	
ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS	97
1 EFFECTIVENESS OF INTERNAL CONTROL SYSTEMS	97
2 CONCLUSIONS OF ASSESSMENT OF INTERNAL CONTROL SYSTEMS	103
3 STATEMENT OF THE INTERNAL CONTROL COORDINATOR IN CHARGE OF RISK MANAGEMENT AND INTERNAL CONTROL	103
PART IV	
MANAGEMENT ASSURANCE	105
1 REVIEW OF THE ELEMENTS SUPPORTING ASSURANCE	105
2 RESERVATIONS	105
PART V	
DECLARATION OF ASSURANCE	107
ANNEX I	
CORE BUSINESS STATISTICS	109
ANNEX II	
STATISTICS ON FINANCIAL MANAGEMENT	119
ANNEX III	
ORGANISATIONAL CHART	122
ANNEX IV	
2021 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT	124
ANNEX V	
HUMAN AND FINANCIAL RESOURCES BY ACTIVITY	130
ANNEX VI	
GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENT	131
ANNEX VII	
ENVIRONMENTAL MANAGEMENT	132

ANNEX VIII
ANNUAL ACCOUNTS

133

ANNEX IX
LIST OF ABBREVIATIONS

135





FOREWORD

2021 was the first full year when the new strategy of the European Union Agency for Cybersecurity (ENISA) (adopted new strategy by the Management Board in June 2020) and its renewed work programme were operational. In terms of cybersecurity challenges, it also proved to be the second year of living with the pandemic and a prelude to the first year of Russia's unprovoked and illegal war on Ukraine, whose cyber dimension started far earlier than the actual invasion and is likely to outlive the atrocities of the current physical confrontation. As an agency, I believe we have learned quickly and have adapted well to both of these external shocks.

The same year showed that we were able to deliver on ENISA's strategic objectives, pursuing a resilient and clear path towards making Europe more cybersecure, as well as adapting our activities to these changing circumstances. Knowing that the political leadership in the EU and in the Member State prioritises cybersecurity continues to be a real boost for the work and motivation of the Agency. The Agency fully carried out its mandate and tasks fully to step up and support the Union by way of the following activities executed in 2021.

The adoption and implementation of policy frameworks is one key response area where the EU is making a difference. Indeed, the policies and initiatives to be put in place in the coming years will determine how the EU faces the cybersecurity challenges of today and tomorrow. Within this framework, ENISA supported Member States with the technical aspects related to Directive (EU) 2016/1148 (the Network and Information security directive (NISD)), and supported the European Parliament and Commission with regard to negotiations on a revised NISD (NISD2) by providing technical expertise through written contributions on supply chain and on the security requirements of the new sector. As connectivity and interdependencies between sectors grow, the proposed expansion of scope under the new NISD2 will cover more sectors and entities, will incentivise these to take better cybersecurity measures and will help fill the persistent gaps, for example in the area of incident-reporting practices. The NISD2 negotiations between the European Parliament and the Council of the European Union have shown a unique cross-party / cross-Member State consensus in favour of this world-leading legislative approach.

The second ENISA network and information security investment study, published in 2021, showed that incentives to invest properly in cybersecurity were still missing. The majority of operators of essential services and digital service providers acknowledged a significant positive impact of the NISD, particularly in detecting information security incidents. However, the implementation of the NISD did not necessarily result in substantial increases in the cybersecurity budgets of organisations. There is still much room for improvement here.

The agency organised and co-organised a number of exercises to test decision-making, internal communication and business continuity. These exercises go a long way in preparing to respond to cyberthreats and incidents, raising resilience and increasing preparedness across the EU.

In area of operational cooperation, ENISA continued to work closely with other European Union institutions, bodies and agencies (EUIBAs), and we were recently reminded by the regular Court of Auditors report that this is an area that needs closer attention. A new memorandum of understanding was signed with the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU) leveraging on the structured collaboration in accordance with the Cybersecurity Act. The annual plan included activities to further develop the Blueprint. ENISA and CERT-EU have aligned actions on developing EUIBA standard operating procedures and improving the Union's common situational awareness.

2021 also saw ENISA further its operational cooperation mandate by working with Member States to consolidate cyber situational awareness analyses with a focus on cyber incidents in the EU and also the impact of incidents from across the world on Europe. ENISA's cyber situational awareness services were provided to EUIBAs and authorities in Member States' authorities through regular weekly reports and ad hoc threat research. In the context of the Joint Cyber Unit initiative, ENISA organised a dedicated workshop to tackle the challenges in this area.

In relation to the EU cybersecurity certification framework, in 2021 ENISA prepared a candidate scheme on European common criteria (EUCC) for cybersecurity certification scheme. Once adopted, this will become the first EU scheme of its kind. In 2022 the candidate scheme on European cloud services will also be submitted following tough talks in the ENISA working group. Furthermore, an ad hoc working group began working in 2021 to prepare a candidate certification scheme for 5G networks. Finalising the candidate schemes for specialised product categories under the EUCC scheme and for cloud services is just the first step, and it is likely to bring about benefits in terms of recognition and trust across government services, business and citizens.

The publication of the 9th edition of ENISA's annual threat landscape report¹ confirmed current and future trends that cyberattacks are becoming ever more sophisticated, targeted, widespread, unattributable and detected too late. These continue to be global trends and their impact was felt in Europe as anywhere else. Cybercriminals are increasingly motivated by monetisation of their activities such as ransomware, the focus of the 9th ENISA threat landscape report. In addition, supply chain attacks of a highly sophisticated and impactful nature proliferated, as highlighted by the dedicated ENISA threat landscape on supply chains.

ENISA worked closely with the European Cybersecurity Competence Centre (ECCC) on the set-up phase and engaged in discussions with the centre in relation to joint administrative services. ENISA identified research and innovation needs and priorities in the field of life science cryptography, artificial intelligence and hyperconnectivity, with the goal of preparing future funding priorities for the ECCC. As a permanent observer on the governing board, ENISA played an active part in the activities of the Competence Centre. ENISA endeavoured to ensure that relevant synergies could be developed, and to provide relevant input during the preparation of the ECCC agenda, work programmes and multiannual work programme.

Russia's war in the Ukraine has once again made clear that ENISA cannot operate in an EU vacuum. That is why we equipped ourselves with an international strategy in late 2021 to offer more focused support to the Union when it comes to addressing countries outside the Union.

The Agency reorganisation initiated in 2020 took full effect in 2021. The new internal organisation was designed to be aligned with the requirements of the Cybersecurity Act and with the strategic objectives and priorities of the newly developed strategy. The new structure was meant to ensure more effective implementation of the tasks defined in our now permanent mandate to steadily move towards 'a trusted and cybersecure Europe'².

The Agency developed new key performance indicators and accompanying metrics during the reporting year, which served to improve the reporting of the 11 activities of the present annual activity report.

I am very proud to report that, thanks to the alignment of the Agency's structure with the Cybersecurity Act, I can see now how all staff members and associated parties of the Agency performed their tasks and exercised their related duties in a more coherent and coordinated manner, thus better serving the objectives of the Agency's mission. There is no doubt that a lot of work remains to be done and that fine-tuning will be needed

1 ENISA, ENISA Threat Landscape 2021 – April 2020 to mid-July 2021, 27 October 2021 (<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>).

2 ENISA strategy - <https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy>

over the coming years to adjust to our very fast-developing cybersecurity world and the inevitable challenges associated with it.

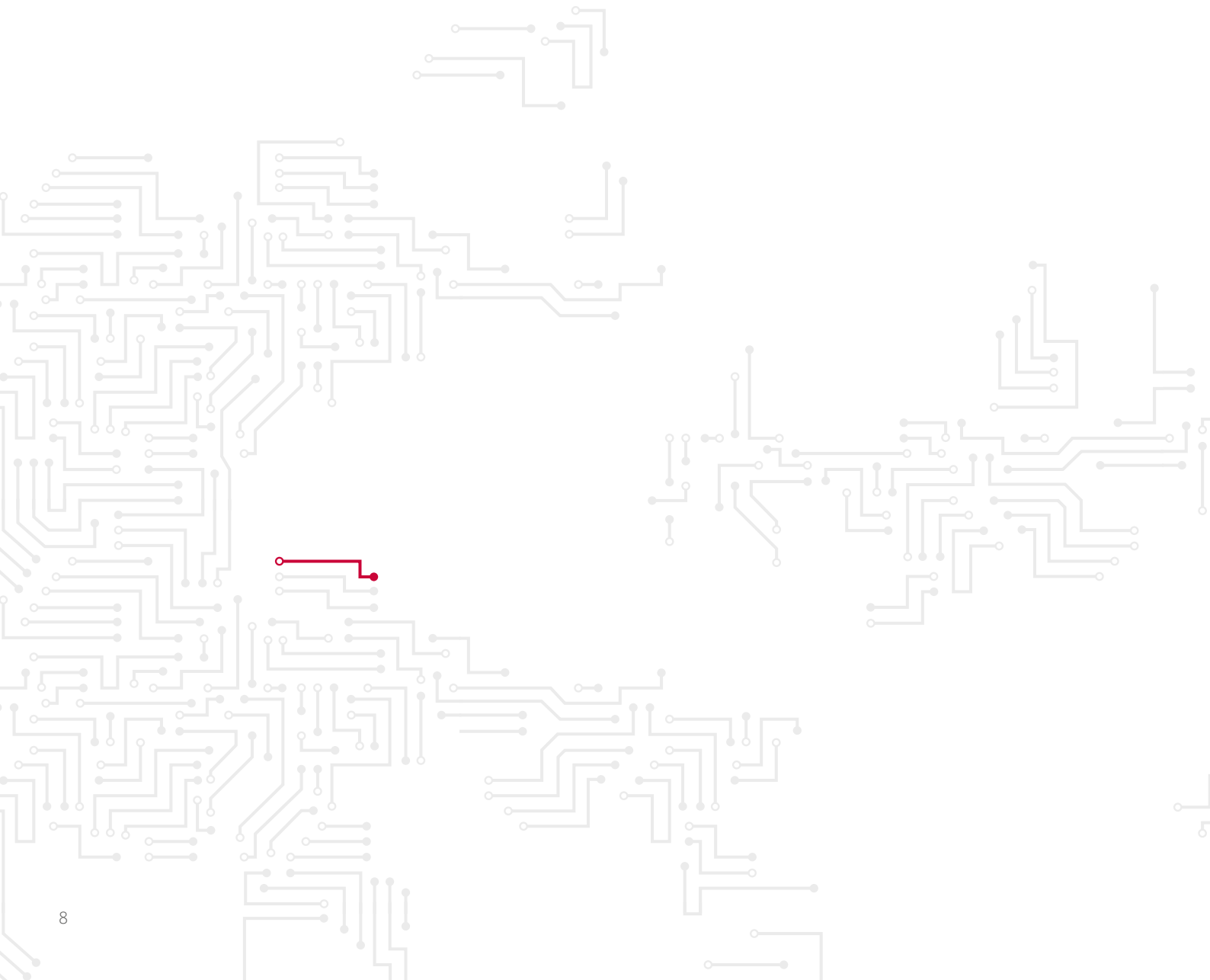
In the meantime, I see the success of the 2021 work programme as a testimony to the capacity of the new structure of the Agency to gather all the required synergies to deliver its mandate in the most effective way.

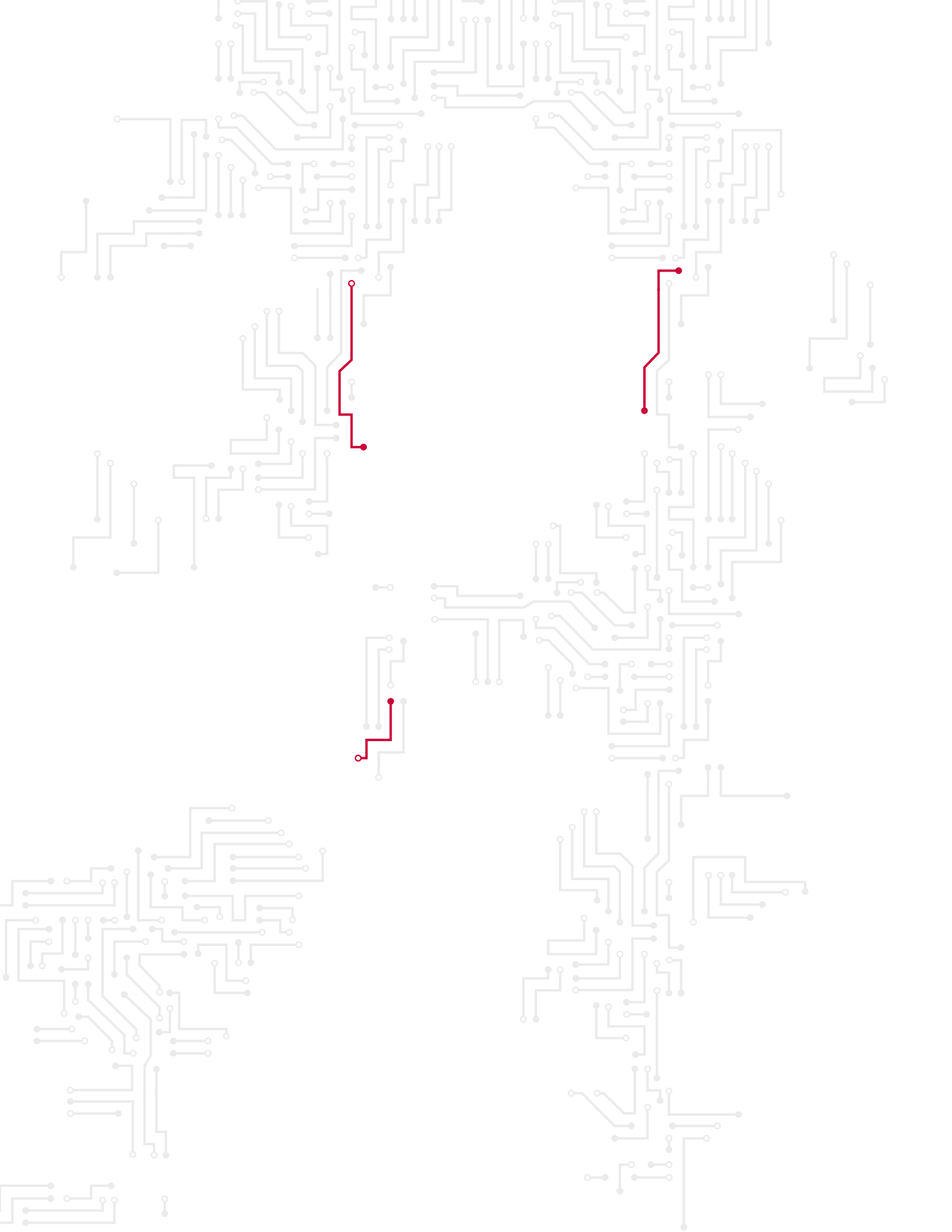
Thanks to the support of the Greek authorities, the Agency planned, prepared and moved to its new headquarters building in Chalandri, Athens, ensuring minimal disruption to its operations.

This is why I cannot be thankful enough to all our stakeholders who contributed to these endeavours in 2021 and without whom ENISA could not deliver its work and support the cybersecurity communities of the EU. I remain grateful for the ever so fruitful cooperation we enjoyed with our communities, with the European institutions and bodies, and, last but not least, with each Member State of the EU .

I also feel very grateful for the renewed commitment of ENISA's staff, including the 31 newcomers whom the agency welcomed in 2021. It is a great satisfaction to me to see how they continued to welcome and embrace our tasks and challenges in such a positive spirit. This is obviously the motivation we need to trigger if we want to successfully achieve our vision of a trusted and secure Europe.

Juhan Lepassaar
Executive Director, ENISA





ENISA MANAGEMENT BOARD ASSESSMENT

Analyses and assessment by the management board of ENISA of the Annual Activity Report for the year 2021 of the authorising officer of ENISA

The Management Board takes note of the consolidated Annual Activity Report (AAR) for the financial year 2021, submitted by the Executive Director of the European Union Agency for Cybersecurity (ENISA) in accordance with Article 48 of the Financial Regulation applicable to ENISA.

The Executive Board received a copy of the draft AAR 2021 produced by the Executive Director of ENISA in his role as Authorising Officer for the implementation of the annual budget on 11 May 2022 and the Management Board received a copy of the draft AAR 2021 on 2 June 2022.

The Management Board performed the analysis of the AAR and completed its assessment. The conclusions of the Management Board are the following:

The 2021 AAR represents the first full year when ENISA's new strategy (adopted by the Management Board in June 2020) and its renewed Work Programme were operational. In addition, structural changes were introduced in 2021 for the effective execution of ENISA's mandate and strategy. A new organisational structure was approved by the Management Board in 2020, effective as of the 1st January 2021.

The challenging circumstances around the COVID 19 pandemic continued well into 2021 that required the Agency to adjust its meetings to the online environment and continuation of 50% office / 50% teleworking arrangements for staff.

The Agency was able to meet the objectives set in the work programme 2021 as shown by the results presented in the report.

The AAR presents key results of the implementation of the ENISA work programme 2021 thus demonstrating how the Agency successfully completed all outputs as agreed with the Management Board in the work programme 2021.

ENISA involved stakeholder in the scoping and validation of all outputs in the work programme 2021, ensuring the added-value and take-up of ENISA deliverables by stakeholders, whether reports, tools, workshops or recommendations.

Newly formulated key performance indicators were reported in the AAR. These indicators provide quantitative and qualitative assessment of each of the operational and corporate activities and will be used as a baseline for future years.

Overall, the AAR is in line with the ENISA work programme 2021 and ENISA's work is well aligned with the overall European Union priorities for the Digital Single Market. A coherent link is provided

between activities planned in the work programme 2021 and the actual achievements reached in the reporting period.

The AAR also describes how ENISA managed its resources and presents the budget execution of the EU subsidy. In the course of 2021, the Agency has been operating with a budget of EUR 23.5 million equivalent to an 8% increase in 2021 compared to the 2020 budget (EUR 21.7 million)

During 2021, ENISA committed a total amount of EUR 22 721 149 representing 99.51 % of the total budget for the year. Payments made during the year amounted to EUR 17 672 344 representing 77.40% of the total budget. The execution of the budget has been high despite the restrictive circumstances imposed by COVID-19.

As compared to 2020, there has been a slight increase in the execution of commitments, 99.51% in 2021 as compared to 97.35% in the previous year, and an increase in the execution of payments, 77.40% as compared to 68.62% in 2020. The target of a 95% for commitment rate set by the Commission (DG Budget) was reached.

The turnover of staff was greatly reduced in 2021. The ratio was only 3% which shows improvement in retaining staff members in the Agency. Furthermore, a combined recruitment procedure organised in 2020 allowed the Agency to progress rapidly in fulfilling its establishment plan with 31 new recruits welcomed in 2021.

The AAR also provides information on the internal control assessment for 2021. This section notes the main categories of deviation that led to exceptions reported. In 2021 the Agency reported three exceptions in the AAR. None of these exceptions has a serious impact for the Agency.

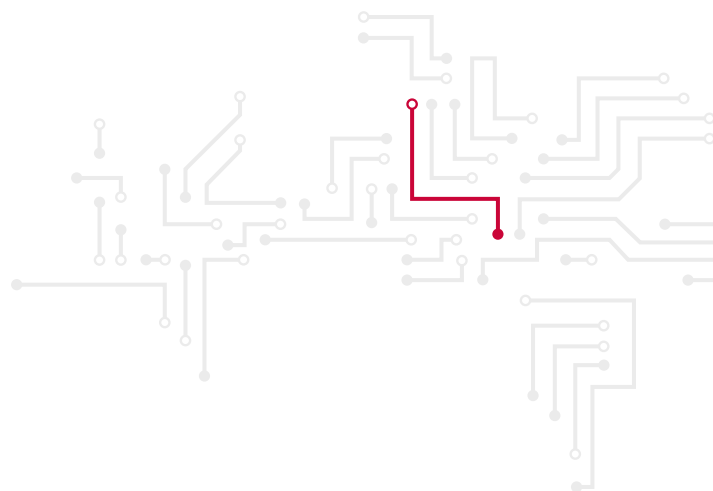
ENISA adopted the revised internal control framework at the end of 2019. The AAR 2021 shows the adequate management of risks, a high level of transparency, clear governance structures and improved performance monitoring.

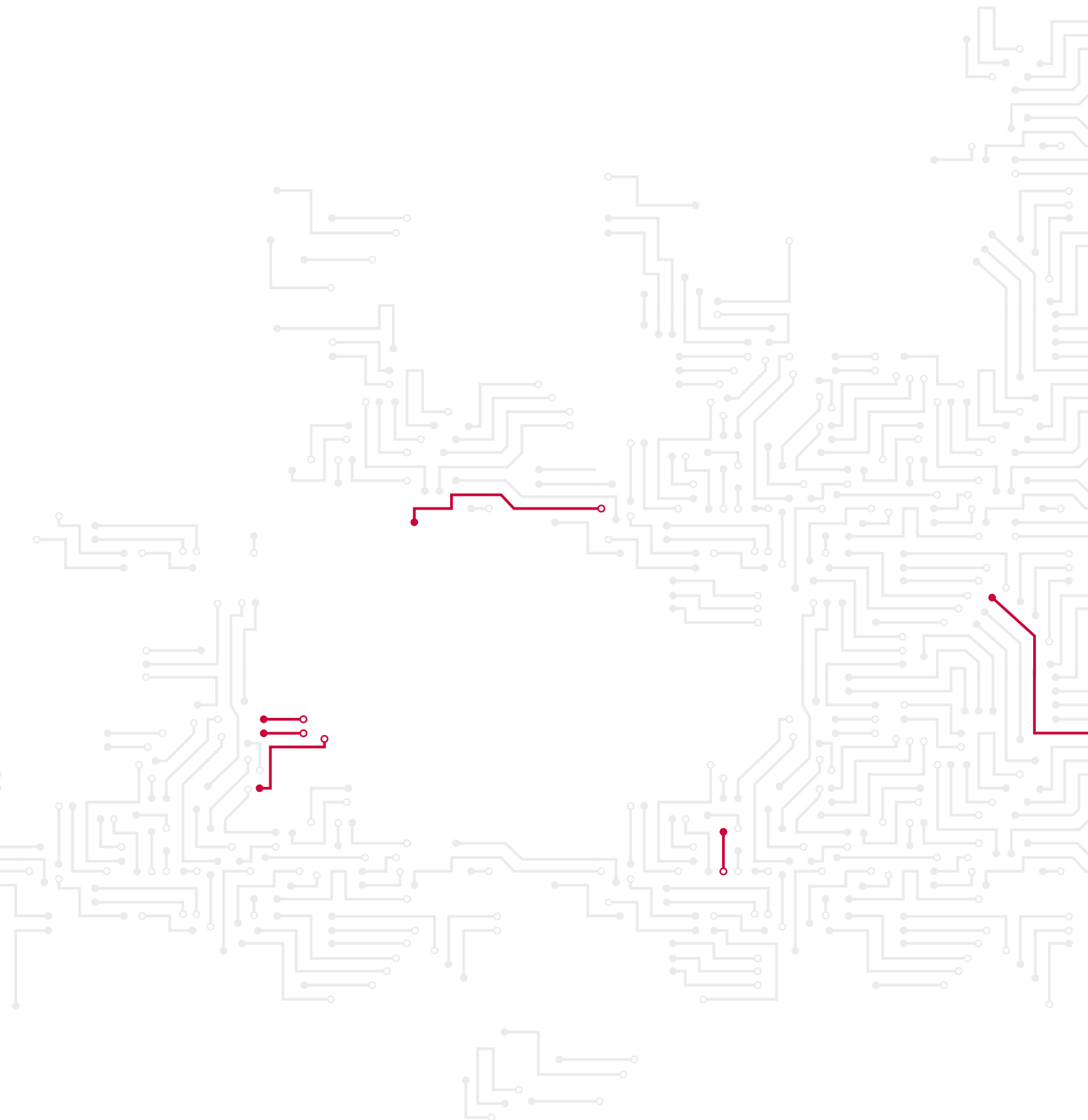
The Management Board notes that infringement of the use of delegation powers and weaknesses in internal controls framework were identified by the European Court Auditors. The Board concludes that necessary actions were undertaken within 2021 to improve the overall efficiency of the Agency in abiding to its principles and congratulates ENISA for all the efforts engaged to that end.

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 2021. The Management Board notes with satisfaction that ENISA was able to deliver the work programme 2021 despite the continued conditions due to COVID -19 showing exceptional flexibility and efficiency in challenging circumstances. The Management Board expresses its deep appreciation to the Executive Director and his staff for their commitment and the excellent performance throughout the year.

In light of the above assessment, the Management Board requests the Management Board Secretariat to forward the AAR, together with this assessment, to the European Commission, the European Parliament, the Council, the Permanent Representations of the Member States and the Court of Auditors.





EXECUTIVE SUMMARY

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

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 Cybersecurity Act (CSA) has now been implemented for two years since it came into force in 2019. 2020 was the first full year the Agency functioned under the new organisation structure which aligns with the new mandate and the newly formed strategy.

The task assigned to ENISA under this regulation is to achieve a high common level of cybersecurity across the Union, including actively supporting Member States, and Union institutions, bodies, offices and agencies, in improving cybersecurity.

In the area of policy ENISA supported the development of new policy files such as the revised Network and Information Security directive (NIS2), the Digital Operational Resilience Act (DORA), electronic identification, authentication and trust services (eIDAS), the European Electronic Communications Code, 5G, digital wallets, artificial intelligence (AI) and the Network Code on cyber security (NCCS). ENISA's work in these areas delivers evidence to inform future policy decisions with a view to strengthening the EU policy and regulatory framework to address cybersecurity challenges.

ENISA continued its efforts in supporting Member States with technical aspects related to Directive (EU) 2016/1148 (the network and information security directive (NISD)), security of electronic communications, data protection, privacy, electronic identification, trust services, incident reporting and vulnerability disclosure policies. It continued its support of established groups, such as the NIS Cooperation Group, its work streams, European Competent Authorities for Security of Electronic Communications Group and the ENISA eIDAS regulation Article 19 expert group. A key highlight is the support ENISA provided in relation to the review of the NISD and the proposal for new sectors. Furthermore, ENISA contributed to the ongoing development of additional policy files, such as on DORA, AI and Network Code on cyber security (NCCS).

In 2021, ENISA contributed to the improvement of capabilities of Member States and EU institutions, bodies and agencies (EUIBAs), raising resilience and increasing preparedness across the EU. Capacity across the Union was built by the organisation and the setting up of several exercises, including Cyber Europe, the Blueprint Operational Level Exercise and CyberSOPEX, as well as in-depth training and accompanying tabletop exercises in support of the maturity and skills of computer security incident response teams (CSIRTs) and other communities. In addition, the Agency assisted Member States in measuring the maturity level of national cybersecurity strategies by developing an online tool to assist Member States to perform a self-assessment exercise with the aim of improving national cybersecurity capabilities by conducting an evaluation of their national cybersecurity capabilities, enhancing awareness of the country's maturity level and identifying areas for improvement in building cybersecurity capabilities.

During 2021, ENISA supported and coordinated a number of networks and technical/operational communities. ENISA supported the activities of the CSIRTs Network in implementing the network's work programme for 2021, and aided the networks during high-profile incidents that required escalation, such as during the Member States exchange Log4j vulnerability. ENISA actively supported the newly established Cyber Crisis Liaison Network (CyCLONE) by carrying out activities designed to improve information sharing and operational cooperation, in particular regarding automated reporting, impact assessment and situational awareness. ENISA also engaged in the initial activities related to the proposal for a Joint Cyber Unit by contributing to and organising several workshops. All these activities helped to identify best practices, challenges and opportunities with a view to improving operational cooperation, situational awareness and coordination for incident response in the EU.

Moreover, ENISA contributed to the development of effective operational cooperation among Member States and EUIBAs by generating and consolidating information (including from the general public) on cyber situational awareness, technical situational reports (threat reports), incident reports and threats. ENISA also actively supported the consolidation and exchange of information on strategic, tactical and technical levels to operational communities, such as the CSIRTs Network and CyCLONE.

In the area of certification, ENISA had made meaningful contributions to the EU cybersecurity certification framework; it had shifted from one

mature scheme to two and it had a third one in the works. ENISA started populating the cybersecurity market analysis area, and redirected standardisation to fit its dual purpose across cybersecurity policy and cybersecurity certification, while developing its relationship with European standardisation organisations yet further. ENISA assisted the Commission with regard to cybersecurity certification bodies – the European Cybersecurity Certification Group (ECCG) and Stakeholder Cybersecurity Certification Group – and continued developing its capability to service the Commission and the Member States on cybersecurity certification by producing guidance on the candidate cybersecurity certification scheme on European common criteria (EUCC) for which the ECCG gave a favourable opinion.

On the basis of an open consultation, the draft candidate cybersecurity certification scheme on European cloud services (EUCCS) was reprocessed and to a great extent finalised. Gradually, the interest in EUCCS shifted towards data localisation and aspects of digital sovereignty. ENISA processed a request for a scheme on 5G certification, which was successfully launched following thorough consultation with stakeholders.

Kicking off a new area, ENISA prepared a cybersecurity market analysis framework and a targeted analysis of the market for connected devices in energy. In terms of standardisation, ENISA launched specific requests to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC), and provided guidance on 5G standards and related organisations and on risk management.

ENISA worked on various fronts in terms of consolidating information, analysing it, and providing analyses and recommendations to serve stakeholders' expectations. Most notable examples of ENISA's efforts in the area of knowledge on emerging cybersecurity challenges include designing the EU cybersecurity index, publishing the annual threat landscape and the supply chain attacks threat landscape and in particular supporting the European Cybersecurity Competence Centre, by identifying the priorities in research and innovation priorities.

Behavioural change is the cornerstone of cybersecurity awareness and education, and requires persistent long-term effort, well-defined objectives, identified target groups, and particularly specific and relevant metrics and indicators for measuring change. Given this, in 2021 ENISA laid the groundwork for all the awareness activities to

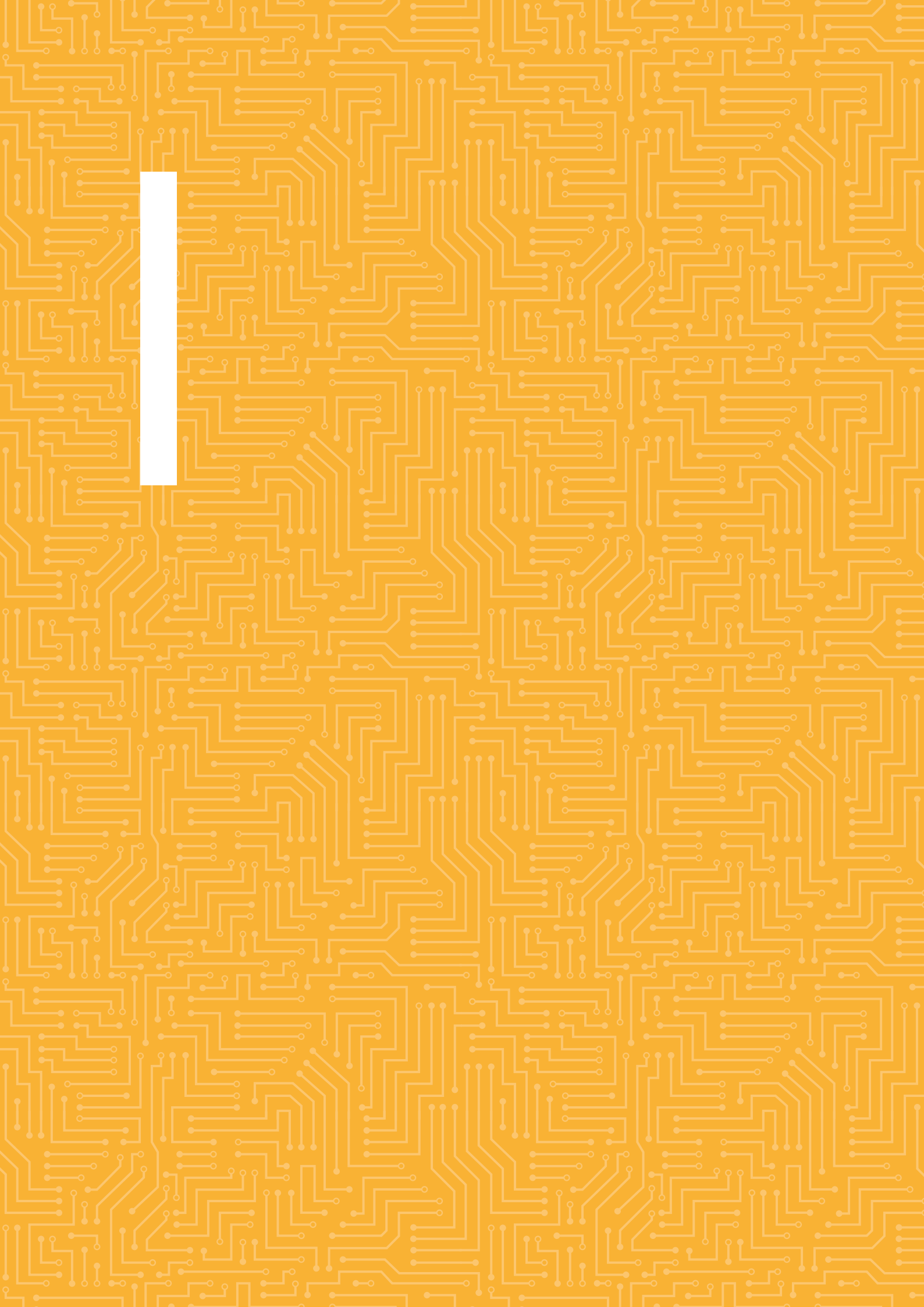
be undertaken by the Agency in the coming years: specifically, the development of a stakeholder strategy; an awareness-raising framework, with a set of processes and requirements for organising an awareness-raising campaign; and finally a promotion and dissemination strategy, presenting the most effective means and channels to use for different target audiences.

A number of structural changes were introduced in 2021 for the effective execution of ENISA's mandate and strategy. A new organisational structure was approved by the Management Board in 2020, effective as of 1 January 2021. The new organisational structure aligns the tasks and functions of the Agency's structural set-up with the CSA, and ensures that all entities and all staff members of the Agency exercise their tasks and obligations in line with the Agency's mission and values, striving to reach and maintain the highest level of openness, transparency and ethical standards.

The management team was established to assist the Executive Director in his functions, ensuring that activities undertaken by the Agency under its work programme add value for the Union and are planned and implemented in a coordinated fashion. A total of six units were established: four operational units tasked with Articles 5–7 of the CSA, and two corporate units responsible for the administrative functions. In addition, four teams were established, tasked with Articles 8–12 and 42 of the CSA.

Two new committees were established in 2021 to help the Agency carry out its tasks. The Budget Management Committee ensures the coherent planning, implementation and follow-up of the Agency's budget, and the Information Technology Management Committee ensures the comprehensive and coordinated management of the Agency's information technology systems and services required to fulfil its core tasks.

Lastly, the Agency, with the agreement of the Greek authorities, moved into new premises in Athens in order to meet the growing needs of the Agency, and a local office in Brussels was established to support the implementation of structured cooperation with Union institutions.



PART I

ACHIEVEMENTS OF THE YEAR

The following sections of the Annual Activity Report are based on the structure of the European Union Agency for Cybersecurity (ENISA) Programming Document 2021–2023. The achievements of each activity are described, including details of the outcome of each output undertaken during the course of 2021.

ACTIVITY 1

Providing assistance on policy development



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, by collecting evidence to support the effectiveness of the existing policy framework and by providing EU policymakers and stakeholders with policy recommendations on future cybersecurity challenges and opportunities.

Achievements

ENISA actively contributed to 26 task forces and bodies, 161 workshops and conferences, and 6 European Commission and Member State initiatives in response to requests. The budget allocated to this activity went almost entirely into activities related to the collection of evidence for assessing existing policies or developing new ones, including expanding the network and information security (NIS) investments report to cover all 27 EU Member States. The Agency also participated in public hearings organised by the European Parliament and followed up the dialogues. This is how the agency 'ensured that EU policymakers are regularly informed about the effectiveness of the existing frameworks and provided with timely and tailor-made policy recommendations'. Activities related to the analysis and interpretation of the evidence itself were performed using internal resources. The development of internal capabilities and skillsets to perform such analyses is under way and will be the focus of the years to come.

The Agency developed internal positions, in cooperation with other teams and units, to support the relevant competent authorities of the Commission and Member States (e.g. on supply chains and on the security requirements of new sectors under the proposed revised network and information security directive (NISD2)), the European Parliament and Council of the European Union with targeted policy analysis and reports.

ENISA developed targeted products and services (e.g. the NIS investments report) following an evidence-based approach in order to 'regularly inform EU policymakers about the effectiveness of the existing framework'. In this context, the Agency established the EU Cybersecurity Policy Observatory (CSPO) as an internal function to support evidence-based policymaking and inform policymakers through the provision of relevant evidence and expert advice. The EU CSPO will help the Agency to contribute efficiently to an increasing number of cybersecurity EU policies.

Strategic cooperation

ENISA maintained and even further developed strategic relationships and cooperation with a number of directorates-general. Examples include the support given by ENISA to the Directorate-General for Communications Networks, Content and Technology (DG Connect) and to the European Parliament with regard to NISD2 negotiations, its support to the European Insurance and Occupational Pensions Authority and the European Banking Authority in preparation for the Digital Operational Resilience Act (DORA) legislation, and its support to the European Union Agency for the Cooperation of Energy Regulators (ACER) for the development of the Network CODE on cyber security (NCCS).

The work of ENISA during the reporting period offered insights into aspects of the impact of policy that so far had not been visible to the EU or to national policymakers in the EU. The NIS investments report is a good example of a maturing product, as it provides the concrete evidence needed to support the evaluation of the impact of Directive (EU) 2016/1148 (the network and information security directive (NISD)) on the cybersecurity of operators of essential services (OESs) / digital service providers (DSPs), and allows the identification of potential gaps and opportunities. When moving from horizontal policy and regulatory instruments, such as the NISD, and into sectoral analyses, the positive impact of the Agency's activities had been limited by the fragmentation of the policy responsibilities of the competent authorities of the Member States on cybersecurity matters. In order to address this issue, ENISA closely engaged with the European Commission and the Member States, and still does so to facilitate the development of appropriate forums and interfaces to support sector-focused discussions.

ENISA was able to deliver opinions and written contributions on all topics identified by the Commission as priorities. A key highlight of this activity is the support ENISA provided in relation to the review of the NISD and the proposal for new sectors.

Resources

ENISA's ability to support different stages of the policy development life cycle is currently limited by a lack of available human resources (HR) and a lack of relevant skills. There is a proliferation of sectoral or thematic policy initiatives that include cybersecurity requirements as part of a broader policy intervention, but the Agency does not necessarily have the resources to follow up all of them. The EU cybersecurity observatory (CSPO) could provide a framework for prioritisation and improved resource allocation, which would partly address the problem of limited HR and pertinent skills.

Overall assessment

The outputs of this activity are relevant and timely but require prioritisation from the Agency to best adapt them to the available resources. With NISD2 bringing ever more sectors under the scope of the directive, it is also essential that the policy frameworks of these sectors take account of cybersecurity aspects. However, the Agency will never have sufficient resources to monitor and offer advice on each sector separately. Thus, the EU CSPO is the concept to be applied to achieve this objective as the number of EU policies increase. The implementation of the EU CSPO and its synergy with the foresight capabilities currently being developed within the Agency are expected to enhance ENISA's advisory capabilities on emerging areas. It will also allow the Agency to bring emerging/future topics of interest to the attention of EU policymakers and stakeholders. Through this process, areas and topics not currently part of the policy agenda can be thoroughly assessed at EU level in order to identify in advance potential needs for policy intervention. The activity could benefit from having additional experts familiar with the EU policy development life cycle, but also from having additional budget to further deploy professional market intelligence in support of the CSPO.

The three outputs of the activity are relevant, as they meet the objectives of the activity and of the relevant strategic objective with a minor change in the scope of output 1.3, which should be policy independent and also allow for the development of a registry of EU cybersecurity policies. 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 such an endeavour. Instead, the Agency proposes to focus the metric on the EU level only and to extend the scope to include reports to which the Agency contributed (e.g. reports of the NIS Cooperation Group).

Objectives



- Foster cybersecurity as an integral part of EU policy (existing and new)
- Regularly inform EU policymakers about the effectiveness of the existing framework
- Provide EU policymakers and stakeholders 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

Results



- Where relevant, support the European Commission in ensuring that EU and national policies take cybersecurity aspects into account

Outputs



- 1.1. Issue reports, studies and analyses on the effectiveness of the current cybersecurity policy framework in requested areas and according to the relevant best practices

Outcome



- ENISA published the second NIS investments report, providing policymakers with insights into the cybersecurity budgets of OESs and DSPs and how these budgets were influenced by the NISD, in order to inform future policy decisions.
- 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.
- The Agency supported ACER by providing guidance on the framework guidelines for the network code on the cybersecurity of cross-border electricity flows.
- ENISA contributed to the development of the Network CODE on cyber security (NCCS) by participating in the drafting team. In this context, ENISA organised a workshop in Athens in September for the technical subgroup on information sharing.

The NIS investments report is available online (<https://www.enisa.europa.eu/publications/nis-investments-2021>).

The output achieved its objectives in 2021. Its scope remains timely and relevant. Based on ENISA's assessment, it should remain in the 2023 single programming document (SPD).

- 1.2. Support the European Commission and Member States by providing tailor-made advice and recommendations on new policy initiatives that tackle emerging technological, societal and economic trends

- ENISA continued supporting the European Commission and the European Parliament with regard to NISD2 negotiations by:
 - providing technical expertise through written contributions on supply chains and on the security requirements of new sector under NISD2;
 - participating in several ad hoc meetings and delivering technical briefings.
- In the area of artificial intelligence (AI), ENISA:
 - supported the European Commission and Member States by contributing to the public consultation on AI proposal for a regulation, organising regular meetings and contributing to the activities of the competent authorities for AI Member State-driven working group;
 - collected and analysed data on AI cybersecurity strategies and policies.
- ENISA provided support to the European Commission and the Directorate-General for Financial Stability, Financial Services and Capital Markets in relation to the legislation for DORA for the financial sector. ENISA supported the European Insurance and Occupational Pensions Authority and the European Banking Authority on harmonisation of incident reporting in preparation for the DORA legislation.

- ENISA participated in the European Strategic Coordination Platform with the objective of preparing the proposal for the regulation of the European Union Aviation Safety Agency, and provided written contributions on the acceptable means of compliance and guidance material, which defines the details of the sectoral policy.
- ENISA established the EU CSPO, which aims to support the European Commission and Member States in different stages of the policy life cycle through services focused on evidence-based policymaking and systematic cybersecurity policy observation.

The output achieved its objectives in 2021. Its scope remains timely and relevant. Based on ENISA's assessment, it should remain in the 2023 SPD.

1.3. Assist the Commission in reviewing the NIS directive

- ENISA supported the consultations on the NISD proposal by providing written contributions to the European Commission and by organising meetings with it. In this context, the Agency prepared two technical reports – one on the new sectors' security requirements in NISD2 and the other on good practices in supply chains – and engaged in more than 15 virtual meetings with the Commission and representatives of the European Parliament.

The output achieved its objectives in 2021. Its scope remains timely and relevant, but it must be policy independent and also allow for the development of a registry of EU cybersecurity policies. With this change, the output should be included in the 2023 SPD.

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	Results
1.1. Number of relevant contributions to EU and national policies and legislative initiatives	Number	Annual	Manual collection from staff members	193
Contributions to task forces and bodies	%	Annual	Manual collection from staff members	13 %
Contributions to workshops and conferences	%	Annual	Manual collection from staff members	83 %
Support actions/contributions to European Commission and Member States for policies and legal initiatives following relevant requests	%	Annual	Manual collection from staff members	4 %
1.2. Number of references to ENISA reports, analysis and/or studies in EU and national policy documents		Biennial	Survey	N/A
1.3. Satisfaction with ENISA's added value and weight of contributions		Biennial	Survey	N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	6	Actual used FTEs		Actual: 4.43
Planned budget (direct costs only)	EUR 280 000	Consumed budget (direct costs only)		EUR 319 585
		Of which carried over to 2022		EUR 0

FTE, full-time equivalent; N/A, not applicable.

ACTIVITY 2

Supporting implementation of Union policy and law



In this activity ENISA continued its efforts to align horizontal cybersecurity policies with sectoral policies to avoid inconsistencies in implementation, and contributed to the efficient and effective monitoring of the implementation of EU cybersecurity policy in Member States. The agency contributed to the effective implementation of cybersecurity policy across the EU, and to the approximation of Member State laws, regulations and administrative provisions related to cybersecurity.

Achievements

The coordination and prioritisation of the Agency's work based on available resources had a positive impact, as it benefited from regular interactions with established groups and EU bodies such as DG Connect, the Directorate-General for Energy, the Body of European Regulators for Electronic Communications, the NIS Cooperation Group (CG), ACER, the European Union Agency for Railways (ERA), the European Data Protection Supervisor (EDPS) and the European Data Protection Board. Prominent examples in support of the relevant strategic objectives include:

- providing support to 10 active work streams of the NISD Cooperation Group to help them meet their objectives, contributing to the development of targeted reports on emerging issues (e.g. open radio access network (O-RAN), top-level domain registry operators, domain name system (DNS) resolvers, coordinated vulnerability disclosure policies) and organising knowledge-building seminars, thus contributing 'to the effective implementation of cybersecurity policy across the EU and approximation of Member State laws, regulations and administrative provisions related to cybersecurity' (SPD Activity 2 objective);
- strengthening its sectoral approach to NISD implementation by developing vertical sectoral products (e.g. a railway sector threat landscape, the Maritime Sector Risk Management Tool, the 5G matrix and an energy threat landscape), building strategic relationships between horizontal and sectoral stakeholders, linking operational cooperation and capacity building, and engaging with sectoral information-sharing and analysis centres (ISACs) to 'Align horizontal cybersecurity policies with sectoral policies and avoid implementation inconsistencies' (SPD Activity 2 objective);
- building on the 5G toolbox with the development of a 5G control matrix, pursuing a leading role in the establishment of the EU digital wallet toolbox, following Recommendation (EU) 2021/946 and thus contributing 'to the effective implementation of cybersecurity policy across the EU' (SPD Activity 2 objective);
- developing several focused publications targeting the needs of stakeholders to help them implement particular policy aspects (e.g. SIM swapping, DNS resolvers, data protection engineering) and also events that brought together stakeholders to discuss good policy options, such as the 1st ENISA Telecom Security Forum and the 7th ENISA Trust Services Forum;
- supporting incident notification processes in accordance with Article 5(6) of the Cybersecurity Act (CSA), for incident reporting under the European Electronic Communications Code (EECC), Regulation (EU) 910/2014 (the eIDAS regulation) and the NISD, delivering three annual EU-wide incident reports, and a prototype for a consolidated EU incident-reporting dashboard.

Resources

The available human and budgetary resources were divided between performing analyses of technical aspects on validated priority areas, promoting good practices, engaging relevant communities and providing support to formally established groups and bodies, such as the NIS CG. The NIS CG work programme reached a high maturity level with 10 active work streams, meaning that the Agency had to prioritise, taking into account political priorities and emerging legislative portfolios such as the EU digital wallet toolbox.

Policy development and implementation tasks cannot be easily outsourced or subcontracted. They require analytical skills of senior experts of the Agency. It is a major challenge for the Agency to recruit and retain

talented senior cybersecurity experts combining holistic policy expertise with technical expertise to support the technical aspects of the implementation of cybersecurity policy.

In addition, the implementation of the NISD2 proposal, as well as important sectoral initiatives (e.g. DORA, Network CODE on cyber security (NCCS), and the Aviation horizontal rule), will require a lot of resources in the coming years to address the new tasks and also to cover all the new critical sectors and sustain the existing ones.

Overall assessment

Currently, the sectoral cybersecurity policy development and implementation activities across the Union are often unaligned and, thus, fragmented. A more holistic approach is required to align sectoral with horizontal policies, to avoid inconsistencies, gaps, barriers and inefficiencies. However, the more sectoral initiatives emerge, the greater the expectations are on ENISA's contribution and engagement, thus creating resource constraints on meeting these expectations. This means there is a need for prioritisation that would take into consideration factors such as the maturity of the sectors trends in technology, criticality, recent incidents and emerging threats. During the reporting year, ENISA worked on developing an NIS strategy intended to streamline its services into standard packages for the NIS sectors, and target the different NIS sectors following a careful assessment of sectoral needs and requirements.

Furthermore, an important opportunity lies in connecting the development and implementation of sectoral cybersecurity policy with operational cooperation and capacity building. The experience of 2021 shows how lessons learned in operational cooperation can feed into policy development and implementation as well as capacity building to result in better and more targeted actions. This means that the agency will seek synergies and align the work under Activities 1 and 2 with the work under Activities 3, 4 and 5 in the ENISA SPD. To achieve the intended results, the Agency will prioritise its efforts and properly utilise its existing resources properly by developing an NIS strategy that will partly address the problem. Still, additional resources will be needed in the near future to deal with the new tasks under NISD2 as well as sectoral policy initiatives (e.g. DORA and Network CODE on cyber security (NCCS)). Seconded national experts can actually be one of the possible solutions to address this problem because of their great experience with the implementation of national policy.

The outputs of the activity are relevant and timely; however, incident reporting (output 2.5 'Analyse and report on incidents as required by Article 5(6) of the CSA on incident reporting') was transferred to Activity 8 in the 2022 SPD to reinforce synergies with the outputs on foresight.

The four outputs of the activity will require additional rescoping to meet the needs of NISD2 and upcoming sectoral regulations, and the work related to telecommunications should be merged into a single output. In addition, sectoral work could be decoupled from the horizontal NISD implementation work to allow for greater focus. The relevance and importance of vulnerability disclosure policies should also be examined in the coming years.

The existing KPIs are valid and relevant, and should be reviewed in the coming years.

Objectives



- Align horizontal cybersecurity policies with sectoral policies to avoid inconsistencies in implementation
- Contribute to the efficient and effective monitoring of the implementation of EU cybersecurity policy in Member States
- Contribute to the effective implementation of cybersecurity policy across the EU and approximation of Member State laws, regulations and administrative provisions related to cybersecurity
- Improve cybersecurity practices taking on board lesson 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 EU policy and law in the area of cybersecurity
- EU cybersecurity policy implementation reflecting sectoral specificities and needs
- Exchange of good practice

Outputs



2.1. Support the NIS Cooperation Group and sectoral work streams in accordance with the NIS CG work programme

Outcome



- ENISA continued supporting the work of the NIS CG work streams, promoting dialogue on supply chain security and relevant security measures.
- ENISA supported cross-border collaboration on incidents experienced by digital service providers by piloting the ENISA Cybersecurity Incident Reporting and Analysis tool.
- The Agency analysed data and developed energy threat reports every two months.
- ENISA developed and organised sessions on cybersecurity topics for the energy sector.
- ENISA developed Member State guidelines on security measures for top-level domain registry operators.
- The Agency took stock, analysed data and drafted reports on security measures and incident reporting for the health sector.
- ENISA assisted with the organisation of events and carried out technical analysis in support of the work streams.
- The Agency researched the security and privacy of public DNS resolvers, providing insights into the effects of the use of encrypted DNS protocols and into drivers for the shift away from traditional DNS resolvers (<https://www.enisa.europa.eu/publications/security-and-privacy-for-public-dns-resolvers>).

The output achieved its objectives in 2021. Based on lessons learned, it is proposed that the scope of this output should change to focus only on horizontal matters of the implementation of the NISD and NISD2. The sectoral policy implementation part should thus be part of a new, dedicated output.

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

- ENISA continued supporting the 5G toolbox by producing a prototype version of the '5G Security Controls Matrix' including detailed security controls, descriptions of evidence and standard references. The implementation is supported by a pilot run with national regulatory authorities and mobile network operators.
- ENISA explored the security challenges of network function virtualisation in 5G networks and identified relevant best practices (<https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices>).

- The Agency supported Member States on 5G security by organising two 5G security knowledge-building seminars for the NIS CG.
- The Agency explored the security challenges and benefits of O-RAN, analysing technical risk scenarios and providing concrete recommendations for updates to the Member States' analysis.
- ENISA supported DG Connect in reviewing the progress made in each Member State in relation to the 5G toolbox implementation, while providing suggestions on improving the questionnaire.

The output achieved its objectives in 2021. Based on the lessons learned, it is proposed that the output should merge with the part of output 2.3 that deals with the European Electronic Communications Code to constitute a single integrated output on telecom security and 5G.

2.3. Recommendations, technical guidelines and other activities to assist with and support the implementation of policies within the NISD sectors, in the area of trust services and electronic identification, under the European Electronic Communications Code and its implementing acts, and in the field of privacy and data protection and artificial intelligence

- ENISA continued the collection and analysis of data on a capability maturity framework for the EU energy sector, providing useful insights for the participants in the study.
- ENISA supported port operators in conducting cyberrisk management by publishing an online tool that helps them identify security measures more easily based on their priorities.
- In close collaboration with ERA, ENISA proposed a number of good practices to follow to identify and manage the cyberrisk in the railway sector (<https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management>).
- ENISA and ERA joined forces and organised a conference on cybersecurity in railways.
- ENISA organised the first ENISA Telecom Security Forum, bringing together stakeholders from public and private sectors to debate on emerging issues related to telecom security across Europe.
- ENISA continued supporting the work of the European Competent Authorities for Security of Electronic Communications (ECASEC) Group of telecom security authorities. The group had three plenary meetings during 2021 and participated in webinars on mobile network security topics organised by ENISA.
- In collaboration with the ECASEC Group, ENISA analysed fraudulent SIM swapping, giving an overview of how SIM-swapping attacks work, the frequency and impact of these attacks in Europe, and a set of good practices to mitigate them.
- The Agency supported the ECASEC Group in exploring consumer outreach concerning cybersecurity threats telecom providers, providing an overview of the current practices in relation to how providers notify users of threats, and a framework to help assess the necessity to carry out such outreach activities.
- In collaboration with the ECASEC Group, ENISA analysed security incidents affecting confidentiality, integrity and authenticity in public electronic communications networks, focusing on those attacks that target individual subscribers.
- ENISA continued supporting technical aspects of implementing the general data protection regulation (Regulation (EU) 2016/679) and worked on analysing data protection engineering technologies and

techniques in addition to promoting pseudonymisation techniques in the healthcare sector (<https://www.enisa.europa.eu/publications/data-protection-engineering>, <https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques>).

- ENISA co-organised with DG Connect the 9th Annual Privacy Forum and hosted discussions on emerging legislative portfolios, including the ePrivacy regulation proposal. In parallel, ENISA pursued an active collaboration with the European Data Protection Board and the EDPS.
- ENISA continued supporting the European Commission and Member States in providing recommendations and technical guidelines in the area of trust services and electronic identification. The emerging topic of digital identification was the focus of two new reports: an analysis of self-sovereign identity and a study of major face presentation attacks (<https://www.enisa.europa.eu/news/enisa-news/beware-of-digital-id-attacks-your-face-can-be-spoofed>). Moreover, a workshop on 'Remote identity proofing: attacks and countermeasures' was organised.
- In collaboration with the European Commission, ENISA organised the 7th Trust Services Forum and hosted discussions on emerging topics such as digital wallets; certification and standardisation in EU digital identities; and the trust services market.
- ENISA continued supporting the work of the ENISA Article 19 EG of eIDAS supervisory bodies, holding three virtual meetings, a workshop on blockchain security and a training course on cloud security.
- ENISA supported the European Commission on the toolbox process for a coordinated approach towards a European digital identity framework and contributed to the security analysis of digital wallets.

The output achieved its objectives in 2021. Based on the lessons learned, it is proposed that the scope of this output should not include the EECC but rather the EECC should be merged with output 2.2 (see assessment above).

2.4. Assist in establishing and implementing vulnerability disclosure policies

- ENISA took stock of the national coordinated vulnerability disclosure (CVD) policies in the EU, publishing a detailed map of the different policies in the EU, and providing an overview of risks, challenges and good practices for the development of CVD policies.
- ENISA supported the exchange of good practices between Member States by organising a workshop for authorities about coordinated vulnerability disclosure policies and initiatives.

The output achieved its objectives in 2021. Based on the lessons learned, its scope should exclude the EU CVD database, which should be part of Activity 4.

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

- ENISA prepared three annual reports concerning incidents reported under the NISD (Article 10(3)), the eIDAS Regulation (Article 19) and the EECC (Article 40).
- ENISA published the 2020 annual report on incident notification by trust service providers: (<https://www.enisa.europa.eu/publications/trust-services-security-incident-2020-annual-report>) and the 2020 annual report on telecom security incidents (<https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020>), while the 2020 annual incident notification report concerning NISD incidents was published by the Commission, as an NIS CG document.

The output achieved its objectives in 2021. Based on the lessons learned, during 2021 this output was moved to Activity 8 in the 2022 SPD.

Key performance indicators Contribution to policy implementation and implementation monitoring at EU and national levels (<i>ex-post</i>)	Unit of measurement	Frequency	Data source	Results
2.1. Number of EU policies and regulations implemented at national level supported by ENISA	Number	Annual	Manual collection from staff members	5
NISD	Number	Annual	Manual collection from staff members	1
EECC	Number	Annual	Manual collection from staff members	1
eIDAS	Number	Annual	Manual collection from staff members	1
5G	Number	Annual	Manual collection from staff members	1
Network CODE on cyber security (NCCS).	Number	Annual	Manual collection from staff members	1
2.2. Number of ENISA reports, analyses and/or studies referred to at EU and national levels	Biennial	Survey	N/A	N/A
2.3. Satisfaction with ENISA's added value and weight of support	Biennial	Survey	N/A	N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	14	Actual used FTEs		Actual: 10.16
Planned budget (direct costs only)	EUR 985 000	Consumed budget (direct costs only)		EUR 934 463
		Of which carried over to 2022		EUR 22 098

N/A, not applicable.

ACTIVITY 3

Building capacity



In 2021, ENISA contributed to the improvement of the capabilities of Member States and EUIBAs, as well as various sectors.

Achievements

The Agency assisted Member States in measuring the maturity level of national cybersecurity strategies (NCSSs) through the deployment of an online tool that was developed with contributions from 20 Member States and is already being considered for use by six Member States. This has provided the basis for the creation of the cybersecurity index quantitative KPIs.

In parallel, significant effort was devoted to the preparation of the new strategy for exercises and training as a result of the CSA. In this context, the preparatory work was carried out for the required switch to the new Cyber Exercise Platform, which is better suited to supporting the objectives set in the new strategy.

In 2021, ENISA was confronted with the challenges brought about by the pandemic, which affected capacity-building activities at multiple levels. On the one hand, a number of courses and exercises had to be converted for online delivery, for obvious reasons. This change posed a number of challenges, since the conversion of a course or exercise to an online medium required rethinking and remodelling the material for delivery.

The Agency organised the European Cyber Security Challenge (ECSC) 2021 final, a competition that was widely acknowledged as the best so far since 2016. We are now confident that the ECSC goal of attracting participation from all EU Member States and European Free Trade Association (EFTA) countries will be reached in the next two or three years. In this context, the process of setting the goals of the ECSC five years from now has already started. This includes features such as expanding participation by admitting accession candidate countries and teams from outside Europe that participate in the competition but are not part of the score board. Moreover, the competition content will be further enhanced through the inclusion of defence against attack, social engineering challenges, etc. Lessons learned in 2021 from both the ECSC and the International Cybersecurity Challenge (ICC) (in 2021, under Activity 9) provided valuable contributions for the future.

ENISA developed a methodology for assessing the potential interoperability of risk management frameworks and methodologies and supported with the identification of cybersecurity skills needs and gaps. In 2022 the assessment of the methodology and the iterative process of improving it will take place.

Resources

All activities were duly resourced, and the budget allocated to them was used as planned. The carry-over amount in Activity 3 mainly relates to the postponement of two big events from 2021 to 2022, namely the Cyber Europe Exercise and the ICC, due to the ongoing pandemic. In terms of HR, all activities were also duly resourced. The slight deviation in the actual FTEs consumed had to do with delays encountered in recruitment, which were compensated for by the existing team. The experience of 2021 is the main driver of budget estimates for 2024 onwards. ENISA is therefore processing its own quantified approach along these lines.

Overall assessment

Although 2021 was an important year for capacity-building activities, it also demonstrated the long road ahead in terms of moving closer to achieving cutting-edge competences and capabilities in cybersecurity across the EU – the Agency's strategic multiannual objective to which the activity contributes. As shown in the evaluation of KPIs of the activity, important gaps persist in terms of both ensuring the maturity of Member States' national strategies (the Member States that participated self-assessed their maturity as low or medium, rather than high) and ensuring that ENISA exercises and training deliver high levels of added value. Although there is currently no overall understanding of the level of capabilities across the Union – a situation that should change after the

pilot cybersecurity index has been conducted in 2022 – evaluation of indicators points to the need for increased efforts and investments in capacity building.

Thus, it is important that for exercises and training one of the main priorities for 2021 was the development of the new approach that takes into account the new conditions set by the CSA, which expands ENISA's audience in terms of capacity building with the addition of EU institutions and agencies. This work had to be carried out at the same time as the Agency had to continue to provide its services to Member States. The direction set by the Management Board during its strategic discussion in March 2022 points to a clear way forward to consolidate ENISA exercises and training and focus them 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. Secondly, the Agency needs to step up and strengthen its support to Member States in terms of helping them to develop and maintain comprehensive and effective national strategic frameworks that underpin national capacity-building.

Objectives



- Increase the level of preparedness of and cooperation within and between Member States and sectors, and EUIBAs
- Prepare and test capabilities to respond to cybersecurity incidents
- Foster interoperable European risk management, consistent methodology and risk assessment practices
- Increase skill sets and align cybersecurity competences
- Increase the supply of skilled professionals to meet market demand, including supporting the necessary educational structures

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 to develop national cybersecurity strategies

Outcome



- ENISA developed an online tool to accompany the national cybersecurity assessment framework in order to help Member States perform a self-assessment exercise meant to improve national cybersecurity capabilities (<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/>).
- ENISA produced a study on good practices on citizens' awareness of cybersecurity (<https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity>).

- ENISA organised the annual NCSS workshop, which took place online (<https://www.enisa.europa.eu/events/9th-enisa-national-cybersecurity-strategies-workshop>).

In the area of NCSSs, all objectives were met in 2021. For 2022, the aim is to develop a good practices framework (expanding on the work of the national cybersecurity assessment framework tool) and to continue the iterative process of reviewing/improving the NCSS map. From 2022 onwards, not only will the work continue in an iterative process (namely, use of the tools – assessment of framework’s effectiveness – improvement of framework) but we will further build on the links of this activity to the cybersecurity index and info hub activities.

3.2. Organise large-scale biannual exercises and sectoral exercises (including Cyber Europe, Blueprint Operational Level Exercise (Blue OLEx), CyberSOPEx)

The Exercises Team of the Agency organised or co-organised the following exercises during the reporting period.

- CyberSOPEx 2021: testing the standard operating procedures (SOPs) of the Computer Security Incident Response Teams (CSIRTs) Network. This was organised and conducted by ENISA.
- CySOPEx 2021: testing the SOPs of the CyCLONe Network. This was co-organised and conducted by ENISA.
- Blue OLEx 2021: testing the CyCLONe SOPs but with the main focus on CyCLONe’s decision-making and internal communication at executive level. This was co-organised and conducted by ENISA.
- Cyber Crisis Coordination Exercise 2021 for the European Commissioners’ cabinets. ENISA was involved in the scenario preparation and supporting the execution.
- EU Cyber Crisis Linking Exercise on Solidarity: preparations started in 2021, and the execution will take place in 2022. ENISA was part of the core planners’ team, together with the National Cybersecurity Agency of France (which was the main initiator) and the European External Action Service (EEAS).
- 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 2021. 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 preparation of the exercise and providing the Cyber Exercise Platform.

In addition, ENISA engaged in the preparatory work for Cyber Europe 2022 together with the Austrian planners. This included updating the current Cyber Exercise Platform, to make it more secure and resilient, and creating extra scenario options. It is also worth noting that the pandemic forced a change in plan of the organisation of Cyber Europe in order to take into account the shifting of the exercise from 2021 to 2022.

The two main achievements in this area (as well as for output 3.3 below) in 2021 were the preparation of the new ENISA strategy on exercises, and training courses meeting the requirements of the CSA. At the same time, the Exercises Team also started the necessary preparatory work

for switching to the new Cyber Exercise Platform in 2022. This was considered to be necessary because the platform currently used by the team was reaching the end of its life. The preparations included stocktaking of user requirements from the group of Member State planners. In 2022–2023, the team will devote effort to informing all relevant communities in accordance with the CSA) of the new strategies on exercises and trainings. Moreover, in 2022 ENISA will focus on implementing the provisions of the new strategies.

3.3. Organise training and other activities to support and develop the maturity and skills of CSIRTs (including NISD sectoral CSIRTs) and other communities

New e-learning material was developed on the topic of ransomware. It involves the ATT&CK framework to help analysts understand and the tactics, techniques and procedures of adversaries. The objective here was to promote mitigation measures in order to ensure better protection against similar threats. In-depth training courses and accompanying tabletop exercises were delivered in 2021: the information security management and information and communications technology (ICT) security courses were held in two iterations each and had 59 participants in total during the 5-day training. The cyber threat management course had 16 participants completing the three days of training. ENISA organised and conducted an interactive tabletop capacity-building activity for representatives of EU Member States participating in the cooperation group's work stream 12 on the health sector.

In its cooperation with CERT-EU, ENISA's objective was to provide a state-of-the-art, relevant and cost-efficient training portfolio for the benefit of both Member States and EUIBAs. A close operational collaboration with CERT-EU and its other key stakeholders was developed to this end and to support cybersecurity capacity building.

3.4. Develop coordinated and interoperable risk management frameworks

- Report Interoperable EU Risk Management Framework. ENISA published a methodology for assessing the potential interoperability of risk management frameworks and methodologies, and presented the results (<https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework>).
- Report Compendium of Risk Management Frameworks with Potential Interoperability. This collection of identified frameworks and methodologies includes well-known and widely used risk management standards that provide high-level guidelines for risk management processes that can be applied in all types of organisations (<https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks>).
- Workshop on interoperability of EU risk management frameworks. The workshop was conducted as a means to present to 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 2021 in this area was the establishment of the risk management framework. In 2022, the focus will now shift to assessing its interoperability potential. The iterative process will be completed by improving on the framework from 2023 onwards.

3.5. Support the capacity-building activities of the NIS CG and sectoral work streams in accordance with the NIS CG work programme

- Capacity-building activity for NIS CG work stream 12 (Health). ENISA delivered an interactive tabletop capacity-building activity that provides a safe environment among peers to increase the overall competence of NIS authorities in addressing cybersecurity in the health sector.
- Roadmap for capacity-building activities for NIS CG work streams. ENISA launched a survey to identify the needs of the NIS CG work streams for capacity-building activities and accordingly to prioritise future activities based on the needs identified. This work is closely related to the work carried out under output 3.2. In this respect, the work on training provided under this output is aligned with the strategy on exercises and training developed under outputs 3.2 and 3.3.

This output, as is also the case for output 3.6, forms a specific use case (for a specific user group) of the work developed under outputs 3.2 and 3.3. In this light, in 2022–2023, the team will devote effort to ensuring (as was the case in 2021) that the work for this user group is fully aligned with the new strategies on exercises and training. Moreover, in 2022, ENISA will focus on implementing the provisions of the new strategies.

3.6. Support the establishment, development and cooperation of European information-sharing schemes based on ISACs, public–private partnerships and other existing mechanisms

- Report Cross-Sector Exercise Requirements for ISACs. This report seeks to identify the skills, exercises and training needed to help information exchange between ISACs (<https://www.enisa.europa.eu/publications/cross-sector-exercise-requirements>).
- Report Zoning and Conduits for Railways. The report is designed to give guidance on building cybersecurity zones and conduits for a railway system (<https://www.enisa.europa.eu/news/building-cyber-secure-railway-infrastructure>).
- Supporting the European Commission with the ISACs Platform. ENISA provided support to the project on developing new ISACs and improving existing ones. The support involved participating in meetings with the Commission and providing expert opinion on cybersecurity architecture and the cybersecurity functions of the platform.
- Supporting EU ISACs. ENISA continued its support to the various EU ISACs. In the finance ISAC, ENISA organised two virtual meetings and one physical meeting. In the energy ISAC, ENISA organised three online webinars (operational technology cybersecurity, vulnerability framework, and AI and operational technology) and prepared an annual ISAC threat landscape. In the maritime and health ISACs, ENISA provided support in organising meetings and exchange of good practices.

3.7. Organise the European Cyber Security Challenge (ECSC)

The 7th edition of the European Cyber Security Challenge, ECSC 2021, was hosted in Prague in October. The organiser of ECSC 2021 was the Czech chapter of AFCEA.

In total, 300 people (contestants, coaches and judges) representing 20 EU and EFTA countries competed in the ECSC final in Prague, and one country from outside Europe participated for the first time in the competition as a guest (Canada). The finalists of ECSC 2021 were the teams from Germany, Italy and Poland.

Furthermore, in view of its participation in the International Cybersecurity Challenge (ICC), for the first time ENISA assembled a European team during the reporting year. A total of 55 candidates from 21 countries were preselected to potentially be part of the final Team Europe that will participate in the finals in June 2022 (in Athens).

To support the selection process, two physical boot camps were held in 2021 (in Tallinn and Turin) together with an online qualifier event. It is also worth noting that the pandemic forced us to re-plan the organisation of ICC in order to take into account the shifting of the final from 2021 to 2022.

Despite the negative impact of the pandemic on the organisation of large-scale physical meetings such as the ECSC, the final of 2021 was the best to date. 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. Moreover, the output will also include a training activity targeting young talents who can participate in the ECSC and ICC (obviously linked to output 3.3). In 2022–2023 and onwards, the emphasis of the ECSC will be on setting the priorities and challenges for the next 5 years, while that of the ICC will be on agreeing an established governance structure for the future.

3.8. Report on cybersecurity skill needs and gaps, and support skills development, maintenance and implementation (including the Digital Education Action Plan and a report on higher education programmes)

- Report Addressing the EU cybersecurity skills shortage and gap through higher education. ENISA contributed to providing an overview of the current supply of cybersecurity skills in Europe through an analysis of data gathered and generated by the recently established Cybersecurity Higher Education Database (<https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>).
- Maintenance of the Cybersecurity Higher Education Database (CyberHEAD). It became the main point of reference for students looking for a cybersecurity job. With more than 130 programmes, it stands as the largest EU-validated source of information for cybersecurity programmes (<https://www.enisa.europa.eu/cyberhead>).

Already in the last few years significant steps have been made in this area, addressing the cybersecurity skills shortage in the EU in a systematic way. Through the development of the skills framework and CyberHEAD, ENISA is making an important contribution in this areas. In 2022–2023, ENISA will continue reviewing and improving the framework in an iterative process while at the same time increasing

the number of academic institutes included in CyberHEAD. Based on the experience of the collaboration with the Awareness Raising and Education Team (ARET), ENISA should consider whether this output is better addressed under Activity 9.

Key performance indicators	Unit of measurement	Frequency	Data source	Results
Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents				
3.1. Increase/decrease in maturity indicators				
Maturity of national cybersecurity strategies				
Number of Member States that rate the overall maturity of their cybersecurity strategy				
High maturity	Number	Annual	Survey	3
Medium maturity	Number	Annual	Survey	4
Low maturity	Number	Annual	Survey	3
Number of Member States planning to use ENISA framework to measure the maturity of their national cybersecurity capabilities				
Already using	Number	Annual	Survey	1
Not using but planning to use	Number	Annual	Survey	5
Don't know or will not use in the foreseeable future	Number	Annual	Survey	4
Number of Member States that have set KPIs to measure progress and effectiveness of the implementation of their strategic objectives when drafting their NCSSs				
Already using	Number	Annual	Survey	3
Not set but planning to use	Number	Annual	Survey	4
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	3
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
Every 4–5 years	Number	Annual	Survey	6
More than 6 years or don't know	Number	Annual	Survey	2
Total maturity of ISACs (self-assessment)				
ISAC A	%	Annual	ISAC dashboard	63 %
ISAC B	%	Annual	ISAC dashboard	56 %
ISAC C	%	Annual	ISAC dashboard	90 %
ISAC D	%	Annual	ISAC dashboard	50 %
ISAC F	%	Annual	ISAC dashboard	63 %
3.2. Outreach, uptake and application of lessons learned from capability-building activities				
CySOPEX 2021 (number of improvements proposed by participants)	Number	Per exercise		5

3.3. Number of cybersecurity programmes (courses) and participation rates^a				
Total number of students enrolled in the first year of the academic programmes (2020)	Number	Annual	Report ^b	4 843
Number of male students	%	Annual	Report	80 %
Number of female students	%	Annual	Report	20 %
Total number of cybersecurity programmes (2020)	Number	Annual	Report	119
Number of postgraduate programmes	%	Annual	Report	6 %
Number of master's programmes	%	Annual	Report	77 %
Number of bachelor's programmes	%	Annual	Report	17 %
3.4. Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey)				
CySOPEx 2021 exercise				
Usefulness low	%	Per exercise	Survey	0 %
Usefulness medium	%	Per exercise	Survey	57 %
Usefulness high	%	Per exercise	Survey	43 %
Relevance low	%	Per exercise	Survey	4 %
Relevance medium	%	Per exercise	Survey	50 %
Relevance high	%	Per exercise	Survey	46 %
CyberSOPEx 2021 exercise				
Usefulness low	%	Per exercise	Survey	22 %
Usefulness medium	%	Per exercise	Survey	78 %
Usefulness high	%	Per exercise	Survey	0 %
Relevance low	%	Per exercise	Survey	0 %
Relevance medium	%	Per exercise	Survey	54 %
Relevance high	%	Per exercise	Survey	46 %
Blue OLEx 2021 exercise				
Usefulness low	%	Per exercise	Survey	5 %
Usefulness medium	%	Per exercise	Survey	77 %
Usefulness high	%	Per exercise	Survey	18 %
Relevance low	%	Per exercise	Survey	7 %
Relevance medium	%	Per exercise	Survey	55 %
Relevance high	%	Per exercise	Survey	38 %
Allocated FTEs as per SPD based on full establishment at year-end 2021	15	Actual used FTEs		10.35
Planned budget (direct costs only)	EUR 1 400 000	Consumed budget (direct costs only)		EUR 1 399 779
		Of which carried over to 2022		EUR 334 734^a

a The carry-over amount mainly relates to the shifting in time of two big events from 2021 to 2022, namely the Cyber Europe Exercise and the ICC. Both events were moved to 2022 because of the ongoing pandemic.

b <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>

ACTIVITY 4

Enabling operational cooperation



Achievements

2021 was a pivotal year for the support to the EU networks. The establishment of the Operational Cooperation Unit, ENISA orchestrated the support envisioned as Secretariat of the CSIRTs Network (defined by NISD1) together with the newly established CyCLONe (Cyber Crisis Liaison Network) launched in September 2020. This enabled ENISA to synergise the support for these networks.

In relation to the CSIRTs Network, ENISA's efforts went beyond the active support of daily operations in case of incidents and brought the CSIRTs Network much forward in terms of operational cooperation. The Secretariat facilitated for example with vendor outreach and supported the Network during extended alert periods relating to high profile situations such as MS Exchange and Log4j. The Secretariat supported with ad-hoc reporting to members and extended its' operational support beyond working hours and holidays, thus prompting the CSIRTs Network members to engage actively, despite the COVID-19 pandemic situation. All these were achieved based on the capacity of the Secretariat to go the extra mile for the benefit of the Network.

It was a milestone year for CyCLONe as it was the first full year of operation and the Secretariat used its existing knowledge from the CSIRTs Network support to bring this newly established network rapidly up to speed in terms of tools and procedures which resulted in 1011% more interactions compared to the Q4 2021. Thus providing a solid basis for future interactions between the CyCLONe and the CSIRTs Network.

2021 was also the first year when the same exercise scenario was tested at both the technical and operational levels in a series of exercises engaging all networks. For the technical level CyberSOPex tested the CSIRTs Network readiness and was followed by other exercises designed at the operational level. CyCLONe was tested for first time during the CySOPex 2021 exercise that was tailored for CyCLONe officers whilst 2021 BlueOlex exercise was tailored for the high-level actors of national cybersecurity authorities. Moreover, under the Slovenian Presidency, ENISA organised the first physical post pandemic meeting, the 15th CSIRTs Network meeting and the first ever shared session with CyCLONe.

In addition to these activities and in cooperation with the European Commission and with the Slovenian presidency, ENISA organised hybrid and virtual workshops to support the discussions around the Joint Cyber Unit initiative: one workshop dedicated to the preparatory activities and two more workshops dedicated to situational awareness of the EUIBAs and EU MSs respectively. These activities initialised the discussions on exploring the potential of the JCU and initiated a better and closer cooperation between the EUIBAs in the field of operational cooperation, more specifically in the area of situational awareness (linked to Activity 5).

ENISA also facilitated the operation and information exchange with infrastructure, tools and expertise. Support activities included the development and maintenance of IT platforms (including MeliCERTes) and communication channels, exchanges of best practices, guidance and advice regarding incident response. For instance, for the MeliCERTes project, activities continued on maintenance of the previous version of MeliCERTes. In addition to this, a complete high-level architecture of the next version of the platform was created and presented to the CSIRTs Network. In 2021, ENISA worked on the technical specifications for this new architecture and started building it up. In particular, ENISA provided high-availability to these infrastructures and tools. To support both versions of MeliCERTes project, interoperability tests were carried out and witnessed by ENISA and funded by the Connecting Europe Facility (CEF) Telecom Cybersecurity program.

In addition, activities were carried out to improve and update maturity frameworks of the EUIBAs and to support cooperation between CSIRTs and Law Enforcement.

ENISA continued to work closely with other EUIBAs (European Union Institutions, Bodies and Agencies). Based on the Memorandum of Understanding (MoU) signed in 2018 between ENISA, EDA, Europol EC3 and CERT-EU, cooperation activities continued with annual activities. In addition, a new MoU was signed with CERT-EU leveraging on structured collaboration in accordance with the Cybersecurity Act.

Resources

As mentioned above, 2021 activities were covered thanks to the ability of the unit staff members to be flexible and go the extra mile. The Unit started the year without staff members in all the allocated posts. Without the commitment of the unit staff members, that also supported the integration of the new colleagues and SNEs, the agency would not have been able to support the extended escalated modes as in the case of MS exchange and Log4j, or to deliver on the unplanned activities such as the one related to JCU initiative (published during 2021). This resulted in a lot of strain on the limited staff members in the Unit. It should be noted that at the time of writing some additional SNEs have been foreseen for the unit in the coming year. To be able to increase its' capability to deliver upon Activity 4, both in terms of the Secretariat and as regards infrastructure and tools, the Unit would require additional resources, also in view of the need to be able to function 24/7.

The Unit took over and manages several tools and platforms that require permanent availability. To ensure continuation of services (for end of the year and the beginning of the next one) some of the services such as licences and maintenance contracts were de-synchronized from the annual budgetary cycle. The unit is reviewing its budget planning to better align service provisions to the financial/budgetary cycles, to reduce the amounts carry over, however the adjustments will most likely only be noticeable as of 2023 due to existing provisions and contracts.

Overall assessment

With the creation of the Operational Cooperation Unit, the baseline for operational cooperation in the EU in a structured way was enabled thus further strengthening the CSIRTs Network, establishing the CyCLONe foothold and initiating greater interaction with the EUIBAs. In order to reach the full potential of such cooperation and further improve capabilities and enable effective incident response and crisis cooperation among Member States and EU institutions, additional resources will need to be allocated to sustain the evolving threat landscape. The unit already planned a re-structuring of the activity dedicated to operational cooperation in 2022. In the 2022 SPD similar activities such as management of tools and platforms were gathered under same output with the same for activities involving common stakeholders. The process to find the best balance and the most efficient mode of organisation will require assessment of the steps already planned for 2022. This activity should also focus on secure communication channels for the various operational communities that would require staff with the necessary experience.

Objectives



- Enhance and improve incident response capabilities across the EU
- Enable effective incident response and cooperation among Member States and EU institutions (including through the blueprint)
- Improve the maturity and capacities of operational communities (including the CSIRTs Network and CyCLONe)

Link to strategic objective (ENISA strategy)



- Effective cooperation among operational actors within the EU should massive cyber incidents arise
- Empowered and engaged communities across the cybersecurity ecosystem

Results



- All communities (EU institutions and Member States) use a rationalised set of SOPs
- An agreed CSIRTs Network approach to selecting, operating and decommissioning tools
- Coherent SOPs for cybercrisis management
- Efficient framework, tools and methodologies for effective cybercrisis management

Outputs



- 4.1.** Support the functioning and operations of the CSIRTs Network (including through MeliCERTes) and CyCLONE, and cybercrisis management in the EU

Outcome



CSIRTs Network-related activities

ENISA, as secretariat of the CSIRTs Network, supported all the aspects related to the functioning of the network, including hosting a variety of tools for the purposes of communication, operational effectiveness, collaboration and information sharing.

Under the 2021 Portuguese Presidency, ENISA organised the 13th and 14th CSIRTs Network meetings, including a shared session with the NIS CG. Under the Slovenian Presidency, ENISA organised the first physical post-pandemic meeting, the 15th CSIRTs Network meeting which was the first ever shared session with CyCLONE.

In line with NISD requirements, ENISA supported the drafting of the third report to the Cooperation Group and, parallel to the ordinary functioning of the CSIRTs Network, ENISA also supported the operational cooperation among all CSIRTs Network members during all the high-profile incidents that required escalation and, among other outcomes, resulted in public statements on the Microsoft Exchange (<https://www.enisa.europa.eu/news/enisa-news/statement-on-microsoft-exchange-vulnerabilities>) and Log4j (<https://www.enisa.europa.eu/news/enisa-news/log4j-vulnerability-update-from-the-csirts-network>) vulnerabilities, and in the establishment of the CSIRTs Network GitHub (<https://github.com/enisaeu/CNW>).

ENISA organised CyberSOPEX in October 2021, in order to further test the readiness of the CSIRTs Network for large-scale cross-border incidents, and the same scenario was also used in the CyCLONE exercises.

Studies dedicated to specific tools and training material were produced for the purpose of improved cooperation and collaboration between Member States and EUIBAs as well as between CSIRTs and LE (<https://www.enisa.europa.eu/publications/2021-report-on-csirt-law-enforcement-cooperation>).

ENISA published an updated handbook (<https://www.enisa.europa.eu/publications/aspects-of-cooperation-between-csirts-and-le-handbook-2021>) and toolset (<https://www.enisa.europa.eu/publications/aspects-of-cooperation-between-csirts-and-le-toolset-2021>) on Aspects of Cooperation between CSIRTs and LE.

Two training sessions were organised in August and in October 2021 to pilot the ENISA training material on CSIRT–LE cooperation.

The 10th ENISA–EC3 Workshop on CSIRT–LE Cooperation took place on 19 October 2021 and brought together the CSIRTs and LE communities from EU Member States and EFTA countries.

Furthermore, together with the CSIRTs Network, ENISA updated and improved the CSIRTs maturity framework (<https://www.enisa.europa.eu/publications/enisa-csirt-maturity-framework>). ENISA coordinated with EUIBAs to draft the first maturity model for the EU's cybercrisis management. The model was made available to the EUIBAs.

CyCLONe Officers Network-related activities

The EU CyCLONe was launched in 2020. In 2021 ENISA focused on further development of this new network by providing the secretariat as well as the tools and support required to ensure the functioning and interactions between the Member States.

Under the 2021 Portuguese Presidency, ENISA successfully organised and coordinated all supporting activities for the 2nd and 3rd CyCLONe Officers Meetings. Under the Slovenian Presidency, ENISA supported the CyCLONe Chair and Members and successfully organised the 4th CyCLONe Officers Meeting and the first ever physical meeting of CyCLONe officers, the 5th CyCLONe Officers Meeting, in a hybrid form in Ljubljana, with a shared session with the CSIRTs Network that resulted in a formal input to the JCU discussions.

This was also the first year that the same exercise scenario was tested at technical and operational levels and it was the CyCLONe first ever operational level through:

- CySOPex 2021, the exercise tailored for the CyCLONe officers, in May 2021;
- Blue Olex 2021, the exercise tailored for the high-level members of national cybersecurity authorities, in October 2021.

ENISA carried out several activities designed to improve information sharing and operational cooperation, in particular regarding automated reporting, impact assessment and situational awareness, using the CyCLONe tools.

Joint Cyber Unit preparatory activities

In the context of the JCU initiative, in cooperation with the European Commission and with the Slovenian Presidency, ENISA organised hybrid or virtual workshops: one workshop dedicated to the preparatory activities for the JCU, and two more workshops dedicated to situational awareness in the EUIBAs and EU Member States respectively.

MeliCERTes project and tools

During 2021, ENISA maintained and applied patches to the Central Service Platform based on the penetration test conducted by the MeliCERTes consortium. In addition, the first-tier helpdesk continued to be provided by ENISA.

Workshops in the CSIRTs Network tooling working group were organised, so that the specifications for the Identity and Access Management system could be defined. For this purpose, a comparative analysis of several proofs of concept was conducted.

In addition, technical requirements for MeliCERTes 2 tools were collected and the expectations for the recovery time objectives and recovery point objectives were defined.

ENISA participated in several exercises for the business continuity plan, and in the risk assessment of specific central services. ENISA also proceeded with the procurement and installation of extra hardware and software needed for the centrally hosted services of MeliCERTes. In particular, ENISA set up the secondary site in Athens to host nodes for the high available services of the MeliCERTes project.

The first stable version of Cerebrate (<https://github.com/cerebrate-project/cerebrate>), an open-source platform meant to act as a trusted contact information provider and interconnection orchestrator for other security tools, was published. A pilot version was installed in ENISA.

ENISA also carried out activities for the development and maintenance of the CSIRTs Network Portal.

With the creation of the Operational Cooperation Unit, the baseline for operational cooperation in the EU in a structured way was enabled thus further strengthening the CSIRTs Network, establishing the CyCLONe foothold and initiating greater interaction with the EUIBAs. In order to reach the full potential of such cooperation and further improve capabilities and enable effective incident response and crisis cooperation among Member States and EU institutions, additional resources will need to be allocated to sustain the evolving threat landscape

4.2. Activities to support the development, implementation and evolution of MoUs between ENISA, Europol, CERT-EU and the EDA

In the context of the MoU, between ENISA, Europol, CERT-EU and the European Defence Agency (EDA), these four organisations identified areas of cooperation based on their common interest. During 2021, the focus was on information exchange, education and training (including cyberexercises), technical/operational cooperation and strategic matters.

ENISA acted as chair of the MoU during the reporting year. Several deliverables were prepared.

- ENISA developed and delivered to the MoU partners a collaboration portal for the project management of the MoU roadmap to facilitate interactions among MoU partners.
- In the area of exercises, ENISA, EC3 and CERT-EU worked together on the preparation of several cybercrisis exercises.
- ENISA and EC3 organised high-level workshops bringing together their respective communities i.e. CSIRTs and LE). During the workshops, representatives from CSIRTs and LE discussed their success stories and challenges related to their cooperation.

In March 2021, ENISA and CERT-EU agreed on a structured cooperation on the basis of the provision of the CSA (Article 7.4) by signing an MoU covering operational cooperation as well as capacity building, knowledge and information. This new MoU was needed because of the operational nature of the cooperation mandated by the CSA. The activities for 2021 were agreed and planned in the annual cooperation plan. As part of the efforts for further development of the Blueprint, ENISA and CERT-EU aligned actions on developing EUIBA SOPs and improving the Unions common situational awareness.

For 2022 this activity has been moved under the new re-defined Output 4.1 in order to streamline the efforts and improve efficiency when interacting with EUIBAs.

4.3. Develop SOPs, procedures, methodologies and tools for cybercrisis management

ENISA's objectives for 2021 were to support the activities dedicated to the cooperation of the operational actors within the Union in the event of massive cyberattacks, and to empower and engage communities. This work supports the implementation of the Blueprint for the EUIBAs and was done in liaison with other EUIBAs.

Several deliverables were prepared in order to analyse the ecosystem of cooperation. In particular, these reports covered a wide spectrum:

- an in-depth research analysis of SOPs;
- a set of comprehensive SOPs;
- an SOP survey of the EUIBAs;
- a set of guidelines for crisis communications.

ENISA also organised a working group of EUIBAs to exchange information, and organised several bilateral and multilateral meetings with the stakeholders to develop the SOPs and a plan for a 3-year exercise programme.

Several steps were undertaken under this output such as crisis communication. The goal of having EUIBA SOPs in place was not achieved because of moving targets such as the JCU. In general, the work under this output should focus more on supporting the task force / JCU.

Key performance indicators	Unit of measurement	Frequency	Data source	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				
CSIRT network				
Increase in active users from 2020	%	Annual	Platform	115 %
Increase in number of exchanges/interactions from 2020	%	Annual	Platform	291 %
CyCLONe				
Increase in active users from 2020	%	Annual	Platform	143 %
Increase in number of exchanges/interactions from 2020	%	Annual	Platform	1 011 %
4.2 Uptake of platforms/tools/SOPs during massive cyberincidents			N/A	4 %
4.3. Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs provided by ENISA	N/A	Biennial	Survey	N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	8	Actual used FTEs		6.70
Planned budget (direct costs only)	EUR 1 110 000	Consumed budget (direct costs only)		EUR 1 128 795
		Of which carried over to 2022		EUR 556 633

N/A, not applicable.

ACTIVITY 5

Contributing to cooperative response at Union and Member State levels



Achievements

ENISA contributed to the development of effective operational cooperation among Member States (MS) and EUIBAs by generating and consolidating information (including for the general public) on cyber situational awareness, technical situational reports (threat reports), incident reports and threats. The Agency fine-tuned its weekly service (OSINT report) distributing information on relevant event to different stakeholder groups, including CSIRT Network, CyCLONe, EUIBAs services, and Member State's national authorities for critical sectors.

ENISA also actively supported the consolidation and exchange of information on strategic, tactical and technical levels to operational communities, such as the CSIRTs Network and CyCLONe as well as relevant EUIBAs services such as DG CONNECT, CERT-EU, Europol EC3, INTCEN, EEAS Security and Defence Policy - Cyber Security, and EEAS Stratcom 2. In particular, as part of its structured cooperation with CERT-EU, ENISA piloted Joint Rapid Report services. This product provides timely information to senior decision makers about on-going cyber events and incidents and is expected to transition to production in the first half of 2022.

ENISA contributed to the incident response and cooperation among Member States and EU Institutions, Bodies and Agencies during some of the major security events and situations, such as the supply chain attack against SolarWinds and the exploitation of critical vulnerabilities, such as those linked to the Log4j 2.0 library, as well as monitoring cyber events related to COVID-19 situation. ENISA ensures active cooperation among key national and European stakeholders, which has led to joint guidance on vulnerabilities and threats. Furthermore, ENISA provided support both in the area of (a) incident impact assessment, (b) facilitation of technical handling of the incidents and (c) sharing relevant situation information with stakeholders.

The Agency increased its efficiency to generate and consolidate information, to assess incidents and to facilitate handling in this way contributed to the EU priority on situational awareness by supporting the consolidation and exchange of information on strategic, tactical and technical levels to operational communities. In doing so the Agency leveraged its internal capabilities, such as its operational toolsets and actively incorporating lesson learning in its operational response processes and after-action reviews.

In addition the Agency contributed to the initial scoping of the potential Joint Cyber Unit by way of a number of workshops on common situational awareness. The Agency together with EUIBAs established a roadmap of deliverables for the EUIBAs contribution to the Union situational awareness.

In line with its mandate, ENISA initiated actions to set up the framework to assist Member States on the basis of Article 7 of CSA, as such a proposal was developed for cybersecurity assistance mechanism with services and a pool of experts.

Resources

The resources for this activity as well as the distribution of talents with the right skillset will need to be assessed to meet expectations. Recognising the critical role of this activity led to the creation of the operations and situational awareness sector, within the Operational Cooperation Unit, in order to enable the Unit to focus on these tasks and to develop the appropriate strategy and plan resources accordingly.

The Operational Cooperation Unit set-up a crisis response team (CRT) mechanism with the aim at helping the Unit and agency to respond to large-scale cross-border incidents and facilitate inter-agency coordination. The mechanism was piloted for the first time to respond to the Log4j event that led to an after action report. The capabilities and the working methods of the mechanism are planned to be refined in the course of 2022.

The cyber situational awareness will require more resources than the ones currently assigned to address the evolving cybersecurity threat landscape. The achievements of this activity, given the limited resources, would not have been achieved without the proactive attitude and enthusiasm of staff members. In addition, when

the mechanism for cybersecurity assistance will be put in place, it will require additional resources to function, regardless of the actual delivery method. It is not foreseen for ENISA to be the delivery party for assistance to Member States on its own but by harnessing an external pool of experts to ensure scalability of the service.

As with Activity 4, the activity manages several tools and platforms that require permanent availability, therefore ensure continuation of services (for the end of the year and the beginning of the next) the services contracted such as licences and maintenance are not synchronized with the annual budgetary cycle, which is the reason for the carryover of budget from one year to the next. The unit is reviewing its budget planning to better align service provisions to the financial/budgetary cycles in order to reduce the amounts carried over, however the adjustments will most likely be noticeable in 2023 due to existing provisions and contracts. Following the above mentioned review of budget planning, as of 2022 several actions managing tools and platforms are gathered under the same output to optimise the coordination.

Overall assessment

In line with the Agency's mandate the foundations have been prepared for contributing to the Union common situational awareness as well for its operational capability to be able to respond to Member States requests in case of large scale cross-border incidents and events. The formalised new sector within the unit will provide the focus required in this activity and in particular around operations and situational awareness to address the increase needs for information exchange. This was also one of the leading themes of the initial work undertaken for the potential joint cyber unit as well the need for the agency to be able to respond to external requests.

The objectives for 2021 have been achieved however to meet increased stakeholder expectations and additional demand the acquisition of additional human resources with diverse skillset is needed in order for the Agency to increase capacity.

Given this assessment focus for the following year will be on organising the resources and strategy for operations and situational awareness and transitioning to a service-oriented approach. This might require a reduction in scope in some areas, due to the need to reassess the use of the tools and budget commitment to scale the delivery of its services and establish metrics that measure effectiveness and efficacy of the actions that seek to achieve the objectives of the activity. Additionally, the unit will focus on increasing its collaboration and partnership with Member States in synergy with Activity 4, build on the work done through the initial scoping of the potential JCU, in particular with EUIBAs services, as well as focusing on building trusted partnerships with the private sector.

Objectives



- Develop effective incident response and cooperation among Member States and EU institutions, including cooperation between technical and political actors during incidents or crises
- Establish a common awareness of cyberincidents and crises across the EU
- Facilitate information exchange and cooperation, both cross-layer and cross-border, between Member States and with EU institutions

Link to strategic objective (ENISA strategy)



- Effective operational cooperation within the EU in case of massive cyberincidents
- Empowered and engaged communities 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 cybersituational awareness, technical situational reports, incident reports and information on threats, and support the consolidation and exchange of information at strategic, tactical and technical levels

Outcome



ENISA produced cybersituational awareness with a focus on cyberincidents in the EU area but also across the world.

ENISA's cybersituational awareness services were provided to EUIBAs and authorities in Member States through regular weekly reports (ENISA's weekly open-source intelligence (OSINT) report) and ad hoc threat research.

ENISA significantly increased the weekly OSINT report outreach to recipients, with its OSINT reports now being sent to approximately 600 recipients.

In 2021, ENISA launched a new pilot product, the joint rapid report, in close cooperation with CERT-EU.

In parallel, ENISA continued improving its tools (Open Cyber Situational Awareness Machine) and delivered new ones (situational awareness team toolbox) that will enable better data ingestion and increase the production throughput.

ENISA's data collection in this area also represents the main source of information for ENISA's long-standing threat landscape reports.

Main outcomes of the work:

- 49 weekly OSINT reports sent to 500–600 recipients;
- 37 executive summaries on healthcare (linked to the COVID-19 pandemic) sent to the European Commission;
- 16 ad hoc threat research papers shared with CERT-EU, DG Connect, EEAS, EC3 and the general public;
- 20 joint rapid reports (including updates), done in cooperation with CERT-EU, for senior stakeholders.

2021 was a foundational year for the agency's situational awareness capability. While, with limited resources, the Agency was able to fulfil to its objective, however appetite for such capabilities have increased for common situational awareness. As such the unit established a sector in the last quarter of 2021 to focus on this capability and additional resources planned in the course of 2022.

Going forward the unit will establish the service portfolio with supporting tools and / or external services.

5.2. Support technical and operational cooperation, incident response coordination during crises and activities with the CSIRTs Network, and CERT-EU, EC3, EEAS and EDA EU-wide crisis communication planning

ENISA made progress on actions to support effective incident response and cooperation among Member States and EU institutions during incidents or crisis. This was achieved by building on the survey of Blueprint stakeholders and follow-up interviews with CSIRTs Network members.

ENISA produced deliverables (restricted for the moment to the CSIRTs Network members) on the mapping of secure communication channels and a methodology proposal for evaluating channels. Several supporting activities were carried out, such as support for the Crisis Communications Management Guide (connected to output 4.3); input to the EUIBAs SOP draft (connected to output 4.3); input to CSIRTs

Network SOPs and support of the CSIRTs Network SOP working group (connected to output 4.1); and support for the CSIRTs Network communications channels check (connection to output 4.1).

To improve interactions with the stakeholders relevant to this activity, this output was discontinued in the 2022 work programme, whilst the actions continue across other outputs in the activity.

5.3. Provide assistance and support on the basis of Article 7(4) and (7) of the CSA

ENISA launched activities in order to set up the framework for the assistance of Member States on the basis of Article 7 of CSA. Such assistance (at the request of Member States) was meant to cover the assessment of incidents and to facilitate the technical handling of incidents or crises. A proposal for assistance was created, covering a cybersecurity assistance mechanism associated with certain services and a pool of experts. Within this output based on structured interviews with Blueprint actors, ENISA produced the following deliverables (available at the moment to CSIRTs Network members): guidelines; processes and procedures; pool of experts' structure. A pilot project was carried out to test the operational activity of the assistance mechanism, and involved testing the provision of assistance with limited scope for three CSIRTs Network members. Results of the deliverables and lessons learned from the pilot project will be used in the further development of the assistance mechanism.

The actions carried out in 2021 set up the basis for a framework to provide assistance and support according to Article 7 of CSA. The outcomes of these actions will be used in organize the assistance mechanism with the aim to provide assistance and support to Member States. The mechanism to be implemented will require additional resources in order to asses, manage, and evaluate both the requests and the technical services to be delivered.

Key performance indicators		Unit of measurement	Frequency	Data source	Results
ENISA's ability to support the response to massive cyber incidents					
5.1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents that ENISA contributes to mitigation efforts		N/A	Biennial	Survey	N/A
5.2. Stakeholder satisfaction with ENISA's ability to provide operational support		N/A	Biennial	Survey	N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	8	Actual used FTEs			3.91
Planned budget (direct costs only)	EUR 1 200 000	Consumed budget (direct costs only)			EUR 1 096 419
		Of which carried over to 2022			EUR 513 412

N/A, not applicable.

ACTIVITY 6

Development and maintenance of EU cybersecurity certification framework



In 2021, Activity 6 sought to produce meaningful outcomes along the lines of furthering the cybersecurity certification framework in order to serve the Agency's strategic objective of a 'high level of trust in secure digital solutions'. More specifically, ENISA assisted the Commission on the governance of the framework, promulgated three cybersecurity certification schemes with different maturity levels and prepared its online services on certification.

Achievements

By the end of 2021, ENISA had made meaningful contributions to the EU cybersecurity certification framework by assisting the Commission with regard to discharging its duties concerning governance (European Cybersecurity Certification Group (ECCG) and Stakeholders Cybersecurity Certification Group (SCCG)) and further processing draft candidate cybersecurity certification schemes in terms of planning and content development. ENISA thus served the strategic objective of a 'high level of trust in secure digital solutions' by reinforcing this aim with new components of certification schemes, some of which have not yet been adopted and implemented by Member States. Achievements include:

- the conclusion of the EU common criteria certification scheme with the opinion of the ECCG;
- the advancement of the EU cloud services certification scheme in a way that allows finalisation in early 2022;
- the launching of the ad hoc working group (AHWG) on the EU5G certification scheme;
- the kick-off of the ECCG subgroup on encryption;
- the conclusion of the Union rolling work programme at SCCG level;
- advances in the design and implementation of the workflow and application programming interface for certificate publication, as well as an analysis for a cybersecurity certification label.

Further enhancements to the certification approach led to adding guidance, pilots and methodological components. The multiannual component of the Agency's programming document provided further guidance and the context for the overall pursuits of the year. During the reporting year, ENISA improved on its systems and services by consolidating the use of collaboration tools of importance for the interactions with external experts. To this end, it developed and implemented a web-based service for the Member States concerning certification.

Resources

While all activities were duly resourced, the consumption of the budget allocated to cybersecurity certification lagged because of a late decision in relation to the support and preparation for the 5G EU scheme. As a result, the allocated resources were not consumed in full, since ENISA accommodated requirements tailored to a multistakeholder environment where consultations and time constraints played a key role.

The main drivers for providing budget estimates in 2024 onwards will depend on the pace of implementation of the Union rolling work programme on cybersecurity certification (i.e. production costs), the concentration of actions to monitor adopted schemes (i.e. maintenance costs) and the transition to an online platform to meet stakeholders' requirements (i.e. community service costs). ENISA is therefore processing its own quantified approach along these lines.

Appropriations carried forward served the purpose of bridging the multiannual cybersecurity certification work from one year to the next, while serving the principle of annual budgets. The small amount carried forward does not affect the ability of the unit to perform its tasks in 2022.

Overall assessment

Cybersecurity certification provides a focal point for the industry and, as the KPIs suggest, increasingly the assistance and support stakeholders need including due guidance for the public authorities concerned, when an adopted scheme becomes available in such a way that it can be implemented and further enforced. The cybersecurity certification framework remained high on the stakeholders' agenda during the reporting year, as demonstrated by the robust support to and interest in ENISA activities as well as the results of KPI metrics. Within the boundaries of its competence, ENISA's timely response and coherent production of schemes and related deliverables and outputs supported the cybersecurity certification framework.

Objectives



- Trusted ICT products, services and processes
- Increased use and uptake of European cybersecurity certification

Link to strategic objective (ENISA strategy)



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

Results



- Support for schemes chosen to run under the European cybersecurity certification framework
- Certified ICT products, services and processes preferred by consumers and, where relevant, OESs and DSPs

Outputs



- 6.1.** Draft candidate cybersecurity certification schemes and contribute to the establishment of the schemes

Outcome



ENISA worked in response to Commission requests for cybersecurity certification schemes as follows.

EU5G.

- In coordination with the European Commission, ENISA established the AHWG to define the candidate EU5G scheme. The AHWG on EU5G is formed of three preparatory work streams mapping the request and seeking to leverage on a methodology meant to identify certification gaps. While ENISA worked closely with public authorities and the Commission in the preparation phase, kick-offs were organised in Q4 2021 with over 100 participants involved (50 % from public authorities and with broad private sector participation).
- During the setting up of the AHWG, ENISA engaged with external experts into the preparation of reference documentation for the important activity of risk and gap analysis of work stream 3 of phase 1 of the scheme's development. ENISA also carried out a pilot on the newly defined methodology for sectoral cybersecurity assessments, to validate its further use for the EU5G project

Cybersecurity certification conference

- ENISA organised its annual cybersecurity conference in December 2021 in Athens. Keynote speakers and panellists discussed cybersecurity certification including changes in the market, approach to emerging technologies (AI, 5G), link with standardisation and the impact on end user consumers. The conference attracted about

25 guest speakers, 50 attendees on site and over 1 200 attendees online (1 800 registrations).

European cloud services

- ENISA continued working on the request of the Commission for an EUCS scheme. In Q1, a public review was launched with several presentations to the public, followed by an analysis of the feedback.
- The results of the survey led to revisions of the first draft candidate scheme, and in particular of the part on requirements. Subsequently these requirements were proposed to CEN-CENELEC Joint Technical Committee 13 for the development of a technical specification. Additional content was developed, in particular about extension profiles and requirements for Conformity Assessment Bodies.
- In Q3/Q4, EUCS prompted by the Member States, ENISA examined aspects related to digital sovereignty and independence from non-EU laws; currently a thematic group is seeking to consolidate an approach to guidance received from the Member States and the ECCG.

Certification

- In 2021, the Agency continued the same high pace of execution of cybersecurity certification requests; as ENISA is gaining experience and maturity, adding concurrent actions will probably take precedence over a high frequency of actions.
- Drafting candidate cybersecurity certification schemes and contributing to the establishment of the schemes are essential actions to underpin and develop the EU cybersecurity certification framework; accordingly, this output can remain. Care needs to be taken to dedicate resources to this output in such a way that they reflect the actual level of execution of the Union's rolling work programme or equivalent request.

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

EUCC

- In relation to the Commission's request for a cybersecurity certification scheme on EUCC, the Agency supported the Commission in prepare the first draft implementing act on the candidate EUCC, which was discussed at the ECCG in June 2021, and it has remained work in progress since then.
- During the reporting year, a guidance strategy on the EUCC scheme was developed by the Agency with a view to supporting the preparations for the implementation of EUCC and the transition from SOG-IS certification to EUCC. In line with the prioritisation foreseen by the ECCG, development of guidance on the following started in 2021: accreditation, certification transition, taxonomy, security of information and certification application forms. Pilots were therefore resorted to for the validation of certain provisions of the EUCC; this part of the work is still ongoing.

EUCS

- In EUCS, eight experiments were organised over the summer to verify the feasibility of some of the new measures introduced in the EUCS draft candidate scheme. Stakeholders from eight Member States and from the United States were involved, including

cloud providers, Conformity Assessment Bodies and National Cybersecurity Certification Authorities, and the results were used to enhance the draft candidate scheme.

- Work was initiated on the development of guidance, in particular around the new requirements on controls. This first phase of work was focused on the format of the information required in the guidance, and an initial version of the guidance was developed across five categories, representing around 25 % of the overall requirements of the EUCS.

Consequently, ENISA managed to be ahead of the planning in terms of content regarding the EUCC; ENISA has been right on track with EUCS and it launched the EU5G scheme, giving an overall picture of the span of its involvement in relation to the EU cybersecurity certification framework. It is also worth mentioning that ENISA further contributed to early policy considerations of the European Digital Identity Wallet in support of the Commission's efforts.

In relation to the output on the implementation and maintenance of the established schemes, including evaluation of adopted schemes and participation in peer reviews, ENISA has taken a dynamic approach and anticipated actions that facilitate the gradual implementation of schemes. This output is essential for maintenance, which will be the culmination of actions starting from the adoption of the first scheme onwards. As such it needs to remain and be further supported with commensurate resources that reflect the expected pace of implementation of schemes adopted.

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

The European Cybersecurity Certification Group (ECCG)

- ENISA assisted the Commission in its efforts to operate the ECCG and enable the ECCG to provide its views on the Union rolling work programme.
- The Agency supported the Commission to set up an ECCG subgroup on cryptography, on developing guidance on cryptographic mechanisms to be embedded in ICT products and services, and on developing related evaluation methodologies.
- Regarding the further development of the EUCS cybersecurity certification scheme that started at the beginning of 2020, a dedicated subgroup meeting was organised in March to allow Member States to discuss and provide input to the Agency on the mitigation of risks by security requirements related to independence from non-EU law for EUCS, an element of the EUCS scheme that was at an advanced stage at the end of 2021.
- Regarding the main projects related to the market, certification and standardisation, regular updates were provided to the ECCG to support the ECCG in its advisory role to the Commission and the Agency on the EU cybersecurity certification framework and the schemes under development.

The Stakeholder Cybersecurity Certification Group (SCCG)

- With support from ENISA, the SCCG assisted the Commission to draft the Union rolling work programme, identifying the strategic priorities for European cybersecurity certification schemes and future areas

for certification; consequently, the SCCG provided its opinion in February 2021.

- ENISA assisted the SCCG and the Commission in defining the KPIs and metrics for the future evaluation of the implementation phase and the first of operational phase of the European cybersecurity certification schemes.
- Regarding the main projects related to the market, certification and standardisation, regular updates were provided to the SCCG to support the SCCG in its advisory role to the Commission and the Agency. In particular, they covered the developments on the EUCC cybersecurity certification scheme for ICT products and the European cybersecurity certification scheme for EUCS.

As this output serves the governance of the cybersecurity certification framework and consumes no financial resources as such, it is required that it stay as is. Small amounts of resources can be dedicated indirectly in relation to output 6.1.

6.4. Development and maintenance of necessary tools for an efficient and effective EU cybersecurity certification framework (including a certification website and collaboration platform

ENISA website dedicated to certification

- With the support of selected Member States, ENISA further designed and developed the IT system to support the requirement for a website dedicated to the promotion of European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity in accordance with Article 50 of the CSA, as well as related information.
- The proposed approach includes a workflow and an application programming interface to facilitate the distribution of objects that ensured integrity and authentication.

Core Service Platform for EU Cybersecurity Certification Stakeholders

- ENISA supported the European Commission to develop and implement the Core Service Platform for EU Cybersecurity Certification Stakeholders. The platform is part of the 'support for set-up of a cooperation mechanism for national cybersecurity certification authorities envisaged by the Connecting Europe Facility 2019–2020 working programme and managed by the European Commission. The activity started in October 2021 with three workshops (one with ENISA, and the other two with the stakeholders proposed by ENISA, who were from the SCCG, the ECCG and the EUCC and EUCS AHWGs). ENISA provided the first use cases for the basic layer of the platform.

Tools and a website are essential conditions for the success of a cybersecurity certification framework. There is a need to reach maturity and deliver the service in order to demonstrate the value from the investment made and the engagement that stakeholders have demonstrated in relation to this service. Looking beyond the horizon, further resources will be necessary to further customise and support the emerging technology platform when the Commission makes it available to ENISA.

Key performance indicators	Unit of measurement	Frequency	Data source	Results
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				
6.1. Number of stakeholders (governments or commercial solution providers) in the EU market using the cybersecurity certification framework for their digital solutions^a				
Percentage of respondents planning to use the cybersecurity schemes to have solutions certified	%	Annual	Survey	24 %
Percentage of respondents planning to use the cybersecurity schemes to use certified solutions	%	Annual	Survey	37 %
Percentage of respondents planning to use the cybersecurity schemes to certify solutions	%	Annual	Survey	44 %
Percentage of respondents referring or planning to refer to certifications within regulations	%	Annual	Survey	36 %
Percentage of respondents planning to use the EUCC	%	Annual	Survey	53 %
Percentage of respondents planning to use the EUCS	%	Annual	Survey	49 %
Percentage of respondents that need assistance from ENISA in their process of preparation for using the EU certification schemes	%	Annual	Survey	66 %
6.2. Citizens' trust in digital solutions		Biennial	Survey	N/A
6.3. Satisfaction with ENISA's support for the preparation of candidate schemes		Biennial	Survey	N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	12	Actual used FTEs		6.72
Planned budget (direct costs only)	EUR 870 000	Consumed budget (direct costs only)		EUR 518 020
		Of which carried over to 2022		EUR 59 093

N/A, not applicable.

- a Activity 6 KPIs implicitly require the adoption of a cybersecurity certification scheme, and due implementation over time in an environment that benefits informed users. As the cybersecurity certification framework remains in its early stages, ENISA obtained responses through a survey concerning the intention of the respondents to use a scheme. The responses are varied but should be regarded as favourable on balance because a significant portion of the market views positively the prospect of an EU certification scheme and intends to benefit from it when it becomes available. In the future, when a scheme is adopted and following user education, the response rate is likely to change.

ACTIVITY 7

Supporting the European cybersecurity market and industry



Under Activity 7, ENISA served the strategic objective of a ‘high level of trust in secure digital solutions’ by launching the cybersecurity market outputs; meaningfully associating standardisation and certification, notably on 5G standardisation; analysing the prospective cybersecurity label; and reporting on vulnerabilities for certified products, services and processes. As announced by European Commission President von der Leyen in her State of the Union Address in September 2021, the Commission was to proceed with an act to establish common cybersecurity rules for digital products and associated services that are placed on the market across the European Union. ENISA contributed to this broader policy goal by analysing the cybersecurity market of connected devices.

Achievements

ENISA kicked off the cybersecurity market output in an effort to gain a meaningful role in a new analysis and recommendations domain. ENISA reasserted its position in the area of standardisation with a newly implemented approach to private standardisation organisations, and further collaboration with European standardisation bodies; meaningful content was developed to mark gaps. ENISA also developed a concept for a cybersecurity certification label, based on an analysis; it also launched a discussion forum that contributes to the analysis of vulnerabilities for certified products, services and processes. While certification remained a background theme across these outputs, ENISA sought to service other priorities of the Agency under Activity 7, notably risk assessment, connected devices and cooperation with policy and awareness raising. Achievements include:

- a market analysis framework and implementation thereof on connected devices;
- reviews of risk assessment and 5G standards (including O-RAN);
- an analysis of cybersecurity labelling approaches;
- guidance on vulnerabilities of certified products, services and processes.

Resources

With three outputs out of four being new, delivering on Activity 7 remained a challenge. Outputs 7.1 and 7.2 could potentially benefit from a reshuffle of in-house capacity to provide the resources needed in order to meet the requirements.

Appropriations carried forward served the purpose of responding to policy priorities of the Commission and thus the Agency in relation to the European Digital Identity Wallet; subsequently deliverables are expected in early 2022. A small amount was directed towards the annual standardisation conference that takes place in Q1, while most arrangements are sorted out beforehand. The amount carried forward does not negatively affect the ability of the unit to perform its tasks in 2022.

Overall assessment

Under the CSA, Activity 7 can gradually grow, should cybersecurity market analysis start covering broader areas and shift to a transversal service pattern. Standardisation has equally strong potential to delve into a dense set of requirements and enhance the ability of the Agency to influence cybersecurity standards in fulfilling its role in cybersecurity certification. Both these areas could benefit from a moderate increase in resources to better cope with the growing demand of stakeholders for analytical market data and a flow of standardisation requirements alike. Further adjustments concerning output 7.3 could allow best practices to be transversely analysed and proposed to stakeholders across the market, certification and standardisation, and outreach policy areas (e.g. the European cybersecurity index). With regard to output 7.4, which serves, inter alia, the purpose of a discussion forum on its subject matter, no changes are proposed hereinafter, except for a modest adjustment in resources, as appropriate.

Objectives



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

Link to strategic objective (ENISA strategy)



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

Results



- Where relevant, contributions towards a more competitive European cybersecurity industry, small and medium-sized enterprises (SMEs) and start-ups

Outputs



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

Outcome



ENISA initiated its activities in analysing the cybersecurity market, with the aim of contributing to a more targeted, market-driven decision-making process for the conception, launching and maintenance of cybersecurity products, services and processes within the EU. The Agency developed the ENISA cybersecurity market analysis framework, which describes how EU cybersecurity market analyses can be performed, and it has been introduced as a building block to be gradually developed further.

- ENISA carried out an analysis of the supply of and demand for internet of things (IoT) cybersecurity in distribution grids, and made detailed suggestions on how this market might further evolve, as a proof of concept.
- During the reporting year, the Agency also established the AHWG on the EU cybersecurity market, which is supporting ENISA in analysing market trends and segments, with a focus on cybersecurity solutions to meet the dynamic market needs of stakeholders: ENISA Cybersecurity Market Analysis Framework (ECSMAF) (<https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf>); EU Cybersecurity Market Analysis – IoT in Distribution Grids (<https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid>); call for the establishing of the AHWG on the EU cybersecurity market (https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-cybersecurity-market).

The market analysis output has the potential to become a flagship activity and the centre of gravity of a range of analyses, data feeds and stakeholders' involvement, across a range of target market areas. The market analysis framework, slightly revisited, could remain the centrepiece, while focus would shift across focal areas. A small but focused range of services could be developed thereafter. An annual conference could bring stakeholders together in a flexible arrangement.

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

ENISA also endeavoured to fulfil its tasks on standardisation as follows.

- It developed a rapport with European standardisation organisations / standards development organisations / private initiatives. ENISA implemented the tasks stemming from its standardisation strategy, in particular through activities whereby ENISA acts as an agent influencing standardisation and as a collaborating partner to the standards development organisations and initiatives. Concrete action consisted in launching or tightening relations with relevant technical committees of standardisation bodies (European Telecommunications Standards Institute technical committees on cybersecurity and on electronic signatures and infrastructures; CEN-CENELEC Joint Technical Committee 13; International Organization for Standardization (ISO) / International Electrotechnical Commission subcommittee 27; International Digital Cooperation project on ICT standardisation), and with private initiatives (GSMA, 3rd Generation Partnership Project, Global Platform), and organising in collaboration with the European Telecommunications Standards Institute and CEN-CENELEC the cybersecurity standardisation conference (over 2 400 registrations) and participation in others. The Agency was active in the development of the rolling plan for ICT standardisation, and the feasibility study of the future standards in support of the CSA, and proposed to the standardisation community new work items for specific standards supporting certification, which were accepted by CEN-CENELEC Joint Technical Committee 13 (methodology sectoral cybersecurity assessment; EUCS controls; accreditation criteria).
- Analysis of standardisation requirements – risk management. ENISA drew up a coherent overview of published risk management standards addressing aspects of risk management and subsequently describing methodologies and tools that can be used to conform with or implement them. Based on a comprehensive inventory of standards in the area, the study provides guidance on their availability and outlines possible gaps, proposing concrete activities to close these gaps (<https://www.enisa.europa.eu/publications/risk-management-standards>).
- Analysis of standardisation requirements – 5G. The Agency prepared a study on 5G standards, in parallel with the preparations for the work on 5G certification scheme. The ambition of this report was to outline the contribution of standardisation to the mitigation of technical risks, and therefore to trust and resilience, in the 5G ecosystem, understood as a multidimensional space encompassing not only technological and functional domains, but also the related technology life-cycle processes and stakeholders (<https://www.enisa.europa.eu/publications/5g-cybersecurity-standards>).
- The Agency produced a study on O-pen-RAN standardisation, focusing on the specification development process in this area. The study was initiated at the request of the Member States and the Commission.

Standardisation has been a flagship activity and it is fortunate that it has gradually been integrated with certification. Further fusion between these two areas will certainly assist reaching better policy outcomes and benefit the cybersecurity certification framework. The annual conference serves as a stakeholder platform to pass key messages about cooperation and content.

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

In terms of labelling for EU cybersecurity certification, ENISA drew up key requirements and consolidated experience from other similar initiatives concerning cybersecurity labels. This stands as a first step towards labelling for certified ICT products, services and processes. Around 50 stakeholders supported a dedicated thematic group, and this output was presented to and discussed by ENISA governing bodies (ECCG, SCCG, national liaison officers (NLOs)).

At the ENISA 2021 cybersecurity certification conference, a panel discussed current IoT labelling initiatives and monitoring developments beyond the EU; views were also exchanged with the National Institute of Standards and Technology.

While labelling is reaching a turning point, good practices have the potential for dynamic growth across a range of areas. This adjusted output, remains for this purpose.

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

In terms of vulnerabilities of certified ICT, ENISA assessed the impact of certification on the handling of vulnerabilities, from the CVD process and certification status points of view. A thematic group supported this output, and it identified the complete set of requirements related to vulnerability handling in the CSA, certification schemes (EUCC, EUCS), NIS and relevant standards. Two scenarios were developed to analyse the gaps between the different requirements and to define a roadmap. The AHWGs' joint session and the ENISA governing bodies (ECCG, SCCG) had an opportunity to review and comment on this output.

While low key, this output remains topical in the market and certification area; as it is fit for purpose, no changes are expected.

Key performance indicators	Unit of measurement	Frequency	Data source	Results
Recognition of ENISA's supporting role for participants in the European cybersecurity market ^a				
7.1. Number of market analyses, guidelines and good practices issued by ENISA				
Cybersecurity market analysis framework	Number	Annual	Reports	2
7.2. Uptake of lessons learned / recommendations from ENISA reports				
Percentage of respondents interested in using ENISA's good practice on market analyses	%	Annual	Survey	87 % high and medium interest
Percentage of respondents interested in using ENISA's standards mapping related to 5G	%	Annual	Survey	84 % high and medium interest
Percentage of respondents interested in using ENISA's standards mapping related to the IoT	%	Annual	Survey	88 % high and medium interest
Percentage of respondents interested in using ENISA's risk-based approach for their cybersecurity certification activities	%	Annual	Survey	72 % high and medium interest
Percentage of respondents interested in using ENISA's consolidated certification labelling process	%	Annual	Survey	84 % high and medium interest
Percentage of respondents interested in using ENISA's vulnerability management process for certified products, services and processes	%	Annual	Survey	82 % high and medium interest
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work	%	Biennial	Survey	N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	9	Actual used FTEs		6.50
Planned budget (direct costs only)	EUR 490 000	Consumed budget (direct costs only)		EUR 450 894
		Of which carried over to 2022		EUR 69 996

N/A, not applicable.

- a The KPIs of Activity 7 allow the Agency to reaffirm its role and obtain feedback on its efforts to take a new standpoint on cybersecurity. ENISA has built a long-standing relationship with stakeholders on cybersecurity standardisation, and the outcome permeates through the results of the survey in terms of stakeholder value.



ACTIVITY 8

Knowledge on emerging cybersecurity challenges and opportunities



This activity intends to provide 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 objective of efficient and effective cybersecurity information and knowledge management for Europe, the activity builds on aggregating and analysing information across the ecosystem (legal, regulatory, technical, societal, etc.), and leverages expertise to provide relevant analyses. In doing so, information from other activities (e.g. NIS investments under Activity 1, output 1.1, incident reporting under Activity 2, output 2.5, and situational awareness under Activity 5, output 5.1) is consolidated under Activity 8 to promote relevant analyses and give recommendations. A prime example is the work on the cybersecurity index that will pull information from across all activities in order to assess the level of cybersecurity maturity of Member States. 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). 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

During the reporting period, ENISA worked on various fronts in terms of consolidating information, analysing it and providing analyses and recommendations to serve stakeholders' expectations. The Agency worked closely with the stakeholders' communities (one established and two new ad hoc working groups, as well as a subgroup of the NLO Network).

ENISA has set the grounds and followed a multiannual perspective in the delivery of Activity 8, engaging in the design of the EU cybersecurity index, the annual threat landscape and the supply chain attacks threat landscape, the methodology on identifying foresight challenges, the design of the information hub (infohub), the work on AI and securing machine learning. Besides, ENISA provided continuous support to the EU research and innovation agenda, and in particular to the ECCC, by helping with the identification of research and innovation priorities. All those projects have long-term plans and adhere to a service-oriented approach to cater for 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 (threat landscapes and cybersecurity index) to understand the *status quo* and identify trends for the future (foreseen and emerging challenges), and use 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). The multiannual perspective followed in Activity 8 (with works on foresight, the cybersecurity index and the infohub in particular), having a 3-year time horizon, was necessary to allow a level of maturity to be attained internally. These particular works were new to ENISA and in this respect – and to allow for synchronisation between the various pieces of work – adequate time was needed to allow ENISA to build its capabilities, and to allow acceptance by the Agency's stakeholders to grow steadily and in a participatory manner. Both latter aspects of stakeholder engagement are deemed necessary for the successful implementation of and buy-in to projects such as the cybersecurity index and the infohub.

Accordingly, targeted information and recommendations are provided to stakeholders at various levels and in a timely fashion to support decision-making and ensure that a solid and future-proof view of cybersecurity is taken into account. The timeliness of the information is an area that can be further improved, by moving towards real-time mapping of the cybersecurity threat landscape, which would require additional efforts on the part of

ENISA to continuously analyse and identify recommendations. Along these lines, the agency is working towards consolidating information from output 2.5 (annual incident reporting) with other information sources, mostly open-source, frequently used in the mapping of threat landscapes, and will streamline relevant efforts towards the consolidation of information.

In identifying the complex nature of outputs under Activity 8 (e.g. output 8.1 addresses the cybersecurity index, foresight and recommendations on future and emerging challenges), already in the 2022 SPD the Management Board of ENISA undertook corrective actions to make the structure more lean and appropriate to satisfy its strategic objectives. In addition, realising the opportunity for synergies with the work on incident reporting under Activity 2 (output 2.5), already in 2022 this work will be considered under Activity 8 to promote cross-fertilisation and integrated knowledge management concerning the threat landscape. More opportunities concerning the streamlining of knowledge management exist, notably with the work on situational awareness under Activity 5, and the Agency is internally promoting closer ties between the two work streams by means of consolidated tooling requirements and by exploring the potential of common analysis techniques.

Resources

Budget implementation for Activity 8 reached 95 % at the end of the reporting year. Considering the impact of the pandemic on the planning of physical events and travel expenses linked to business travel, this implementation came as a very positive result for the Agency.

In terms of FTE resources, Activity 8 faced the challenge of having two horizontal teams, with team members contributing various percentages towards the team and one operational unit working together to meet the objectives.

The KPIs of Activity 8 are diverse in nature. 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 2021, since only the design of the infohub and the knowledge management framework were introduced in 2021. KPI 8.2 assesses the quantity and depth of ENISA's work in terms of analyses, challenges and recommendations. With an average of 36 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 involves a biennial stakeholder satisfaction survey, which will be held at the end of 2022.

Overall assessment

Activity 8 met its objectives during the reporting year. KPIs revealed that ENISA had a notable impact in identifying recommendations, analyses and challenges, and that it delivered the expected results. However, the objective of increasing Member State and EU resilience and preparedness for handling future cybersecurity challenges and opportunities remains difficult to assess. At this point in time, the Agency expects the EU cybersecurity index to serve as a benchmark and to therefore help assess how this objective will be met in the future. ENISA expects to analyse and process the results of the cybersecurity index, although more resources will be required than those of 2021, in order to develop and maintain the index during the coming years.

Objectives



- Identify and understand future cybersecurity challenges and opportunities, and assess the interlinks between cybersecurity and relevant disrupting technologies in the current and future digital transformation
- Increase the resilience and preparedness of Member States' and the EU's in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities

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 policymaking and decision-making

Outputs



8.1. Identification, collection and analysis of present and emerging challenges (e.g. technological, economic or societal) in cybersecurity (including developing and maintaining a European Cybersecurity Index)

Outcome



- In 2021, ENISA commenced work on designing, developing and maintaining a European Cybersecurity Index. A multi-annual plan was launched, including the design and development, the piloting, and eventually the deployment and maintenance of the index. A dedicated subgroup of ENISA's NLO Network was established to continuously engage with the Member States.
- In 2021, ENISA worked together with Member States and delivered the following internal reports and studies:
 - analysis of existing cybersecurity capabilities assessment frameworks and indexes;
 - a set of EU cybersecurity indicators;
 - empirical validation of indicators and domains;
 - the EU Cybersecurity Index Framework version 1.0 (a 'live' document);
 - requirements for cybersecurity index supporting tools.
- Concerning analysis of present and emerging challenges, in the course of 2021 ENISA worked on two topics, namely AI and cryptology with a focus on post-quantum cryptography (PQC). To this end, with the support of the ENISA ad hoc AI working group, the Agency delivered a report on securing machine learning algorithms, following up from the recommendations of the ENISA AI threat landscape that was published in 2020. With regard to cryptology, the Agency worked on the issue of post-quantum integration and crypto assets, and relevant reports will be published in 2022.

- In 2021, ENISA laid the foundations for foresight, namely to identify, collect and analyse present and emerging challenges across various dimensions (e.g. technological, economic or societal). To this end, the Agency established an ad hoc working group on foresight for emerging and future cybersecurity challenges.
- In 2021, ENISA worked with the Foresight Working Group and the futures and foresight community to develop a methodological process to apply foresight to cybersecurity. The result of this work was published and will serve as guidance for the foresight efforts of ENISA and other cybersecurity organisations in the future.
- Securing Machine Learning Algorithms (<https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>).
- Foresight Challenges (<https://www.enisa.europa.eu/publications/foresight-challenges>).

Output 8.1 addresses the cybersecurity index, foresight and recommendations on future and emerging challenges. Already in the 2022 SPD the Management Board of ENISA undertook corrective actions to make the structure leaner and more appropriate to satisfy its strategic objectives. Accordingly, the work on the index will be part of a dedicated output, and the work on foresight and emerging challenges also has a dedicated output in the 2022 SPD.

8.2. Provide targeted as well as general reports, recommendations, analysis and other actions in relation to future cybersecurity scenarios and threat landscapes (incident response landscape mapping for NIS directive sectors)

During 2021, ENISA restructured the delivery of threat landscapes by establishing an ad hoc working group on cyberthreat landscapes and laying the groundwork for a transparent and public methodology. By incorporating a plethora of cyberthreat intelligence sources and following a service-oriented approach, the work on threat landscapes increased in confidence.

- In 2021, the ENISA Annual Threat Landscape was published for the ninth time and an additional thematic threat landscape on supply chain attacks was also published:
 - ENISA Threat Landscape 2021 (<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>);
 - ENISA Threat Landscape for Supply Chain Attacks (<https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>).
- Building on its work on supporting operational cooperation across EU over recent years, in 2021 ENISA conducted a study on mapping incident response capabilities and developments in a sector to which the NISD dedicates attention, namely the healthcare sector. The report provided practical recommendations on future developments in incident response in the healthcare sector:
 - CSIRT Capabilities in Healthcare Sector (<https://www.enisa.europa.eu/publications/csirt-capabilities-in-healthcare-sector>).

The work on threat landscapes was highly appreciated by the stakeholders and contributed greatly to the strategic objective of efficient and effective knowledge management in Europe. Realising the opportunity for synergies with the work on incident reporting under Activity 2 (output 2.5) has already been integrated into Activity 8 during the 2022 work programme to promote cross-fertilisation and integrated knowledge management concerning the threat landscape.

8.3. Develop and maintain a portal (information hub), a one-stop shop for organising and making available to the public information on cybersecurity, and establishment of a procedural framework to support knowledge management activities

ENISA opted for a multi-annual approach to deliver the infohub. In 2021, the agency established an initial procedural framework to support the knowledge management activities of a future infohub. This included the development of relevant taxonomies, templates and potential processes for knowledge acquisition and validation, setting out the baseline procedures and processes that will be considered for integration in the technical specifications upon which the development of the prototype portal will be built.

Moreover, during 2021 ENISA carried out the identification of leading best practices among existing cybersecurity knowledge management frameworks and information portals, with 81 individual knowledge resources analysed. Based on lessons learned and the scoped leading-practice experience, inferred through surveys and interview sessions, key potential components of the infohub's structure have been identified, feeding into the design of a procedural framework.

For the validation of the work and to increase acceptance, ENISA engaged stakeholders from 13 Member States through one workshop, three surveys and eight interviews. Moreover, NLOs and experts from the European Cybersecurity Atlas were also engaged in this activity and provided input and comments.

When it comes to the infohub (output 8.3), further efforts should be pursued to better establish the ties between the infohub and consolidated knowledge management and awareness-raising activities. Such efforts would greatly contribute towards achieving the strategic objective of empowered and engaged communities across the cybersecurity ecosystem.

8.4. Support EU research and development programmes and activities of European competence centres, including the four EU pilot projects for the European Cybersecurity Competence Centre and Network of National Coordination Centres

During 2021, ENISA consolidated and analysed the proposals and recommendations of the four pilot projects and the European Cyber Security Organisation, supporting the European Commission to prepare input for future discussions on the ECCC strategic agenda.

In 2021, ENISA identified research and innovation needs and priorities in the fields of life science, cryptography, AI and hyperconnectivity, with the goal of preparing future funding priorities for the ECCC.

Efforts related to research and innovation under output 8.4 need to be better streamlined to reflect the recent policy developments with the establishment of the ECCC. In 2021, efforts on both research and innovation priorities for the cybersecurity agenda of the EU and support for the ECCC were bundled under one output, and corrective actions were already taken in the 2022 SPD to split these into distinct lines of work.

Key performance indicators ENISA's ability to contribute to Europe's cyberresilience through the provision of timely and effective information and knowledge	Unit of measurement	Frequency	Data source	Results
8.1. Number of users and frequency of use of a dedicated portal (observatory)			N/A	
8.2. Total number of recommendations, analyses and challenges identified and analysed (reports)	Number	Annual	ENISA reports and studies	288
Threat landscape supply chain	% of total	Annual	ENISA reports and studies	13 % (37 of 288)
Foresight	% of total	Annual	ENISA reports and studies	6 % (17 of 288)
ENISA threat landscape report 2021	% of total	Annual	ENISA reports and studies	46 % (132 of 288)
Crypto assets	% of total	Annual	ENISA reports and studies	0.3 % (1 of 288)
Securing machine learning	% of total	Annual	ENISA reports and studies	19 % (55 of 288)
Cybersecurity index	% of total	Annual	ENISA reports and studies	10 % (29 of 288)
PQC integration	% of total	Annual	ENISA reports and studies	0.3 % (1 of 288)
Healthcare CSIRT	% of total	Annual	ENISA reports and studies	4 % (12 of 288)
8.3. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research		Biennial	Survey	N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	9	Actual used FTEs		7.36
Planned budget (direct costs only)	EUR 1 155 000	Consumed budget (direct costs only)		EUR 1 096 980
		Of which carried over to 2022		EUR 1 200

N/A, not applicable.

ACTIVITY 9

Outreach and education



The aim of this activity is to empower and engage stakeholders through building awareness of cybersecurity issues and good practices. The activity also focuses on creating an international position for ENISA in the cybersecurity ecosystem.

Overall, the concept of behavioural change towards cybersecurity requires persistent long-term effort, well-defined objectives, an identified target group, and ultimately specific and relevant metrics and indicators.

Achievements

The deliverables of the team for 2021 were mostly internal, to create the stable foundation for all the awareness activities the Agency will undertake in the coming years. Specifically, the team worked on:

- the ENISA stakeholder strategy, a massive exercise of consolidating feedback and information from across all ENISA units and teams, but also from external stakeholders, in a holistic inclusive framework;
- the awareness-raising framework, a set of processes and requirements for organising an awareness-raising campaign and programme, including all necessary steps to communicate the right messages;
- the promotion and dissemination strategy, presenting the most effective means and channels to use for each target audience and some advice on how to increase outreach to the community.

These documents were not published, as they are intended for internal use.

The outreach projects focusing on external stakeholders under this activity concern numerous large- and small-scale campaigns; more specifically:

- the European Cybersecurity Month (ECSM), the flagship pan-European cybersecurity awareness campaign, which increased its outreach;
- the thematic campaigns on several cybersecurity topics (i.e. ransomware and certification; creating synergies; and long-term objectives).

The multidisciplinary nature of the awareness-raising and education team helped create good and strong collaboration points, and identified new synergies with the work of the other units.

Finally, to engage the stakeholder communities, under this activity the ad hoc working group on awareness raising, composed of experts, was created as well as the enterprise security group focusing on SMEs. The terms of reference for the ECSM coordinators group were drafted and approved by the group itself.

Resources

Concerning resources, Activity 9 had a budget utilisation of 95 %, which is assessed as being positive given the pandemic and the impact it had on the planning of physical events and travel expenses. In terms of FTE resources, Activity 9 is challenged by the team's specific nature, with colleagues coming from different units or other teams and therefore not fully involved timewise. Even if such a team obviously presents opportunities for synergies, it inevitably means lack of ownership of, commitment to and responsibility for the team projects. With regard to carry-over of funds, certain outputs take place late in the year, so delivery of those projects took place in 2022, and in other cases such as the ICC the entire project was postponed as a result of the COVID-19 pandemic. The ARET would benefit from more resources to support existing projects (heavily needed under the OES campaigns to achieve the goal of behavioural change) but also to offload support provided by other sectors of the Agency such as the communications sector. Approximately 30 % of the resources focused on internal projects (including the international strategy).

Overall assessment

Overall, the outputs under this activity contributed into the strategic objective of empowered and engaged communities, although at this stage it remains unclear to what extent the relevant communities are engaged and empowered – a situation that should be clarified in the 2022 annual activity report, as the stakeholder strategy implementation plan sets up a process to monitor and evaluate the actual engagement of stakeholder groups under all activities in the annual activity report.

With regard to the current KPIs, they are all geared to measuring engagements during different awareness-raising campaigns, but that might not give a full picture of actual impact or added value, even if one compares similar results in the coming years. Thus, the second KPI should be further refined to offer insights on the effectiveness of ENISA projects at raising awareness, as the current proposal cannot derive conclusions on the specific ENISA outputs.

A proposal for a new output under this activity is also put forward to combine all activities of the Agency that relate to education, thus absorbing output 3.8 on the skills framework and also the task that will be created under the cybersecurity educational roadmap.

Objectives



- 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 an ENISA stakeholder strategy and undertake actions for its implementation

Outcome



During 2021, under this output the team conducted two projects.

- The stakeholder strategy package, a set of documentation that includes the stakeholder strategy (to be published), the implementation guide, the management plan and the requirements for tooling. All documents are to be used internally to support a structured approach to stakeholder engagement and management in the Agency.
- The awareness-raising conceptual framework, the basis for future ARET campaign development. The framework outlines the life cycle of awareness campaigns and awareness-raising programmes, including a detailed plan for evaluation. During the collection of project feedback, stakeholders expressed great interest in seeing a public version of the framework – view that is reflected in the 2022 SPD.

None of the documents is publicly available. A public version of the ENISA stakeholder strategy will be published in 2022.

This output was replaced in the 2022 SPD with the task of seeking to achieve behavioural change for OESs.

9.2. Develop an ENISA international strategy and outreach activities

In February 2021, the ENISA task force for international cooperation was set up and tasked with drafting the ENISA international strategy. Based mainly on the input from the Member States, the strategy was developed and adopted by the ENISA Management Board in November 2021 (<https://www.enisa.europa.eu/publications/corporate-documents/enisa-international-strategy>). The ENISA international strategy covers cooperation with non-EU countries and with international organisations. It sets out the principles governing ENISA's international cooperation, and sets out three different approaches (limited, assisting and outreach) that the Agency can use in terms of its level of engagement and commitment of resources.

In 2021, ENISA received several requests for international cooperation and accommodated a number of them. For instance, it provided assistance in the context of some cyber dialogues with non-EU countries and contributed to international events organised by the Council of Europe, such as the 2021 Octopus Conference ([https://www.coe.int/en/web/cybercrime/octopus-interface-2021#%22106157651%22:\[10\]](https://www.coe.int/en/web/cybercrime/octopus-interface-2021#%22106157651%22:[10])).

In 2021, ENISA laid the ground work international outreach activities by formulating and publishing its first international cooperation strategy through a cross-unit task force. In 2022, the international team (INT) published the international strategy implementation guidelines and it is working on creating synergies with the Agency's operational units and with Commission and EEAS services, and it has created a roadmap for the Agency's international partnerships. It will also release an annual report on the Agency's international cooperation as defined in the international strategy. INT will continue to provide services to the Agency's operational units in 2022 and onwards, to fulfil its strategic intent.

9.3. Organise the ECSM

The 9th edition of the ECSM saw great increase in outreach; for the first time June was also included as a promotion month for the ECSM activities, and the winning team of the ECSC announced the ECSM's inauguration and became ECSM ambassadors.

The campaign had two themes: Be Cyber Secure from Home (cyber hygiene and good practices for online presence) and Cyber First Aid (guidance when citizens are victims of cyberattacks). Twenty-six Member States actively participated in the campaign, conducted national campaigns and participated in the evaluation of the ECSM. An interactive EU map was created in collaboration with the national campaign coordinators, on which citizens can find what services are available in their country so they may ask for advice and help should they fall victim to a cyber incident. Ambassadors and, in general, the concept of multipliers are fundamental to achieve greater outreach and to overcome the language barrier and the culture gap. ECSM activities were given a boost by having the winning ECSC team launch the campaign, and by Member States' efforts to approach national celebrities to promote the campaign in their countries.

In 2021, a concept was created for measuring the impact of the campaign and its effect on behavioural change. It will be tested and deployed in 2022.

The ECSM 2021 deployment report can be found online (<https://www.enisa.europa.eu/publications/european-cybersecurity-month-2021-deployment-report>).

The ECSM continues for the 10th year in 2022. Overall, this is a highly appreciated project, and Member States see great value in ENISA's coordinating actions. ENISA should further reflect on spreading activities throughout the year, achieving a peak in October. The output should remain as is for the 2023 SPD.

9.4. Organise the International Cybersecurity Challenge

Because of the COVID-19 pandemic and the restrictions imposed by the Greek government on events organised indoors, the ICC event was postponed to June 2022. Despite the COVID-19 restrictions, ENISA was able to expand the steering committee of the ICC, which now comprises more than 100 people from 64 countries. ENISA organised monthly meetings in which all ICC teams participated actively throughout 2021.

The Agency also designed logos for ICC and the EU team, identified sponsors for the event, developed a media strategy and established the platforms that will host the ICC challenges in June 2022. Furthermore, all the administrative issues (venue, catering and transportation needs for teams, website, merchandise, awards for the winning teams, invited guests) were completed in 2021, ensuring a successful event in 2022.

ENISA was responsible for forming and training the EU team to enter the ICC. To this end, ENISA formed a pool of 55 candidates from 21 Member States and organised two training events, which took place in Tallinn and Turin, in which the vast majority of the EU team candidates participated. In these events, ENISA provided training on multiple modules (cryptography, forensics, mobile exploitation, web exploitation, reverse engineering, attack and defence, and ethics).

It is imperative that ENISA continues its involvement in the ICC, as ENISA has:

- successfully managed to have all seven teams travel to participate in the 2022 ICC (more than 65 countries provide participants in these teams);
- streamlined the 2023 ICC (it will be hosted by the Cybersecurity and Infrastructure Security Agency in the United States, probably during Black Hat in Las Vegas), and there are already nominations for the 2024 and 2025 ICCs (nations from Oceania and Africa);
- will continue to be responsible for handling the ICC steering committee and guiding the rules and governance of ICC;
- will need to train and form the EU team that will take part in the 2023 ICC, commencing this activity from July 2022;
- engaged with sponsors that are interested in capacity building globally (ISACA and Northern Ireland Co-operation Overseas (NiCo), which has funding from the EEAS) and is assisting developing countries in creating and participating in capture the flag's.

9.5. Activities to promote and ensure the uptake of information on good cybersecurity practices (including on EU strategies, security by design and privacy by design at EU level, and cybersecurity certification schemes) by different target groups

The projects under this activity comprised thematic campaigns and the deployment of a supporting framework (for internal use):

- publication dissemination and promotion strategy for awareness-raising providing pragmatic steps to define, address and evaluate awareness-raising campaigns (report for internal use);
- two in-house campaigns and three campaigns in collaboration with other EU institutions:
 - in-person awareness-raising campaign for SMEs, highlighting the SME tool, report and booklet on best practices for SMEs, and with the additional goal of understanding the ecosystem of SMEs and how to reach SMEs and raise their awareness;
 - an awareness-raising campaign on certification called ‘What’s In It for the Conformity Assessment Bodies?’ aims to empower these key players in future EU certification through a short video and frequently asked questions;
 - #NoMoreRansom with Europol to raise awareness of ransomware through a dialogue led on Twitter;
 - #Women4Cyber and #CyberBecause in collaboration with the Commission to invite women and students to choose cybersecurity careers.

The analysis of the results of each campaign indicate that a systematic approach and proper planning is the key. Given this, ENISA will continue projects launched in 2021 through the coming years, focusing each year on another target audience. For 2022, the continuation of these campaigns is already planned, with an earlier coordination of contributors and more resources dedicated to them.

The output should be continued, as it reflects the tasks of the CSA on awareness and promotion of cybersecurity practices. The educational roadmap is also included as a project under this output, which we advise maintaining for the 2023 SPD as a separate output.

Key performance indicators	Unit of measurement	Frequency	Data source	Results
Level of awareness of cybersecurity, cyberhygiene and cyberliteracy across the EU				
9.1. Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics				
Women4Cyber campaign				
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	201 188
Social media engagements	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	3 865
Video views	Number	Annual	YouTube	1 283
Cybersecurity for SMEs campaign				
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	44 497
Social media engagements	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	957

Key performance indicators Level of awareness of cybersecurity, cyberhygiene and cyberliteracy across the EU	Unit of measurement	Frequency	Data source	Results
Video views	Number	Annual	YouTube	736
Website visits	Number	Annual	ENISA website	24 362
Media references	Number	Annual	Media monitoring	~ 40
Participation in events	Number	Annual	Website announcements	5
NoMoreRansom campaign				
Social media impressions	Number	Annual	Social media (Twitter)	54 022
Social media engagements	Number	Annual	Social media (Twitter)	465
ECSM campaign				
Social media impressions	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	20 400 000
Social media engagements	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	110 266
Video views	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	2 018 441
Website visits	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	47 939
Certification campaign				
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	85 599
Social media engagements	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	1 701
Video views	Number	Annual	YouTube	669
Website visits	Number	Annual	ENISA website	1 239
CyberHEAD campaign				
Social media impressions	Number	Annual	Social media	25 292
Social media engagements	Number	Annual	Social media	466
Website visits	Number	Annual	ENISA website	49 964
9.2. Level of awareness of cybersecurity across the EU / general public (e.g. EU barometer)	Biennial			N/A
Allocated FTEs as per SPD based on full establishment at year-end 2021	6	Actual used FTEs		Actual: 5.10
Planned budget (direct costs only)	EUR 1 010 000	Consumed budget (direct costs only)		EUR 933 693
		Of which carried over to 2022		EUR 399 768

N/A, not applicable.

ACTIVITY 10

Performance and risk management



Achievements

Internal process guidelines (SOPs) for developing and implementing the SPD were adopted internally in 2021 and are being applied as of 2022. This is important, as it creates a uniform understanding of how to ensure best performance and manage risks. It also solidifies the role of NLOs and the ENISA Advisory Group in the scoping and validation of outputs and deliverables.

The Agency also developed and put in place a framework for evaluating the allocation of its HR and reviewing this annually, to be able to reassign resources in an agile fashion in line with its operational priorities. This should further strengthen the Agency's performance management and planning.

In addition, the Agency prepared for the roll-out of a new document management system (Advanced Records System (ARES)) by signing a service level agreement (SLA) with the Directorate-General for Informatics. The testing and final implementation of ARES are expected to take place in 2022; this, along with the established internal IT strategy, intellectual property rights (IPR) strategy and sensitive posts policy, helps to better mitigate any administrative risks.

Resources

The continuation of a number of projects had to be carried forward to 2022, such as the revision of the business continuity plan and ENISA website revamp, because of internal human resource constraints, in particular legacy aspects, duty of care and projects initiated in 2020 without clear internal support. Weaknesses in internal controls found by the European Court of Auditors (ECA) in 2020 resulted in reassessment of staffing needs to support this function in the course of 2021, which will be further implemented in the course of 2022.

Overall assessment

The structure of Activity 10 supports the mandate of the Executive Director's Office. The KPIs in relation to the performance management framework needs better alignment with the staff survey to allow broader coverage of its dimensions. In 2022 a new output was introduced to better outline the corporate communications strategy. Since the Executive Director's Office also supports the secretariats of several statutory bodies – namely the Management Board, the Executive Board, the Advisory Group and the NLO Network – a separate output could be considered to better reflect resource needs for this task.

Objectives



- Increase effectiveness and efficiency in achieving the agency's objectives
- Make the performance of ENISA fully compliant with legal and financial frameworks (build a culture of compliance)
- Protect the agency's assets and reputation, while reducing risks

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.** Roll out an Agency-wide performance management framework and systems across its functions

Outcome



At the end of 2020, ENISA had developed a performance management roadmap with five dimensions. In 2021 the following initiatives were undertaken within each dimension.

- External stakeholders dimension: stakeholder strategy project begun in 2021 and expected to be delivered in 2022 by ARET.
- People and capabilities dimension: strategic workforce review initiated and concluded in 2021 by Corporate Support Services. As part of this dimension under the constraints of the working regime during the COVID-19 pandemic, emphasis was put on developing internal communication, in particular to support remote work. Regular online meetings with staff were organised, including introducing the ENISA Academy to facilitate internal knowledge building.
- Organisation culture dimension: continuous information flow by the Communications sector via weekly question and answer sessions and intranet notifications among others.
- Internal processes dimension: evaluation of ENISA tooling needs carried out in 2021 by Executive Director's Office. Implementation of the new project management tool is expected in 2022. In addition, the preparation for ARES included the development of a filing plan and special retention list for documents.

The outcome of the work conducted in 2021 provides a basis for improving performance across the agency in both operational and corporate areas. The implementation of these roadmap dimensions, namely internal processes and costs and benefits, will continue in 2022 by complementing an overall corporate strategy to be developed in coordination with Activity 11. The roll-out of this output should also continue in 2023 with an assessment by the end of 2022 of whether the scope should be revisited.

- 10.2.** Develop, establish and implement a risk management plan and systems, including an anti-fraud strategy, a conflict of interest policy, a whistleblowing policy, an information security policy, an anti-harassment policy and an IPR policy

The main achievements in 2021 were:

- ENISA's anti-fraud strategy was updated and adopted (Management Board Decision MB/2021/5); a dedicated anti-fraud website is available on ENISA's intranet for all staff;
- ENISA's conflict of interest policy was updated and adopted (Management Board Decision MB/2021/15);
- the revision of the ENISA's IT policy and procedural framework was kicked off, including the Agency's information security policy;
- the ENISA's IPR policy was developed, adopted and published online (<https://www.enisa.europa.eu/about-enisa/legal-notice/enisa-ipr-policy-public-version>);

- several specific risk assessments were conducted in different areas with a view to establishing lessons learned and recommendations for the future (e.g. in the areas of recruitment, IT security and incident management).

In 2021 the agency handled complaints to the European Ombudsman, reports and recommendations of the European Anti-Fraud Office, the ECA and the Internal Audit Service (IAS) as well as the legal aspects related to the implementation of ENISA's seat agreement with the host country, in accordance with the overview provided under the KPIs.

The Data Protection Officer provided advice on several operational and administrative matters, maintained the ENISA's register of processing activities, cooperated with the EDPS and contributed to the activities of the EUIs Data Protection Officers network (co-chair of Data Protection Officers–ICT Advisory Committee of the EU Agencies and Institutions Working Group).

ENISA has a full-time Information Security Officer, appointed since 2019, who coordinates its information security management system. ENISA's Information Security Officer contributed to several related activities in 2021, such as the ENISA annual security risk assessment exercise, regular vulnerability assessments and penetrations tests of ENISA systems, network security monitoring and incident response, advising on internal security policies, etc. The Information Security Officer works in close cooperation with the CERT-EU on the aforementioned matters.

Overall, the output in 2022 continues to maintain compliance aspects. Some work planned in 2021 was not completed, namely updating the whistleblowing policy and implementing the risk management plan and systems. In 2021 the main focus was on lessons learned, with a view to establishing a comprehensive risk assessment methodology for ENISA in the course of 2022. Output is adjusted in the 2022 work programme and should be continued in line with the results of ENISA's risk assessment, and the risk appetite and risk-mitigating measures defined by the ENISA Management Team in 2022.

10.3. Develop and implement an agency-wide IT strategy

An agency-wide IT strategy was developed and adopted.

The output will continue in 2022 with an emphasis on developing and updating several IT-related policies in close coordination with Activity 11, aiming to introduce the ISO 27001 standard at ENISA by the end of 2024.

10.4. Carry out relevant training and develop guidelines for staff

- Four internal courses on data protection (general data protection, procurement and cloud services, events, data protection by design) were held.
- Information security awareness training (via an external platform) took place.
- There was an information session on ENISA's IPR policy.
- Assistants trained ENISA newcomers in the use of internal tools and its financial cycle.
- Guidance was issued to staff on several implementation provisions of the Seat agreement with the Hellenic Republic.

- The output in 2021 focused on compliance and this will continue in 2022 with an emphasis on guidance for staff on ethics, conduct, tools and processes introduced as part of outputs 10.1 and 10.2.

Key performance indicators	Unit of measurement	Frequency	Data source	Results
Organisational performance culture				
10.1. Proportion of key performance indicators reaching targets				N/A
10.2. Individual contributions to achieving the objectives of the agency through clear links to key performance indicators (career development reports (CDRs))				
Policy development and implementation unit	%	Annual	Objectives 2021	100 %
Capacity building unit	%	Annual	Objectives 2021	23 %
Operation cooperation unit	%	Annual	Objectives 2021	85 %
Market, certification and standardisation unit	%	Annual	Objectives 2021	22 %
Executive Director's Office	%	Annual	Objectives 2021	47 %
Corporate support services	%	Annual	Objectives 2021	38 %
10.3. Exceptions in the risk register	Number	Annual	Internal control	16
Deviation from financial regulations	Number	Annual	Internal control	14
Deviation from staff regulations	Number	Annual	Internal control	2
10.4. Number of complaints filed against ENISA, including number of inquiries or complaints submitted to the European Ombudsman	Number	Annual	See below	19
To European Ombudsman	%	Annual	ENISA functional mailbox	16 % of 19
Under Article 90	%	Annual	Internal control files	79 % of 19
Under Article 24	%	Annual	Internal control files	0
To EDPS	%	Annual	Internal control files	5 % of 19
10.5. Results of the annual risk assessment exercise – see separate chapter on internal control framework PART III				
10.6. Observations from external audit bodies (e.g. ECA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings)	Number	Annual	See below	4
IAS	Number	Annual	IAS Section 2.7.1	Three important recommendations
ECA	Number	Annual	ECA Section 2.7.2	One critical observation
Planned budget (direct costs only: consultancy and business travel linked to Activity 10)	EUR 485 000	Consumed budget (direct costs only: consultancy and business travel linked to Activity 10)		EUR 454 443
Actual used FTEs	19.10	Of which carried over to 2022		EUR 257 589

N/A, not applicable.

ACTIVITY 11

Staff development and working environment



In 2021, ENISA implemented its wide ranging reorganisation plan, which saw the restructuring of its activities across operational and administrative areas. Newly appointed middle managers were asked to assist in bringing about meaningful outcomes as a result of the reorganisation. The new way of working and operating under a matrix set-up brought out a lot of knowledge-sharing opportunities and steered the agency resources towards a first step of more flexible ways of operating.

Staff motivation was a priority, and ENISA continues to strive to keep staff highly engaged. However, nearly one quarter of ENISA staff find that they have limited opportunities to grow within the Agency, and are not satisfied with their work. This is a clear indicator that the Agency needs to further address staff development, and enhance job satisfaction. The matrix set-up also allowed staff to unfold talents and use them to achieve quality outcomes across all areas of agency activity; however, the Agency needs to work more concretely towards this goal, revamp its learning and development policy and move towards business-driven learning needs. The Agency conducted its annual staff survey, in which staff had the opportunity to express their views, and for the Agency to carry out follow-up actions. The Agency took measures to address complaints and continues to establish open communication channels with staff, both directly and through representatives on the staff committee.

As the Agency shifted to a combined qualitative as well as quantitative approach to management, new management instruments were introduced to monitor performance on quarterly, four-monthly and annual bases, providing a dense framework of performance and continuous improvement. The reclassification exercise was improved in order to steer the process towards qualitative elements of assessment and focus on outputs and behaviours that are widely observed and recognised, as means to promote best practices.

Since the start of the COVID-19 pandemic and during 2021, the agency has introduced and maintained permanent teleworking options while maintaining and enhancing employee motivation, efficiency and development. Such measures enhanced the Agency's flexibility and drive to manage its people and services using modern HR practices. Such measures also helped the Agency recognise the importance of staff flexibility in the modern working environment while shifting process improvement to remote management practices.

During 2021 ENISA 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 develop personally and professionally, while keeping staff engaged and motivated and providing a sense of belonging.

Action has been taken to build an attractive workspace by establishing and maintaining excellent working conditions (premises, layout of office space). The move of ENISA to its new office location, the refurbishment and the improvement of the office space were steps towards improved working conditions. Such improvements occurred while developing user-centric (tele)working functionalities. The existing infrastructure for secure remote connections enabled the Agency to switch to teleworking seamlessly when the building became unavailable because of the lockdowns triggered by the pandemic. However, the Agency is facing significant challenges in its audiovisual and videoconferencing capabilities, which need to be further upgraded and steered towards more state-of-the-art services in order to help the Agency meet its operational objectives. Moreover, the Agency needs to further review its IT policies, practices and monitoring to improve the service delivery it offers to its users. However, the IT tools the unit uses do not support a modern, sustainable and flexible working environment, and they require significant investment in order to move towards simpler but user-centric tools.

Resources

In terms of resourcing, the unit faced resource constraints on implementing its activity programme due to the increased administrative procedures and the move to the new premises. To perform its objectives, the Agency relied heavily on delivering its services through interim agents who supported the day-to-day administrative burden in the support functions. Considering that increased support was also needed following the reorganisation, 10 additional interim agents were allocated to cover ongoing needs. The preparation for the new building also put an additional strain on the financial and procurement team, which had to administer additional financial processes to implement the move in compliance with approved standards.

While tasks were assigned based on the physical location of the Agency (Athens, Brussels, Heraklion), this old way of managing resources did not support a more flexible way of operating and as a result increased the daily operational complexity and staffing needs. A particular constraint that was established was in the area of facility management, where the scope and breadth of activities was greater; however, the Agency had allocated 1 FTE located in Heraklion to managing the facilities at all locations, or requirements were addressed ad hoc. Some of the facility management activities had been undertaken by the retiring security officer, which resulted in an operational gap for the unit.

As a result, a lot of activities in facility management were not tackled. In addition, the introduction of the Information Technology Management Committee (ITMC) and Budget Management Committee (BMC), while the Agency moved to more centralised IT governance, created a new way of operating for the Corporate Support Services Unit, which brought about further delays in project implementation. At the end of the year, to address the Agency's operational needs for meetings, a refurbishment plan was proposed and endorsed to reconstruct part of the conference area and part of some office space. The refurbishment also included the redesign of the boardroom. For this reason, a carry-over (EUR 643 407) was planned in order to cater for this project.

Regarding the unit's knowledge, additional investment needs to be made in educating the unit further and bringing its human capital up to date with the latest practices by means of traditional conventional training and on-the-job learning and job-sharing activities. This would establish a solid basis for further enhancing the operational capability of the team to meet its objectives. Considering that the Agency operates on project-based methodologies and has reorganised its operation, the unit struggles to keep up with the new way of working as incoming requests come from all users. Also considering that this was the first year it operated following the reorganisation and the arrival of a new head of CSS, the unit has started to build up its knowledge levels slowly but steadily. While peer-learning continues, the professionalisation of the CSS services must go hand in hand with service optimisation while at the same time building up the knowledge level of its staff. Besides that, one of the challenges the unit faces is the grading of its staff in relation to the activities, and responsibilities fulfilled. While the unit will engage in a service delivery roadmap transition, the job responsibilities and grading will be reviewed in order to reflect the exact level of responsibilities performed.

Overall assessment

Overall, it is evident that the relevance of the structure of the activity, its outputs and its KPIs need to be reviewed in order to reflect the full-service provision the unit offers. During the implementation, it was evident that not all service outputs were identified under Activity 11, while there were overlaps with Activity 10 on many occasions, as both units share a compliance, coordinating, project and policy-driven angle but tackle it from different perspectives. Therefore, activities 10 and 11 need to be revised in the 2023 SPD to more closely reflect the work carried out.

Based on the existing output description in the SPD, it has proven challenging to link various initiatives of the CSS unit to the output descriptions of this activity and to cater for the main elements of service provision, which are recurrent services. This has created a lot of challenges in the implementation capabilities as well as the reporting capabilities of the unit. Overall, the recurrent service provision, service optimisation and security-related outputs should be further reflected in the 2023 SPD while redrafting the existing outputs in a way that supports more flexible implementation of activities in order to assist the Agency to meet its corporate objectives. Considering the 2021 results, in 2022, CSS went for a back-to-basics action plan (review of rules, tools, map as-is format, etc.) in which the building blocks are being set up to cater for the challenges of the future. This initiative will need to continue in 2023 onwards while building upon the strategic and service delivery model.

Having regard to the need to reorganise the services of the unit, and work on the synergies identified among the various sectors, the Agency suggests that the Management Board adjust the outputs of this activity and redefine them in a way that supports the Agency's transformation in order to meet its strategic objectives. It is also further envisaged that Activities 10 and 11 be redefined to better synergise the complementarity of the two units.

Objectives



- Engaged staff who are committed and motivated to deliver and who are empowered to fully use 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 corporate objective



- Build an agile organisation focused on people

Results



- ENISA as an employer of choice

Outputs



- 11.1.** Implementation of the competence framework (including the training strategy, CDR report, internal competitions, exit interviews)

Outcome



In 2021, the HR sector embarked upon a continuation of the development of the competency framework. It wished to operationalise the competency framework in different processes of the talent management life cycle, namely recruitment, performance management and appraisals, reclassification and contract renewal, and learning and development. The challenges faced in the matter were related to the differentiation of competency expectations (i.e. competencies and proficiency levels), between different roles and grades in the organisation, as well as internal consistency in the use of competency expectations (i.e. competencies and proficiency levels). It was also deemed crucial to have overall clarity and transparency for staff, and related principles such as objectivity, transparency and fairness.

HR worked on addressing challenges related to the construction of the competency framework, potentially necessary changes and adaptations, and a conceptual approach on how to use the competency framework in HR processes. This was closely related to having staff members who are highly motivated and loyal to the organisation and whose competencies are used in the right place, at the right time.

In practice, the newly established competency framework is proving to be quite challenging to implement, so a further simplification review is envisaged in the course of 2022–2023. The Agency plans a revision of the framework to simplify it with the possible aim of tying it to a revision of its job-mapping and -grading structure for future strategic workforce-planning activities.

HR examined the feedback from the exit interviews and staff surveys to identify those points that need to be addressed in order to continue improving its services. Feedback received was mainly directed at the cumbersome administrative processes, lack of internal communication or unclarity about where the information may be found easily, and sometimes at organisational complexity or complacency that prevents innovative ideas and practices from contributing more to the strategic objectives.

Regarding recruitment and onboarding, a lot of emphasis was given to sourcing good candidates with diverse backgrounds; however, budget restrictions prohibited the use of a wide range of sourcing options. The administrative process behind the recruitment procedures was lengthy and cumbersome, which led to operational delays. Emphasis needs to be put on simplifying the recruitment procedures, educating ENISA staff and obtaining a tool to speed up ENISA's response to sourcing talents that would help the Agency fulfil its strategic needs.

The results of the KPIs associated with this output indicate a first good step towards the activity outputs; however, there is a lot of work that the Agency needs to do to further establish the pillars for talent development and increased job satisfaction. The parameters can move outside the barriers of HR and also encompass working conditions, digitalisation of services, self-service functionalities, simplification of procedures, etc.

Given the outcomes of 2021, the added value achieved and the related actions already planned in the 2022 SPD, the output description was very restrictive and limited the possibilities and breadth of actions the unit could engage in. The Agency needs to move towards more forward-looking practices and adopt an overall corporate strategy that addresses its HR, IT, security, facility management and financial challenges. Therefore, a more holistic revision of this objective is needed, in close partnership with the Executive Director's Office, to address the corporate objective and the challenges of the future.

Therefore, the Agency suggests that the Management Board adjust the outputs for the 2023 SPD and redefine them in a broader context that would better fit the corporate objective.

11.2. Actions to develop and nourish talent (in line with output 11.1)

During Q4 2021, HR deep-dived into performance management and revamped the current framework, within the limits of the applicable Management Board rules adopted in 2015. Nourishing performance and career progress is a top priority for the HR sector, which is why there were numerous and extensive training courses organised for staff and management, as well as several seminars dedicated to the performance management framework. The appraisal exercise is under way, and the lessons learned from the new approach will be evaluated in the course of 2022.

In response to the pandemic and the need to have a digitally enabled workplace and environment, in Q1 2021 the agency extended its welfare scheme by adopting a decision on the reimbursement of Internet expenses since March 2020 retroactively. Within the context of a broader welfare package, the Agency continues to pay attention to the benefits it offers to its staff in order to balance out the reduced coefficient rate and legal limitations regarding flexible work practices.

The Agency also ensured that ergonomic equipment such as chairs, monitors and peripherals were distributed to staff, to ensure that their home environments were sufficiently equipped for them to continue to perform their duties.

In terms of nourishing talent, besides the broad learning offer that is available to staff, the Agency offers on-the-job development opportunities through its annual call for contributions in its teams. This is a way to enhance talent, work on fields outside one's own, bridge the gap between operational and support units, and give opportunities for new ideas and new contributors to combine knowledge sharing with additional outputs. It is unfortunate that not many candidates from support units contributed to the team outputs, which is an indicator the Agency needs to consider thoroughly. Besides that, the Agency needs to further develop the 70-20-10 model for learning and development in the course of its upcoming SPD to capitalise on its staff strengths and competencies and promote a collaborative, open culture of learning. To do so, the Agency needs to steer its budget not only towards training activities that would enhance the technical aspects of the training, which need to be more closely focused on its strategic objectives, but also towards investing in educating staff. Additional budget would need to be provided following the review of the Agency's L&D policy and framework.

The Agency needs to further explore and reassess its corporate strategy and consequent HR strategy in order to identify ways of improving ENISA and attracting talents in the competitive cyberfield world. While doing so, the Agency needs to shift its talents towards a more flexible and agile workforce so resources are allocated to business priorities. Therefore, the Agency needs to build on its current base and adopt an efficiency gains strategy addressing all levels by revising its HR, finance and corporate services practices. By doing so, the Agency needs to further elaborate and align its strategic workforce-planning practices, data analytics and workload indicators while reviewing and simplifying its current administrative procedures by improving its tools or revising its existing practices. Additional revision of ENISA's financial model is required in order to enhance accountability across all layers of the Agency while reducing administrative procedures. The introduction of Mission Integrated processing system and the Public Procurement Management Tool in 2022 and 2023 would be a first step towards this model revision.

The results of the KPIs associated with this output indicate a first good step towards the activity outputs; however, there is a lot of work that the Agency needs to do to further establish the pillars for talent development and increased job satisfaction. The parameters can move outside the barriers of HR and also encompass working conditions, digitalisation of services, self-service functionalities, simplification of procedures, etc. Significant work needs to be done on revisiting the job descriptions and moving towards job profiling and competency development, while focusing on learning activities that add value to the business objectives and support professional advancement, establishing multiple career path options.

Given the outcomes of 2021, the added value achieved and the related actions already planned in the 2022 SPD, the output was partly achieved, as it was focused only on the HR component in isolation. In line with the revised CSS way forward, the agency suggests that the Management Board redefine this output and increase its scope in the 2023 SPD.

11.3. Undertake actions to support a digital working environment and develop necessary tools and services in line with output 10.3

While continuing with a burdensome administrative way of working, in 2021 the Agency enhanced the structure of its digital working environment, by improving its collaboration platforms by moving to SharePoint 2019 on its premises, and by migrating ENISA's repository structure to an updated environment. ENISA also built up its conferencing capacity by renewing Webex online conferencing and activating end-to-end encryption, and set up a boardroom facility in the new headquarters in Athens as the basis of an updated videoconferencing infrastructure.

ENISA also reinforced the ability of staff and contractors to telework by promoting a replacement teleworking solution for the current system, which is reaching the end of support (Microsoft Direct Access), and moving towards a new teleworking solution (FortiVPN), which started as a successful pilot in 2021 and aspires to be functional in Q3 2022. Finally, the Agency undertook an assessment of its tooling needs under Activity 10 (see main achievements under Activity 10).

In terms of digital simplifications, 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 and ARES. In 2021, the Agency also conducted an analysis conducted internal testing on introducing Mission Integrated processing system and the Public Procurement Management Tool for its mission and procurement procedures. The pilot phases were successful and the Agency is now preparing the transition to the full Agency in 2022. However, it has to be noted that introducing all these systems came in addition to the work performed by staff, without additional resources being provided.

In 2021, with the arrival of the new head of CSS, the Agency will look further into the service provision of its services and move towards a service-based model. A further analysis needs to be made in 2022 in order to identify and map which services it will keep in house and those it will outsource. To do so, the Agency will need additional budget to cater for the new modus operandi and look in more detail at its outputs and workload indicators, so that it can reshuffle priorities according to its business needs. To further support the efficiency gain strategy and the business model transformation, additional budget is needed to support the units in outsourcing services to external providers.

The results of the KPIs associated with this output indicate a first good step towards the activity's outputs; however, these were primarily IT driven, and other components are needed to contribute towards an improved digital working environment. The Agency needs to further redefine its IT service provision model and service optimisation in order to cater for the challenges of the future, while including in its scope activities beyond IT that contribute to this goal.

Given the outcomes of 2021, the added value achieved and the related actions already planned in the 2022 SPD, the output was partly achieved, as the concrete outputs under this activity and the KPIs reflected the former set-up of the CSS unit. In line with the revised CSS way forward, the Agency will suggest to the Management Board to redefine this activity and increase its scope in the 2023 SPD.

11.4. Planning, preparation and completion of the establishment of the Agency's headquarters in its new premises in line with the objectives of the activity

During 2021, the Agency planned, prepared and moved to its new headquarters building, ensuring minimal disruption to its operations. An internal team supported the move throughout the process and coordinated with internal and external stakeholders, including the creation of a detailed plan for all phases of the successful implementation.

Throughout the year, all ENISA staff and managers were involved in exploring the best use of the new facilities and how the future work of the Agency should be conducted to strengthen the Agency's creativity, collaboration, values and mandate. The building is now operational; however, additional work is required in order to improve the existing facilities, improve its audiovisual services, and cater for more open and collaborative work practices. The Agency also needs to reflect more holistically on its hot-desking and office-sharing policy, so that its facilities practices contribute practically to an open and collaborative yet agile way of working. The new building also brings a lot of daily challenges in facility management, and the Agency has decided to outsource the facility management service in order to alleviate pressure on resources while maintaining a fully functioning building. Thus, additional funds are needed in order to ensure that the Agency fulfils its strategic objectives.

The Agency also proceeded further in preparing to open a Brussels office, which will help keep operational activities secure and assist the Agency in fulfilling its operational mandate.

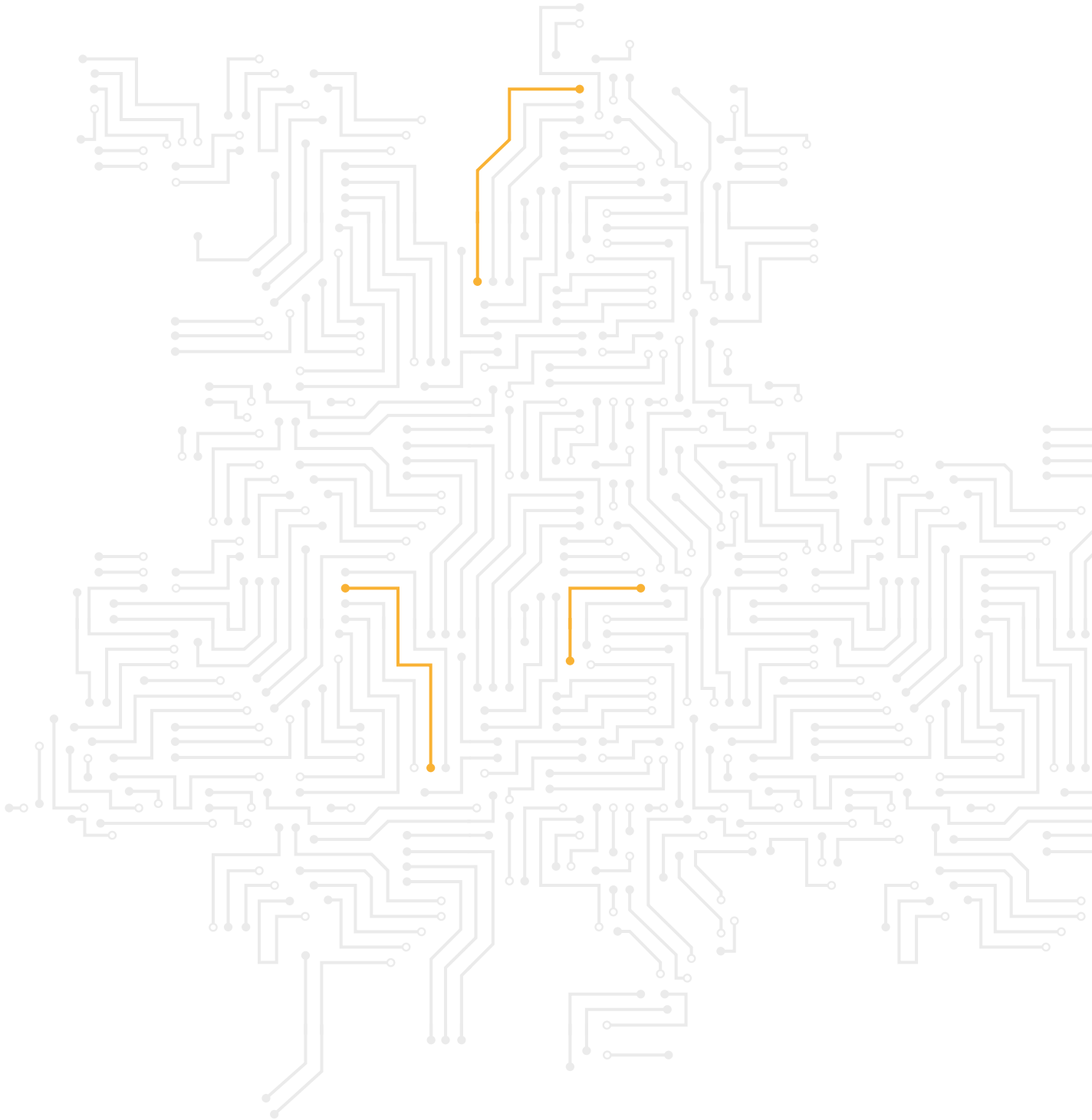
Given the outcomes of 2021, the added value achieved and the related actions already planned in the 2022 SPD, the output description was met. The Agency needs to move towards more forward-looking practices and adopt an overall corporate strategy that addresses its HR, IT, security, facility management and financial challenges. Therefore, the Agency suggests that the Management Board adjust the output for the 2023 SPD and redefine it in a broader context.

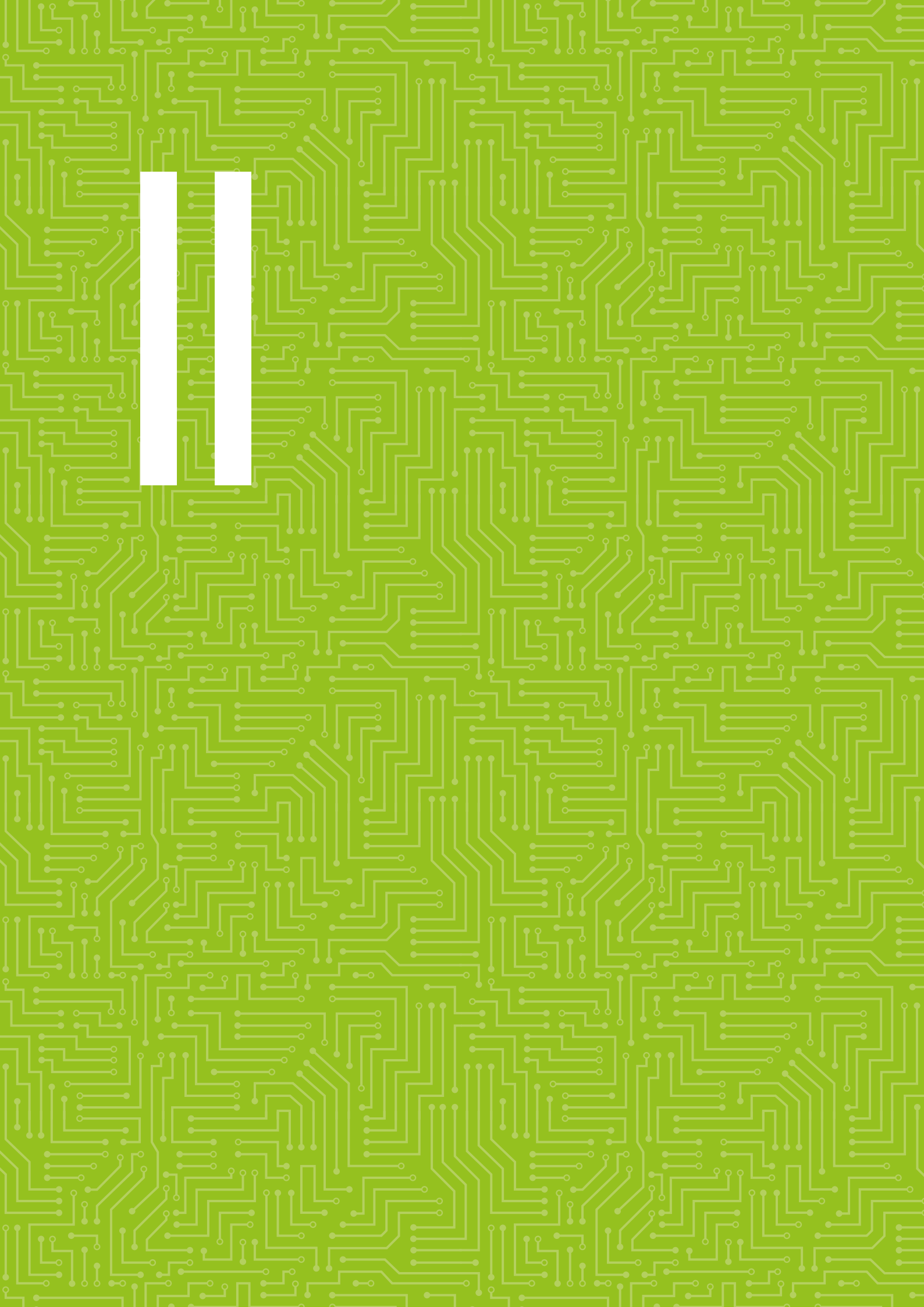
Key performance indicators	Unit of measurement	Frequency	Data source	Results 2020	Results 2021
Staff commitment, motivation and satisfaction					
11.1. Staff satisfaction survey (including the attractiveness of ENISA as an employer, staff empowerment, organisational culture, opportunities for internal mobility, workspace, work environment and work tools)					
Percentage of staff seeing a positive atmosphere within ENISA since the reorganisation	%	Annual	Staff satisfaction survey	70 %	58 %
Percentage of staff feeling confident working within the new organisational culture	%	Annual	Staff satisfaction survey	61 %	68 %
Percentage of staff satisfied with their work	%	Annual	Staff satisfaction survey	74 %	80 %
Percentage of staff indicating their line manager provides sufficient feedback on their performance	%	Annual	Staff satisfaction survey	68 %	76 %
Percentage of staff indicating their line manager sets clear objectives	%	Annual	Staff satisfaction survey	66 %	76 %
Percentage of staff that feel well informed by ENISA leadership regarding important matters	%	Annual	Staff satisfaction survey	80 %	73 %

Key performance indicators	Unit of measurement	Frequency	Data source	Results 2020	Results 2021
Staff commitment, motivation and satisfaction					
11.2. Quality of ENISA training and career development activities organised for staff					
Percentage 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 %
Percentage of staff indicating that courses match their training and development needs	%	Annual	Staff satisfaction survey	N/A	58 %
Percentage 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 %
Percentage 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 %
Percentage of staff finding that they have had the opportunity to grow in their careers at ENISA since the reorganisation	%	Annual	Staff satisfaction survey	N/A	35 %
11.3 Reasons for staff departure (exit interviews)	Scale 1-10	As required	HR files	N/A	7.1
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
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
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
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
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
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
On a scale of 1 to 10, did you have clear performance objectives in your job? (10 being crystal clear and 1 being not clear at all)	Scale 1-10	As required	HR files	N/A	6.8
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
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
Turnover rates	%	Annual	HR files	2 %	3 %

Key performance indicators Staff commitment, motivation and satisfaction	Unit of measurement	Frequency	Data source	Results 2020	Results 2021
11.4. Resilience and quality of ENISA IT systems and services					
Critical systems downtime	%	Annual	Uptime report of Fortimail appliance in Heraklion	N/A	99.38 %
Percentage of central IT infrastructure assessments with few (< 5) critical findings	%	Annual	Intranet repository of all proactive assessments and their findings	N/A	100 %
Percentage of central infrastructure patched to the last formal versioning of 1 year	%	Annual	Yearly IT maintenance plan in PDF	N/A	95 %
Percentage of major IT helpdesk requests resolved in a satisfactory way within 2 business days	%	Annual	Graph created from IT ticket repository	N/A	80 %
Percentage of staff indicating supported by ENISA's IT infrastructure for remote working	%	Annual	Staff satisfaction survey	N/A	76 %
Percentage of staff indicating that the IT helpdesk responds within a reasonable time	%	Annual	Staff satisfaction survey	N/A	75 %
Percentage of staff indicating that the IT central services are stable	%	Annual	Staff satisfaction survey	N/A	62 %
Percentage of staff finding the digital applications easy to use and covering job requirements	%	Annual	Staff satisfaction survey	N/A	67 %
Percentage of staff finding that digital applications for the job are supported in a timely manner	%	Annual	Staff satisfaction survey	N/A	65 %
Percentage of staff indicating that connectivity issues are resolved swiftly	%	Annual	Staff satisfaction survey	N/A	65 %
Planned budget (direct costs only)	EUR 1 432 878	Consumed budget (direct costs only)		EUR 1 611 756	
Actual used FTEs	Actual: 19.90	Of which carried over to 2022:		EUR 643 407	

N/A, not applicable.





PART II (A)

MANAGEMENT

1 MANAGEMENT BOARD

In 2021 the Management Board met for two ordinary meetings.

In total, the Management Board made 19 decisions during the year, such as on the anti-fraud strategy and its action plan, on the setting up of a local office in Brussels and on EU classified information.

As part of its functions, the Management Board adopted its analysis and assessment of the 2020 annual activity report, in which it commended the Agency on the very high standard achieved in the delivery of its work. The Management Board also expressed its favourable opinion on the final annual accounts for 2020 and adopted the ENISA programming document 2022–2024, including the 2022 budget and the 2022 establishment plan.

Sharing information with the Management Board regularly, ENISA reported on the work programme and budget implementation, and gave updates on the reorganisation and the relocation of the ENISA headquarters in Athens, among other pertinent matters.

In addition, the Management Board provided guidance on the ENISA stakeholder strategy.

The Executive Board had one formal meeting per quarter.

2 MAJOR DEVELOPMENTS

The 2021 work programme was developed to enable the Agency to fully exploit its permanent mandate and fulfil all the tasks given to it by the CSA, while taking into account all other changes in the EU's regulatory framework. In addition, the 2021 work programme was aligned with ENISA's new strategy, which was adopted by the Management Board in June 2020 and was used as a baseline to set the strategic objectives and priorities for planning the Agency's work using a multi-annual framework.

Reorganisation

The 2021 programming document was drawn up in parallel with the reorganisation of the Agency, which was agreed by the Management Board in June 2020 and became effective on 1 January 2021. The new organisational structure is aligned with the tasks and functions of the Agency's structural set-up under the CSA, thus allowing more efficient delivery of the activities in the work programme. A framework was established for the organisation of the work of all staff members of the Agency. The Management Team assists the Executive Director in his functions, ensuring that activities undertaken by the agency under its work programme add value for the Union and are planned and implemented in a coordinated fashion. Its role is to enhance cooperation and to build synergies across the organisation through an

open exchange of views and shared information. The following units were established to ensure the performance of the tasks of the agency as set out in the CSA:

- Policy Development and Implementation Unit to implement Article 5 of the CSA;
- Capacity Building Unit to implement Article 6 and Article 7(5) of the CSA;
- Operational Cooperation Unit to implement Article 7 (except for Article 7(5)) of the CSA;
- Market, Certification and Standardisation Unit to implement Articles 8 and 22 and Title III of the CSA.

The following four teams were established and tasked with articles of the CSA:

- Knowledge and Information Team to implement Article 9;
- Awareness Raising and Education Team to implement Article 10;
- Research and Innovation Team to implement Article 11;
- International Cooperation Team to implement Articles 12 and 42.

In addition, two corporate units were established to support the Executive Director:

- the Executive Director's Office ensures that the Agency has in place an operational performance management framework, anti-fraud policies, and an internal evaluation and control framework so that the agency follows the objectives of sound budgetary management and complies with its legal obligations (including conflict of interest rules and ethical standards);
- the Corporate Support Service ensures that the Agency has modern capabilities and tools to manage and develop its HR, in particular talent management programmes (learning and development), a workforce recruitment and retention strategy, and adequate employee services (including individual rights and salaries).

Establishment of IT Management Committee and Budget Management Committee

The ITMC was established in the first quarter of 2021, to ensure the comprehensive and coordinated management of the Agency's IT systems and services required to fulfil its core tasks, as described by its operational mandate, and corporate functions.

The mandate of the ITMC encompasses the entire life cycle of all relevant IT projects, including setting the overall framework and guiding the development, roll-out and implementation as well as follow-up and analysis.

The BMC was established in the last quarter of 2020. The mandate of the BMC is to ensure coherent planning, implementation and follow-up of the Agency's budget, and encompasses the entire life cycle of the budget, including assisting in setting the overall framework and guiding the development, roll-out and implementation as well as follow-up and analysis of the budget. Therefore, the BMC issued budget implementation reports and submitted them to the Management Team, reflecting the status of implementation of the budget as of 1 May 2021 and 1 September 2021, and targeted interim reports every quarter to tackle specific issues arising from the implementation of the budget.

Structured cooperation with the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies

The reporting year also marked the point when structured cooperation between ENISA and CERT-EU in the field of operational cooperation became fully operational with the annual cooperation plan and the MoU between ENISA and CERT-EU.

New headquarters in Athens

In agreement with the Greek authorities, ENISA moved into its new headquarters in Athens in 2021 to meet the growing needs of the Agency.

The Agency moved into the new headquarters building in the third quarter of 2021, ensuring minimal disruption to operations. An internal workgroup supported the move throughout the process and coordinated with internal and external stakeholders, including the creation of a detailed plan for all phases of successful implementation.

Throughout the year, all ENISA staff and managers were involved in exploring the best use of the new facilities and how the future work of the Agency should be conducted to strengthen the Agency's creativity, collaboration and corporate values. In response to the COVID-19 pandemic, new consideration was given to hybrid ways of working that will affect how the Agency best uses its resources. During this discussion, the environmental impacts of the Agency's operations

and performance were considered in the light of the desired environmental management strategy that was developed.

Brussels local office

The ENISA local office in Brussels was established with a view to implementing structured cooperation with CERT-EU and maintaining regular and systematic cooperation with EUIBAs including but not limited to CERT-EU, the EEAS, Europol, the EDA and/or other competent bodies involved in cybersecurity, in order to benefit from synergies and avoid the duplication of activities.

In agreement with the Greek authorities, ENISA moved into its new headquarters in Athens in 2021 to meet the growing needs of the Agency.

Recruitment

In 2020 the Agency embarked on a large-scale novel recruitment exercise to create a sufficiently diverse and broad reserve shortlist of 75 candidates with broader competences and skills that could be used to recruit staff and thus fill the gaps in the current establishment plan, as well as serving as a pool of candidates for the future establishment plan. Through the success of this call, ENISA welcomed 31 newcomers in 2021 (22 temporary agents, 5 contract agents, 3 seconded national experts and 1 trainee), an increase in staff

members of over 25 %. ENISA's workforce planning has allowed the Agency to proactively estimate, engage, develop and align its HR with the evolving strategic focus of its activities and objectives as directed by its SPDs, the Management Board and Union legislation.

3 BUDGETARY AND FINANCIAL MANAGEMENT

a) FINANCIAL MANAGEMENT

The Agency operated with a budget of EUR 23.5 million, equivalent to an 8 % increase in 2021 compared with the 2020 budget (EUR 21.7 million). An amending budget was adopted by the Management Board by written procedure on 21 December 2021, reflecting new challenges and priorities stemming from the move to the new office building in Athens and the COVID-19 pandemic. Amending budget 1/2021 was adopted in order to finance new projects and activities amounting to EUR 0.5 million, mostly related to refurbishment needs for the new office.

In 2021 ENISA concluded a total of 58 public procurement procedures (two of which were undertaken jointly with the European Centre for the Development of Vocational Training (Cedefop)):

- 31 were done through reopening of competitions under framework contracts (53 %);
- 15 were done through negotiated procedures for middle- and low-value contracts (26 %);
- 8 were done using the open procedure (14 %);
- 3 were done using the restricted procedure (5 %);
- 1 was done using the CEI procedure (2 %).

EUR 3.02 was paid in 2021 to suppliers as interest for late payments.

The table below shows ENISA's budget implementation targets and achievements in 2021, which remained high under the restrictive circumstances imposed by COVID-19.

Area	Objective	Target 2021	Level of completion 2021
Budget implementation (appropriations committed through the year)	Efficiency and sound financial management	99 %	99.51 %
Payments against appropriations of the year (C1 funds)	Efficiency and sound financial management	85 %	77.40 %
Payments against appropriations carried over from previous year (C8 funds)	Efficiency and sound financial management	95 %	96.55 %

b) BUDGET EXECUTION OF EU SUBSIDY (C1 FUNDS OF CURRENT YEAR 2021)

During 2021, ENISA committed EUR 22 721 149, representing 99.51 % of the total budget for the year. Payments made during the year amounted to EUR 17 672 344, representing 77.40 % of the total budget. The budgetary execution was high despite the restrictive circumstances imposed by COVID-19. Compared with 2020, there was a noticeable increase in commitment execution – 99.51 % in 2021 compared with 97.35 % in 2020 – and a noticeable increase in payment execution – 77.40 % compared with 68.62 % in 2020. 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 2021 were carried forward to 2022.

c) AMENDING BUDGET / BUDGETARY TRANSFERS

According to Article 26 of ENISA's applicable 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. Transfers within the same title are permitted without limit. Beyond the limit referred to above, the Executive Director may propose to the Management Board transfers of appropriations from one title to another. The Management Board has two weeks to oppose the proposed transfers. After that time limit, the proposed transfers are deemed to be adopted.

The Agency made four transfers in the reporting year by the decision of the Executive Director on the initial budget, and one transfer by the decision of the Executive Director on the amended budget (in comparison, the Executive Director made three transfers on the initial budget and four transfers on the amended budget in 2020). The four transfers on the initial budget included one transfer within title and three transfers between titles and within title. The only transfer on the amended budget was both within title and between titles. Because of COVID-19 restrictions and of the move to the new building, funds were mainly redirected from salaries, meetings, conferences, other events and business travel to support mostly refurbishment-related needs for the new office, and staff development and learning needs.

The table below summarises the execution of the budget in 2021 by title.

2021 budget (C1)						
Area of budget allocation	Appropriation amount (EUR) (1)	Commitment amount (EUR) (2)	Percentage committed (2)/(1)	Payment amount (EUR) (3)	Percentage paid (3)/(1)	Amount carried forward to 2022 (EUR)
Title I	10 707 109	10 701 572	99.95	9 993 015	93.33	708 558
Title II (*)	3 662 751	3 636 207	99.28	1 472 134	40.19	2 164 073
Title III	8 463 200	8 383 370	99.06	6 207 195	73.34	2 176 174
TOTAL	22 833 060	22 721 149	99.51	17 672 344	77.40	5 048 805

(*) Title II does not include the subsidy of up to EUR 640 000 from the Greek authorities for the rent of the building. Further details on budget execution are provided in Annex II.

The table below summarises the changes to the budget in 2021.

2021 budget (C1) (EUR)				
2021 area of budget allocation	Initial budget	Amended budget	Transfers approved by the Executive Director	Final budget
Title I	10 775 409	10 682 109	25 000.00	10 707 109
Title II (*)	2 907 651	3 662 751	—	3 662 751
Title III	9 150 000	8 488 200	- 25 000.00	8 463 200
TOTAL	22 833 060	22 833 060	—	22 833 060

(*) Title II does not include the subsidy of up to EUR 640 000 from the Greek authorities for the rent of the building.

d) CARRY-FORWARD OF COMMITMENT APPROPRIATIONS

The commitment appropriations corresponding to the EU subsidy (C1 appropriations) that were not fully paid at the end of 2020 were carried forward to 2021 (C8 appropriations).

Compared with 2020, there was a nearly 1 percentage point increase in payment execution (96.55 % in 2021 compared with 95.86 % in 2020), showing an improvement in financial management in this regard.

The following table shows the commitment execution and payment execution in 2021.

2021 budget (C8)				
2021 area of budget allocation	Appropriations carried forward from 2020 to 2021 (EUR)	PAYMENT AMOUNT (EUR)	Percentage paid	Amount cancelled (EUR)
Title I	1 209 759	1 135 981	93.90	73 779
Title II	1 762 732	1 672 080	94.86	90 651
Title III	3 102 500	3 057 545	98.55	44 955
TOTAL	6 074 991	5 865 606	96.55	209 385

4 DELEGATION AND SUB DELEGATION

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 of 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 transaction. ENISA did not implement any further subdelegations in 2021.

Controls on these delegation rights are done through a periodical revision of the rights granted in the main financial system Accrual Based Accounting (ABAC) and are shared on an annual basis with the Commission (Directorate-General for Budget).

5 HUMAN RESOURCES MANAGEMENT

In 2020 the ENISA Management Board established a structure for the Agency, set in place principles under which the organisation should function, and imposed guidelines for the proportional allocation of resources between its operational units and those that support the administrative and corporate functions. On 1 January 2021, the new organisational structure was in effect.

The HR sector continued to support the operational and administrative goals of the Agency in terms of staff acquisition and development. In 2021, ENISA HR welcomed 31 newcomers (22 temporary agents, 5 contract agents, 3 seconded national experts and 1 trainee). ENISA's workforce planning was for the first time mapped by an Executive Director decision (17/2021). The aim of this decision was to set the basis for strategic workforce planning, which would allow the Agency to proactively estimate, engage, develop and align its HR with the evolving strategic focus of its activities and objectives as directed by its SPDs, the Management Board and Union legislation. Following this decision, the Executive Director promptly launched the 2021 strategic workforce review by Decision No 28/2021.

In 2021, ENISA carried out tasks to support the deployment of the Commission's information management system for HR, Sysper.

In the context of the COVID-19 pandemic, in 2021 ENISA staff continued to telework. Staff guidelines were drawn up and teleworking was authorised in lieu of working in the office for all staff. The Agency continued to exercise its duty of care and allow staff members to take precautions based on numbers of intensive care units available in each relevant Member State. During the pandemic, daily updates were sent to all staff members via a designated functional mailbox, detailing the number of cases and the most recent developments in the world, so as to keep staff abreast of the latest news.

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 such as in the area of personal data protection.

Implementing rules adopted

In 2021, ENISA adopted two European Commission decisions: on a procedure for dealing with professional incompetence, and on laying down general implementing provisions on the conduct of administrative inquiries and disciplinary proceedings.

Brief description of the results of the screening/benchmarking exercise

ENISA continued in 2021 to partially apply the benchmarking exercise following the European Commission's methodology. The third table in Annex IV depicts the results of the exercise based on the type of posts with regard to administrative support and coordination, operational and neutral. A slight increase can be observed in the type of posts under 'administrative support and coordination' and 'neutral' in comparison with 2020³. The Management Board set out a transition period for the Agency within the 2022–2024 SPD based on the requirements outlined in Article 3(3) of Management Board Decision MB/2020/9, which direct the Executive Director to take steps in order to ensure that the average number of staff members assigned to the Executive Director's Office and the CSS does not exceed the average number of staff member assigned to operational units.

3 While the percentages in 2021 show a 'decrease' in the operational figures, in reality the % of the operational staff have increased not decreased, compared to 2019-2020. The numbers reported under the old structure did not reflect mandates of structural units accurately. The numbers reported under the 2021 exercise did not take fully into consideration the qualitative elements of the Commission's methodology which indicates, among others, that structural entity takes precedence over the function of the post (e.g. administrative function supporting operational units are counted as operational roles as they provide support of an operational nature), that the exact job purpose of the post needs to be looked at when in doubt (e.g. HR payroll is considered neutral and not administrative support even though the role belongs in HR, while internal control with emphasis on process is administrative support and not neutral) or the reference to the legal act needs to be looked at (how the job role fits under the Cybersecurity Act). The Agency intends to rectify this exercise in 2022 by fully aligning with the Commission methodology.

6 STRATEGY FOR GAINS IN EFFICIENCY

In 2021, the agency focused on implementing internal gains in efficiency in various areas as per the performance management roadmap.

Over the recording year, the reorganisation led to a complete revision of its way of working for internal decision-making. The Agency progressively optimised its structure and working methods, and implemented cost efficiency measures in its business model, for example by introducing the Commission tools Sysper, Mission Integrated processing system and ARES.

This led to an improvement in performance in various areas but also to a strengthening of service continuity.

Furthermore, the implementation of several MoUs and SLAs signed in 2020 and early 2021 led to close cooperation with other EUIBAs, namely Cedefop, eu-LISA, CERT-EU, the EDA and Europol. SLAs with Commission services allow the Agency to optimise its resources spent on administrative support. HR, treasury services and the cybersecurity of ENISA's IT systems are supported through such SLAs.

In 2022 the Agency is actively seeking gains in efficiency by developing an approach to sharing services with the newly established European Cybersecurity Industrial, Technology and Research Competence Centre⁴, in particular in the area of administrative support.

7 ASSESSMENT OF AUDIT AND EX-POST EVALUATION RESULTS DURING THE REPORTING YEAR

7.1 Internal Audit Service (IAS)

The IAS audit report on HR management and ethics was issued in September 2019. Three very important and four important recommendations were issued in this audit.

Although four recommendations were closed by the IAS following the corrective actions implemented by ENISA, three important recommendation remained open at the end of 2021, which were not fully implemented within the set time frame.

4 See Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623160399041&uri=CELEX%3A32021R0887>).

The table below shows ENISA's planned recruitment goals for 2020 to 2021.

Area	Objective	2021 performance	2020 target	2021 target
Efficient management of selection procedures	Reduction of time taken to hire (in line with the standard EU HR definition, this is the time frame set from the deadline for candidates to submit applications until the signing of the reserve list by the Executive Director)	4 months	≤ 5 months	≤ 5 months
Turnover of staff	Reduced turnover rate of statutory staff (temporary agents and contract agents)	3 %	< 15 %	< 15 %
Staff performance management	Implementation and monitoring of the appraisal and reclassification exercises (launching and completion of the exercises)	100 %	100 %	100 %

They delays are mainly imputable to the reorganisation of ENISA stemming from the adoption of the CSA. To better address the new challenges under this new regulatory framework, ENISA, with a stronger mandate and increased financial resources, was significantly reorganised and restructured with effect from 1 January 2021.

This had the consequence that many internal processes had to be rethought to fit the structure as approved by the Management Board in June 2020, and have introduced new ways of working.

This affected the roll-out of the corrective HR plan as initially planned with the IAS in late 2019. A new timeline to implement the three remaining recommendations was agreed with the IAS.

In 2021 the IAS conducted an audit on strategic planning programming and performance management in ENISA and issued its final audit report in April 2022, with three important recommendations that ENISA commits to address in the course of 2022 and onwards.

7.2 European Court of Auditors

In 2021 the ECA issued its report on the 2020 annual accounts of the agency⁵. In the ECA's opinion, the accounts of the agency for the year ended 31 December 2020 present fairly, in all material respects, the financial position of the agency at 31 December 2020, 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 accounting rules adopted by the Commission's accounting officer.

⁵ Available online (<https://www.enisa.europa.eu/about-enisa/accounting-finance/>).

Moreover, payments underlying the accounts for the year ended 31 December 2020 are legal and regular in all material respects, except for a weakness in the delegation of financial rights whereby financial transactions had been authorised without proper financial delegation rights in place. This led to the ECA's qualified opinion on the legality and regularity of the payments underlying the accounts.

It is important to note that these financial transactions did not affect the reliability of the financial records: these transactions would have been processed by the Agency anyway, as all of them were free of conflict and completed in pursuance of the Agency's objectives and for its official use.

As already reported in the 2020 annual activity report, the Agency welcomed this audit finding and a corrective action plan was immediately devised to address this legal issue and to reinforce relevant internal controls.

An additional independent and specific report was requested on this matter from ENISA's external auditors, Mazars, in late 2021. It confirmed that these transactions were duly justified in pursuance of the Agency's objectives and for its official use.

Following up on previous ECA observations, ENISA adopted a sensitive functions policy in 2021 (entering into force in May 2022) and is still reducing its usage of interim staff.

European Court of Auditors audit on cybersecurity of EU institutions, bodies and agencies

The ECA conducted in 2021 an audit on the level of cybersecurity preparedness of EUIBAs. The scope of the audit included three main questions, on the key cybersecurity practices adopted across EUIBAs, the efficiency of cooperation between EUIBAs on

cybersecurity, and the adequacy of the cybersecurity support provided to EUIBAs by ENISA and CERT-EU. ENISA was specifically surveyed by ECA to that end. The final ECA audit report was published in March 2022⁶. ENISA welcomed the recommendations and observations of the report⁷, which highlight the key roles that ENISA and CERT-EU can play in increasing the level of cyber preparedness of EUIBAs and underline the need for adequate resources to do so.

7.3 Ex-post control evaluation results

In 2021, ENISA performed *ex-post* controls of financial transactions in accordance with the ENISA financial regulation's Article 45(8) and (9) for the financial year 2020.

A total of 254 financial transactions were scrutinised, representing 16.38 % of all the Agency's financial transactions and 80.38 % of the Agency's budget.

Four recommendations were made and none of them was critical. In particular, the financial delegations and underlying financial circuit have since been revised and its implementation has been taken effect as from 1st January 2021. Acknowledging the efforts made by ENISA, the ECA has deemed that these weaknesses have been properly addressed by ENISA as the related observations have been flagged as completed in its follow-up of previous year's observations in its 2021 annual audit report of the Agency.

8 FOLLOW UP OF RECOMMENDATIONS AND ACTION PLANS FOR AUDITS AND EVALUATIONS

As highlighted in Sections 2.7.1 and 2.7.2 above, ENISA took the necessary steps to address the ECA and IAS findings.

All recommendations from past audits have been addressed, with the exception of the three remaining important recommendations from the IAS 2019 audit on HR management, which will be implemented in accordance with the new agreed timeline.

9 FOLLOW-UP OF RECOMMENDATIONS ISSUED FOLLOWING INVESTIGATIONS BY THE EUROPEAN ANTI-FRAUD OFFICE

The recommendations issued by the European Anti-Fraud Office were endorsed by the Agency during 2021, following all the necessary steps provided in the regulatory framework.

10 FOLLOW-UP OF OBSERVATIONS FROM THE DISCHARGE AUTHORITY

In relation to the 2020 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 2020 financial year. The closure of the Agency's accounts for the 2020 financial year was also approved by the discharge authority.

In reply to observations and comments made by the European Parliament in its discharge of 2020, the Agency provided further information on actions taken to address previously identified areas for improvement and highlighted some actions taken that are 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 the concerns on recruitment and gender balance, ENISA redefined its recruitment strategy as from 2020;
- the sensitive post policy was adopted by the Executive Director on 22 December 2021.

11 ENVIRONMENTAL MANAGEMENT

The Greek authorities concluded a lease agreement on behalf of ENISA for its headquarters building in Athens, which was fully operational as of 1 July 2021. The building and office space are rented by the Greek authorities for ENISA's use. No longer occupying a shared building will enable ENISA to set a wider set of green measures to be implemented, as all electrical systems such as heating/cooling/lighting will be directly controlled by the agency, therefore enabling it to directly monitor those systems and assess the impact of any greening measures implemented. During the set-up of the new office, the path to

6 Available online (<https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60922>).

7 Available online (<https://www.enisa.europa.eu/news/enisa-news/securing-eu-institutions-bodies-and-agencies>).

carbon neutrality was already visible. The agency renovated the office space to better align with operational needs and incorporate considerations of greater energy savings and responsible energy consumption.

12 ASSESSMENT BY MANAGEMENT

The achievement of the work programme was far ahead of management's expectations across many areas thanks not only to the new streamlined organisational structure, which mirrors the CSA and ENISA's strategy, but also to the additional processes such as the inception and closure of projects by the Management Team.

The introduction of inception and closure of all operational projects by the Management Team allowed for enhanced synergies and efficiencies

across the Agency, and ensured that stakeholders were consulted to align the outcomes of the project with their needs. Project managers were asked to present their project plans according to a predefined template of questions. The Management Team would assess the projects objectives, the quality of the plans and resources required, including stakeholders' input into the scope of the project, after which the Management Team provided its own input and the project was approved for implementation. Project closures followed a similar process, in which project managers presented the outcome of the work to the Management Team, including feedback from stakeholders, after which the Management Team provided input and the project was deemed delivered.

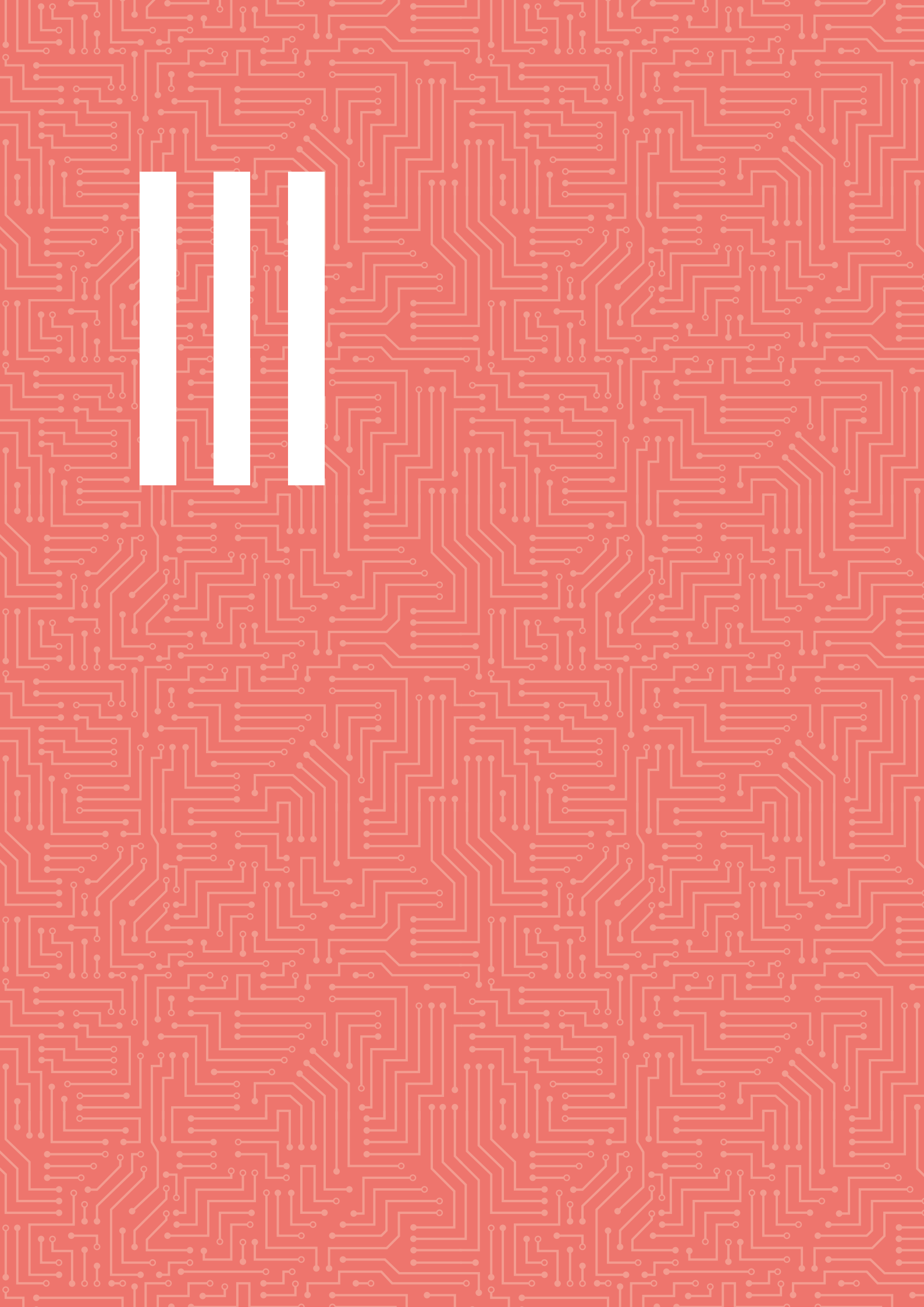
The achievement of the work programme has been described in detail under each of the activities, including the added value of each of the outputs.

PART II (B)

EXTERNAL EVALUATIONS

In 2021, ENISA continued to follow up actions from the *ex-post* evaluation of 2019 performed by external consultants. The key findings of the report were presented using the following criteria: effectiveness, efficiency, coherence and coordination, relevance, and EU added value. These findings were followed by an action plan composed of concrete recommendations to adjust and improve ENISA's activities. Recommendations included the reworking of KPIs, balancing and tailoring the agency's activities and outputs, and finally reinforcing the position of the Agency within the cybersecurity ecosystem.

To this end the Agency developed new KPIs and metrics to measure the performance of each of the activities. These KPIs and metrics are being reported for the first time in the 2021 annual activity report and will be used as a basis for measuring performance in the years to come. The activities and outputs in the work programme of the Agency are now aligned with the relevant articles of the CSA, thus providing a coherent way to measure the performance of each activity against the mandate of the Agency.



PART III

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

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 (COSO) (<https://www.coso.org>).

In this context, ENISA adopted its internal control framework by Management Board Decision MB/2019/12. It is based on the relevant framework of the European Commission (which follows the COSO framework) and includes five internal control components and 17 internal control principles.

The five internal control components are the building blocks that underpin the structure of the framework. They are interrelated and must be present and effective at all levels of ENISA for internal control over operations to be considered effective.

Each component comprises one or more internal control principles. 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.

In order to assess the components and principles of the internal control framework, a set of 57 indicators has been adopted (as part of MB/2019/12). 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, which is conducted on an annual basis. For 2021, this assessment was based on the indicators of the framework, as well as additional information from specific (risk) assessment reports, audit findings and other relevant sources. The assessment also followed the related guidance and templates developed under the EU Agencies Performance Development Network.

1.1 Assessment of control environment component

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

Principle 1: ENISA demonstrates commitment to integrity and ethical values

The Agency promotes yearly training on ethics and integrity. The management encourages all staff to take these courses. In order to increase the level of

participation, the Agency will consider a diversity of training plans/programmes to address different levels of staff knowledge/maturity. Various types of information material are at the disposal of the staff, such as training content and the most up-to-date reports by the Commission's Investigation and Disciplinary Office. ENISA's code of conduct, including the code of good administrative behaviour, is due to be published in 2022.

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

The declaration of assurance of the Executive Director is included in the annual activity report (Part V). All authorising officers by delegation signed their own declarations of assurance covering their areas.

Following the ECA's 2020 audit finding (reported in ENISA's 2020 AAR) regarding the lack of delegation for a staff member, the Agency took immediate action in 2021 to assess if the use of ENISA's financial resources had respected the principle of sound financial management, in particular in the context of any situation giving rise to potential conflicts of interests. In addition, corrective actions were taken as regards the delegation of authorising officers and relevant internal controls.

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

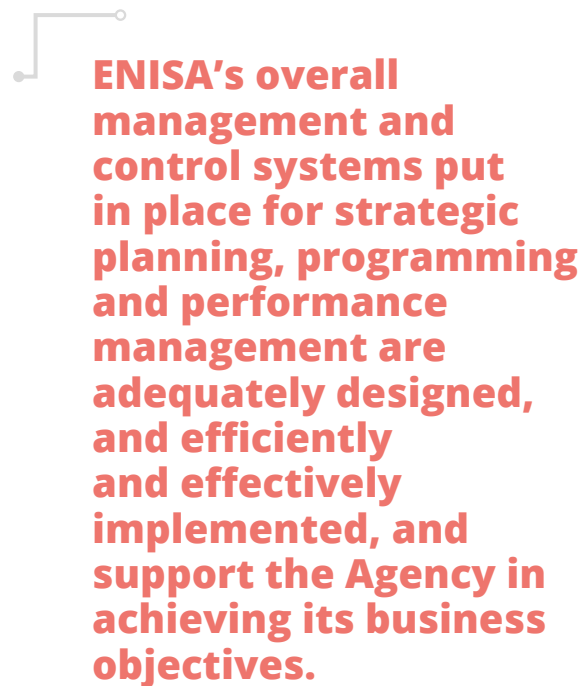
Every month the Agency publishes on its intranet the adopted and updated organisation charts. The organisation charts are updated based on the Agency's overall objectives.

The Executive Director's Decision 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. The 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 three months after the change of the person of the Executive Director, unless the new Executive Director explicitly confirms the delegations in place.

The IAS conducted an audit on strategic planning, programming and performance management in ENISA in 2021. According to the IAS draft audit report

(final report to be published in 2022), ENISA's overall management and control systems put in place for strategic planning, programming and performance management are adequately designed, and efficiently and effectively implemented, and support the Agency in achieving its business objectives. The three potential inconsistencies that have been identified by the IAS (in the areas of staff appraisal and performance assessment, performance management guidelines, and project management guidelines) will be addressed under ongoing actions during 2022.

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

A callout box with a red border and a white background, containing a large red text block. A thin grey line connects the top-left corner of the box to the main text area above it.

ENISA's overall management and control systems put in place for strategic planning, programming and performance management are adequately designed, and efficiently and effectively implemented, and support the Agency in achieving its business objectives.

The publication of ENISA's vacancy notices in 2021 was widely advertised via various channels (including ENISA's website and specific platforms such as Euractiv).

The turnover of staff was low (3 %) in 2021, which shows ENISA's ability to retain staff members in the Agency.

All staff members performed their CDRs within 2021; the relevant dialogues were held between the staff members and their line managers.

In order to develop and retain competent individuals, a learning and development policy is adopted every year. This policy is detailed and includes the training plan as well as the budgetary resources needed.

Internal mobility is available to all staff. Two possibilities are offered to the staff. They can apply for internal vacancies or request internal mobility during the CDR exercise. In addition, staff members had the possibility in 2021 of participating in the horizontal teams, established under the new organisational structure, which also constitutes a form of internal mobility.

In 2021 a task force was established by the Executive Director to review the large-scale recruitment exercise of 2020 (temporary agents / contract agents / heads of unit) with a view to establishing lessons learned and providing resultant recommendations for the future. The task force's observations will be further analysed and considered in the context of the Agency's broader recruitment policy.

Principle 5: ENISA holds accountable for their internal control responsibilities in the pursuit of objectives

The Agency reviews its annual objectives during the year. While mid-term reviews are planned, significant effort is put on into 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 a clear view and follow-up of the annual objectives during the whole year.

In order to be able to deliver the amended or new objectives, some job descriptions can be reviewed when needed. In 2021, there was no revision of job descriptions, as a detailed exercise was performed in 2020 during the Agency's reorganisation.

The staff's efficiency, abilities and conduct in the service are assessed annually against the expected standards of conducts and set objectives. Promotion of staff is decided after consideration of the comparative merits of eligible staff, taking into account their appraisal reports.

1.2 Assessment of risk assessment component

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

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

On the basis of ENISA's strategy, adopted in 2020, the Executive Director's Decision 35/2020 on the internal structures was adopted, elaborating in detail the mission statements of all units and teams (amended by Decision 3/2022 to reflect the latest organisational structure and consequent mission statements).

In addition, the adoption of ENISA's SPD is based on input from all units and teams across the Agency, and consultation with stakeholders, before being formally adopted by the agency's Management Board. Throughout the year, the agency's outputs are inceptioned, reviewed and finalised in close consultation with the stakeholders, including ENISA's Management Board, Advisory Group and NLO Network.

ENISA uses objectives as a basis for allocating resources to achieve policy, operational and financial performance goals. In 2021, the Agency's budget implementation rate was 99.51 %, while the budget outturn was 98.57 %.

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

ENISA identifies and assesses risks at the various organisational levels, analysing internal and external factors. Management and staff are involved in the process at the appropriate level. ENISA estimates the significance of the risks identified and determines how to respond to significant risks, considering how each one should be managed and whether to accept, avoid, reduce or share the risk.

While risks are identified in the context of different processes (during the inception/revision/finalisation of projects, as part of the business continuity project, in the yearly ICT security risk assessments, in the assessment of sensitive functions, etc.), a holistic centralised risk management approach has not yet been implemented at Agency-wide level. To this end, in 2022 ENISA will kick off the development of a formalised enterprise risk management methodology that will be used to consolidate risks and contribute to the maintenance and continuous updating of a central ENISA risk register.

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

The Agency's anti-fraud strategy was updated in 2021 and formally adopted by Management Board Decision MB/2021/5. All objectives and actions for 2021 were delivered, with the exception of the code for good administrative behaviour, which is due for 2022. A dedicated web page was created on ENISA's intranet where all regulations, documents, training materials and a toolbox are now available to all the staff.

The course in fraud prevention is part of the training in ethics and integrity, and was delivered in 2021. An advanced course on fraud prevention and ENISA's anti-fraud strategy was scheduled for 2022.

Principle 9: ENISA identifies and analyses significant change

Change is managed via different processes within the Agency. At operational level, continuous monitoring of the work programme activities via 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 (IT Management Committee, Budget Management Committee, IPR Management Committee) further supports change management at corporate level. During the reporting year 2021, change and subsequent risks have been managed in this context, considering also changes arising from the external environment, as for example the change in tele-working conditions that was deemed necessary within 2021, due to the COVID-19 pandemic. The establishment of a comprehensive risk management framework within 2022 will further enhance the Agency's possibilities to identify and manage change. The maintenance of a centralised risk register is part of this framework.

1.3 Assessment of control activities component

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

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

Under the new ENISA organisational structure there is continuous monitoring of performance, at both the beginning (inception) and closure (finalisation) of

projects, as well as throughout the year with reporting and/or validation at the weekly Management Team meetings. In addition, both the scope and the performance of the indicators are continuously validated with external stakeholders, in particular the NLO Network and ENISA's Advisory Group, as well as various ad hoc working groups established in different thematic areas.

In order to ensure a high level of control, the Agency applies ex-ante verification to 100 % of its financial transactions. In order to complete this control, an ex-post control verification is performed every year. In 2021, a sample of 254 transactions was selected, following ENISA's relevant policy/guidelines for ex-post verification. These transactions represent 80.38 % of the total by value and 16.38 % by volume.

Roles and responsibilities are being reviewed within the Agency with a view to ensure segregation of duties where needed. Identified weakness identified by the European Court of Auditors in the area of internal controls has been addressed through the reorganisation. Another area that requires risk mitigation is the ENISA Financial sector that is currently led by the acting Head of Sector who is also in charge for accounting and compliance. A new recruitment is planned in the course of 2022.

While controls were integrated into different processes (e.g. inception process, validation with stakeholders, management committees), the holistic internal control assessment was not fully formalised at Agency-wide level. In addition, further development of the Agency's business continuity plan is needed. The internal control framework assessment for 2021 provided specific recommendations to address these elements.

In 2021, the sensitive functions policy was adopted by the Executive Director's Decision 2021/86 (entering into force in May 2022). The decision provides a high-level methodology for defining the sensitive functions at ENISA, together with broad categories of mitigation measures that can be applied to manage the risks. Following the adoption of the decision, the first risk assessment of the Agency's sensitive functions was conducted by the Executive Director's Office in March 2022. This risk assessment defined the sensitive functions at Agency level. The risk assessment (methodology and result) was endorsed by ENISA's Management Team in March 2022.

Principle 11: ENISA selects and develops general control over technology to support the achievement of objectives

In 2021, following a proposal by ENISA's ITMC, the Agency adopted its IT strategic framework, which also covers information security at strategic level. In addition, following the Commission's draft proposal for the regulations on common binding cybersecurity rules and on information security, a process for reviewing the agency's IT security framework was initiated and will be continued in 2022.

In order to ensure a high level of control, the Agency applies ex-ante verification to 100 % of its financial transactions.

Every year, the Agency performs an IT security risk assessment (under the control of ENISA's Information Security Officer). The IT security risk assessment was concluded in 2021. A broader IT risk assessment, however, including a business continuity plan, was not conducted at the Agency. Still, a register of all IT systems at the Agency (and their owners) was created, as part of ENISA's IT strategy.

The Agency uses a register in which security incidents and personal data breaches are recorded. In particular, each security incident or personal data breach is documented in the register based on specific incident-reporting templates (including date, description of incident, those involved, causes, risk assessment and actions taken).

In 2021 there was one incident that was assessed as potentially being of high risk. In particular, in July 2021, due to the exploitation of a zero-day vulnerability, unauthorised access was obtained to a number of mailboxes of the Agency's corporate email server. The incident did not affect any other corporate or operational system of ENISA and did not pose any threat to ENISA's operational mandate. Once the incident was identified, ENISA, in co-operation with CERT-EU and competent authorities, conducted a full forensic investigation. The findings

have been shared with all relevant parties and Member States. ENISA took immediate actions to contain the event and assess its impact. All necessary actions were taken in compliance with the Regulation (EU) 1725/2018, including the timely notification of the European Data Protection Supervisor.

In addition, an internal Task Force was created to establish the technical facts that led to the incident. The Task Force report, which was submitted to the ED on December 2021, demonstrated a number of gaps in the IT governance at ENISA, as well as in the related IT policy and procedural framework. The task force recommended a number of corrective actions to that end (action plan), which were endorsed by the Agency's Management Team and further presented to and adopted by the ENISA's Management Board. The action plan includes specific timelines and responsible actors within ENISA for all foreseen actions.

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

In 2021, the majority of recommendations stemming from the IAS performance audits were addressed and submitted to IAS. However, there are still some open findings to be addressed in 2022.

The Agency keeps its register of exceptions updated on a yearly basis. There is a dedicated workflow in Paperless to report an exception. The workflow contains the link to the form that needs to be filled in by those responsible for the exception.

For 2021, three exceptions are reported herein, none of them of a critical nature, as follows.

1. While the timelines of the staff appraisal exercise were respected, there was a delay in the timeline for reclassification; in particular, the appeal period had to be shortened by 5 working days, which is a deviation from the Agency's relevant rule (MB/10/16), which allows 10 working days for staff members to appeal. The delay was due to additional validation of the data, which was necessary in order to meet ENISA's obligations and ensure an equal and fair comparison of merits for all ENISA staff.
2. A service contract for cleaning services for the amount of EUR 28 000 was awarded directly (extension of the service with the same contractor), instead of launching a procurement procedure. The exception was necessary for business continuity purposes and did not expose the agency to any serious legal risk.

3. In 2021, the Agency paid the amount of EUR 18 800 and committed an additional amount of EUR 24 900 (equivalent to a total expenditure of EUR 43 700) for Greek value added tax (VAT), which was not exempted by the local Greek administration in due time. This issue mainly relates to invoices issued before 2020 for which the non-exemption of VAT was identified only in 2021. The VAT exemption process has since been revised to improve its monitoring by processing digital copies instead of using hard copies, which left an insufficient audit trail of the work performed.

The Agency performs a yearly external *ex-post* evaluation of its activities based on the effectiveness, efficiency, coherence, coordination and added value of its activities.

1.4 Assessment of information and communication component

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

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

The Agency registers and archives all its official documents (outgoing and incoming) in a specific registration system. In 2021 the Agency kicked off its migration to the ARES registration system of the European Commission. The completion of this project is expected in 2022. This new development supports the principle of single administration (same tools and processes used by staff internally) within ENISA.

ENISA uses various tools for internal communications. The most common tools are ENISA's intranet, email, Skype for Business and WebEx.

The Agency can retrieve 100 % of the documents requested by the IAS/ECA. All documents are archived in ENISA's intranet, Paperless and financial report requests using Business Object and ABAC.

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

There is transparency in the Agency regarding objectives, challenges, actions taken or to be taken, and results achieved. The minutes of the weekly

Management Team meetings minutes are made available by email to all staff. In addition, weekly question and answer sessions for all staff on different aspects of the new MIP organisation were organised throughout 2021.

Mid-term reviews are used to communicate objectives achieved and ongoing, while substantial effort is put into *ex-ante* evaluation of the projects, starting with a detailed inception proposed during the Management Team meetings. The same projects may then be reviewed for guidance during the Management Team meetings and will then be presented to the Management Team for finalisation. This ensures a clear view and follow-up of the annual objectives during the year.

There is a separate communication line for whistleblowing arrangements. The basic principles, definitions and reporting mechanism are described in ENISA's whistleblowing policy.

Principle 15: ENISA communicates with external parties about matters affecting the functioning of internal control

The Agency's press coverage is monitored monthly and quarterly, detailing the media used. The most recent corporate communication strategy is from May 2021. While certain actions under the communication strategy have been endorsed at Management Team level, the Agency is also working to provide the new stakeholder strategy (to take effect during 2022). The awareness raising and education team actively cooperates with the communication sector (under the Executive Director's Office) on ENISA's stakeholder strategy.

The Agency communicates about its internal control matters through the annual activity report.

1.5 Assessment of monitoring activities component

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

Principle 16: ENISA obtains or generates and uses relevant quality information to support the functioning of internal control

ENISA continuously monitors the performance of the internal control system with tools that make it possible to identify internal control deficiencies, register and assess the results of controls, and control deviations and exceptions.

The Agency follows up, in a timely manner, the recommendations of the auditors, as well as risks identified in the *ex-ante* and *ex-post* controls and relevant evaluations. While four recommendations were closed by the IAS during 2021, following the corrective actions implemented by ENISA, three important recommendations remain open and have not been fully implemented within the set time frame. The delays are mainly imputable to the reorganisation of ENISA stemming from the adoption of the CSA. This affected the roll-out of the HR corrective plan as initially planned with the IAS in late 2019. A new timeline to implement the three remaining recommendations was agreed with the IAS.

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

The deficiencies are communicated to the parties responsible and to the Management Team. Mitigation measures are addressed immediately. They are planned and have a date for implementation. The Agency follows up these deadlines closely as well as the result of the mitigation measures proposed.

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 of the Agency, taken together, facilitate its effective and efficient operation, help to ensure the quality of internal and external reporting, and help to ensure compliance with its regulations. That being said, some improvements are needed in certain principles, in order to increase effectiveness and ensure proper implementation of the internal controls in the future. These improvements include the refinement of the Agency's internal control framework indicators, the establishment of an enterprise risk management framework, the revision of the IT governance and underlying policy and procedural framework, the revision of the Agency's recruitment policy, as well as the update of the Agency's Business Continuity Plan. The follow up on these improvements will be assessed for the next mid-term review of the Agency.

3 STATEMENT OF THE INTERNAL CONTROL COORDINATOR IN CHARGE OF RISK MANAGEMENT AND INTERNAL CONTROL

I, the undersigned,

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

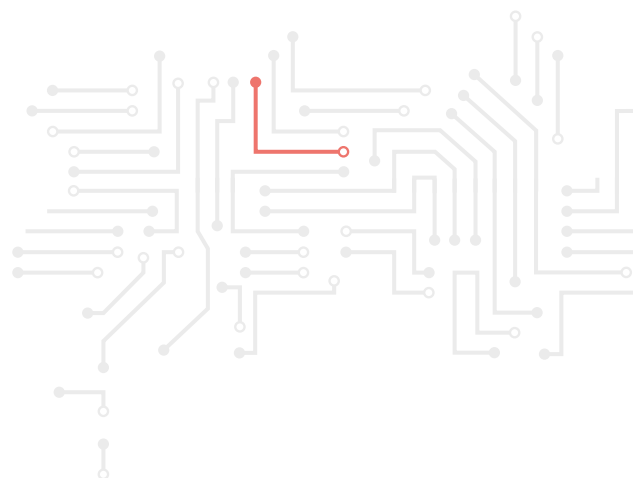
in my capacity as manager in charge of risk management and internal control, declare that, in 2021 risk management and internal controls was responsibility of the Executive Directors Office and this area was identified in problem analysis that led to reorganisation of ENISA effective as of 2021. In accordance with ENISA's internal control framework, I have reported my advice and recommendations on the overall state of internal control in the Agency to the Executive Director.

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

Athens, 30th June 2022



Ingrida Taurina



The image features a large, bold, white letter 'W' centered in the upper half. The background is a solid light blue color, overlaid with a dense, repeating pattern of white lines that form a complex circuit board or PCB layout. The lines are thin and create a maze-like structure of interconnected paths, with small circular nodes at various points along the lines. The overall aesthetic is clean, modern, and tech-oriented.

W

PART IV

MANAGEMENT ASSURANCE

1 REVIEW OF THE ELEMENTS SUPPORTING ASSURANCE

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

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

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

2 RESERVATIONS

Considering the results of the 2021 annual audits performed by the ECA and the IAS, the 2021 results of the internal controls (*ex-post* controls, review of the register of exceptions, internal control framework assessment) and the 2021 results of the key financial and operational indicators, the authorising officer can conclude that ENISA operated in 2021 in such a way as to manage the risks appropriately.

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



V

PART V

DECLARATION OF ASSURANCE

I, the undersigned,

Juhan LEPASSAAR,

Executive Director of the European Union Agency for Cybersecurity,

in my capacity as authorising officer,

declare that the information contained in this report gives a true and fair⁸ view of the state of the Agency's affairs, and state that I have reasonable assurance that the resources assigned to the activities described in this report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

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

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

Athens, 30th June 2022



Juhan LEPASSAAR
Executive Director

⁸ True and fair in this context means reliable, complete and accurate.

The image features a large, bold, white capital letter 'A' centered in the upper-left quadrant. The background is a vibrant green color, overlaid with a complex, repeating pattern of white lines and small circles that resemble a printed circuit board (PCB) or a digital network. The lines are thin and form a dense, interconnected web of paths, with small circular nodes at various points along these paths. The overall aesthetic is clean, modern, and tech-oriented.

A

ANNEX 1

CORE BUSINESS STATISTICS

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
ENISA's added value to EU institutions, bodies and Member States in providing support for policymaking (<i>ex-ante</i>)				
1.1. Number of relevant contributions to EU and national policies and legislative initiatives	Number	Annual	Manual collection from staff members	193
Contributions to task forces and bodies	%	Annual	Manual collection from staff members	13 % of 193
Contributions to workshops and conferences	%	Annual	Manual collection from staff members	83 % of 193
Support actions/contributions to European Commission and Member States for policies and legal initiatives following relevant requests	%	Annual	Manual collection from staff members	3 % of 193
1.2. Number of references to ENISA reports, analysis and/or studies in EU and national policy documents		Biennial		N/A
1.3. Satisfaction with ENISA's added value and weight of contributions		Biennial	Survey	N/A
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
NISD	Number	Annual	Manual collection from staff members	1
EECC	Number	Annual	Manual collection from staff members	1

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
e-IDAS	Number	Annual	Manual collection from staff members	1
5G	Number	Annual	Manual collection from staff members	1
Network CODE on cyber security (NCCS)	Number	Annual	Manual collection from staff members	1
2.2. Number of ENISA reports, analyses and/or studies referred to at EU and national levels		Biennial	Survey	N/A
2.3. Satisfaction with ENISA's added value and weight of support		Biennial	Survey	N/A
Increased resilience against cybersecurity risks and preparedness to respond to cyberincidents				
3.1. Increase/decrease in maturity indicators				
Maturity of national cybersecurity strategies				
Number of Member States that rate the overall maturity of their cybersecurity strategy				
High maturity	Number	Annual	Survey	3
Medium maturity	Number	Annual	Survey	4
Low maturity	Number	Annual	Survey	3
Number of Member States planning to use ENISA framework to measure the maturity of their national cybersecurity capabilities				
Already using	Number	Annual	Survey	1
Not using but planning to use	Number	Annual	Survey	5
Don't know or will not use in the foreseeable future	Number	Annual	Survey	4
Number of Member States that have set KPIs to measure progress and effectiveness of the implementation of their strategic objectives when drafting their NCCSS				
Already using	Number	Annual	Survey	3
Not set but planning to use	Number	Annual	Survey	4
Don't know or have not set KPIs currently and will not set KPIs	Number	Annual	Survey	3
The frequency with which Member States update their strategy to adapt to technological advancements and new threats				
Every 2-3 years	Number	Annual	Survey	2
Every 4-5 years	Number	Annual	Survey	6
More than 6 years or don't know	Number	Annual	Survey	2
Total maturity of ISACs (self assessment)	%	Annual	ISAC dashboard	63 %
ISAC A	%	Annual	ISAC dashboard	60 %
ISAC B	%	Annual	ISAC dashboard	56 %
ISAC C	%	Annual	ISAC dashboard	90 %

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
ISAC D	%	Annual	ISAC dashboard	50 %
ISAC F	%	Annual	ISAC dashboard	63 %
3.2. Outreach, uptake and application of lessons learned from capability-building activities				
CySOPEx 2021 (number of improvements proposed by participants)	Number	Per exercise		5
3.3. Number of cybersecurity programmes (courses) and participation rates				
Total number of students enrolled in the first year of the academic programmes (2020)	Number	Annual	Report ⁹	4 843
Number of male students	%	Annual	Report	80 %
Number of female students	%	Annual	Report	20 %
Total number of cybersecurity programmes (2020)	Number	Annual	Report	119
Number of postgraduate programmes	%	Annual	Report	6 %
Number of master's programmes	%	Annual	Report	77 %
Number of bachelor's programmes	%	Annual	Report	17 %
3.4. Stakeholder assessment of the usefulness, added value and relevance of ENISA capacity-building activities (survey)				
CySOPEx 2021 exercise				
Usefulness low	%	Per exercise	Survey	0 %
Usefulness medium	%	Per exercise	Survey	57 %
Usefulness high	%	Per exercise	Survey	43 %
Relevance low	%	Per exercise	Survey	4 %
Relevance medium	%	Per exercise	Survey	50 %
Relevance high	%	Per exercise	Survey	46 %
CyberSOPEx 2021 exercise				
Usefulness low	%	Per exercise	Survey	22 %
Usefulness medium	%	Per exercise	Survey	77 %
Usefulness high	%	Per exercise	Survey	0 %
Relevance low	%	Per exercise	Survey	0 %
Relevance medium	%	Per exercise	Survey	54 %
Relevance high	%	Per exercise	Survey	45 %
Blue OLEx 2021 exercise				
Usefulness low	%	Per exercise	Survey	5 %
Usefulness medium	%	Per exercise	Survey	77 %
Usefulness high	%	Per exercise	Survey	18 %

⁹ <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
Relevance low	%	Per exercise	Survey	7 %
Relevance medium	%	Per exercise	Survey	55 %
Relevance high	%	Per exercise	Survey	38 %
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				
CSIRT network				
Active users increase from 2020	%	Annual	Platform	115 %
Number of exchanges/interactions increase from 2020	%	Annual	Platform	291 %
CyCLONe				
Active users increase from 2020	%	Annual	Platform	143 %
Number of exchanges/interactions increase from 2020	%	Annual	Platform	1011 %
4.2. Uptake of platforms/tools/SOPs during massive cyberincidents				N/A
4.3. Stakeholder satisfaction with the relevance and added value of platforms/tools/SOPs provided by ENISA	N/A	Biennial	Survey	N/A
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 for which ENISA contributes to mitigation efforts	N/A	Biennial	Survey	N/A
5.2. Stakeholder satisfaction with ENISA's ability to provide operational support	N/A	Biennial	Survey	N/A
1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions				
2. Effective preparation of candidate certification schemes prepared by ENISA				
6.1. Number of stakeholders (governments or commercial solution providers) in the EU market using the cybersecurity certification framework for their digital solutions				
Percentage of respondents planning to use the cybersecurity schemes to have solutions certified	%	Annual	Survey	24 %
Percentage of respondents planning to use the cybersecurity schemes to use certified solutions	%	Annual	Survey	37 %
Percentage of respondents planning to use the cybersecurity schemes to certify solutions	%	Annual	Survey	44 %
Percentage of respondents planning to refer to certifications within regulations	%	Annual	Survey	36 %
Percentage of respondents planning to use the EUCC	%	Annual	Survey	53 %
Percentage of respondents planning to use the EUCS	%	Annual	Survey	49 %
Percentage of respondents that need assistance from ENISA during their preparation for using the EU certification schemes	%	Annual	Survey	66 %

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
6.2. Citizens' trust in digital solutions		Biennial	Survey	N/A
6.3. Satisfaction with ENISA's support for the preparation of candidate schemes		Biennial	Survey	N/A
Recognition 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	2
7.2. Uptake of lessons learned / recommendations from ENISA reports				
Percentage of respondents interested in using ENISA's good practice on market analyses	%	Annual	Survey	87 % fully or partly interested
Percentage of respondents interested in using ENISA's standards mapping related to 5G	%	Annual	Survey	84 % high and medium interest
Percentage of respondents interested in using ENISA's standards mapping related to the IoT	%	Annual	Survey	88 % high and medium interest
Percentage of respondents interested in using ENISA's risk-based approach for their cybersecurity certification activities	%	Annual	Survey	72 % high and medium interest
Percentage of respondents interested in using ENISA's consolidated certification labelling process	%	Annual	Survey	84 % high and medium interest
Percentage of respondents interested in using ENISA's vulnerability management process for certified products, services and processes	%	Annual	Survey	82 % high and medium interest
7.3. Stakeholder satisfaction with the added value and quality of ENISA's work	%	Biennial	Survey	N/A
ENISA's ability to contribute to Europe's cyber resilience through the provision of timely and effective information and knowledge				
8.1. Number of users and frequency of use of a dedicated portal (observatory)				N/A
8.2. Total number of recommendations, analyses and challenges identified and analysed	Number	Annual	ENISA reports and studies	288
Threat landscape supply chain	% of total	Annual	ENISA reports and studies	13 % (37 of 288)
Foresight	% of total	Annual	ENISA reports and studies	6 % (17 of 288)
ENISA threat landscape report 2021	% of total	Annual	ENISA reports and studies	46 % (132 of 288)
Crypto assets	% of total	Annual	ENISA reports and studies	0.3 % (1 of 288)
Securing machine learning	% of total	Annual	ENISA reports and studies	19 % (55 of 288)

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
Cybersecurity index	% of total	Annual	ENISA reports and studies	10 % (29 of 288)
PQC integration	% of total	Annual	ENISA reports and studies	0.3 % (1 of 288)
Healthcare CSIRT	% of total	Annual	ENISA reports and studies	4 % (12 of 288)
8.3. Stakeholder satisfaction with the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges and opportunities, including in research		Biennial	Survey	N/A
Level of awareness of cybersecurity, cyber hygiene and cyber literacy across the EU				
9.1. Number of activities and participation in awareness-raising actions organised by ENISA on cybersecurity topics				
Women4Cyber campaign				
Social media impressions	Number	Annual	Social Media (Facebook, LinkedIn, Twitter)	201188
Social media engagements	Number	Annual	Social Media (Facebook, LinkedIn, Twitter)	3 865
Video views	Number	Annual	YouTube	1 283
Cybersecurity for SMEs campaign				
Social media impressions	Number	Annual	Social Media (Facebook, LinkedIn, Twitter)	44 497
Social media engagements	Number	Annual	Social Media (Facebook, LinkedIn, Twitter)	957
Video views	Number	Annual	YouTube	736
Website visits	Number	Annual	ENISA website	24 362
Media references	Number	Annual	Media monitoring	~ 40
Participation in events	Number	Annual	Website announcements	5
NoMoreRansom campaign				
Social media impressions	Number	Annual	Social media (Twitter)	54 022
Social media engagements	Number	Annual	Social media (Twitter)	465
ECSM campaign				

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
Social media impressions	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	20 400 000
Social media engagements	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	110 266
Video views	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	2 018 441
Website visits	Number	Annual	ENISA analytics plus Facebook and Twitter built-in tools and social media monitoring platform of contractor	47 939
Certification campaign				
Social media impressions	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	85 599
Social media engagement	Number	Annual	Social media (Facebook, LinkedIn, Twitter)	1 701
Video views	Number	Annual	YouTube	669
Website visits	Number	Annual	ENISA website	1 239
CyberHEAD campaign				
Social media impressions	Number	Annual	Social media	25 292
Social media engagements	Number	Annual	Social media	466
Website visits	Number	Annual	ENISA website	49 964
9.2. Level of awareness of cybersecurity across the general public in the EU (e.g. EU barometer)		Biennial		N/A
Organisational performance culture				
10.1. Proportion of key performance indicators reaching targets				N/A
10.2. Individual contributions to achieving the objectives of the agency through clear links to key performance indicators (CDRs)				

KPI Metric	Unit (of measurement)	Frequency	Data source	Results	
Policy development and implementation unit	%	Annual	Objectives 2021	100 %	
Capacity building unit	%	Annual	Objectives 2021	23 %	
Operation cooperation unit	%	Annual	Objectives 2021	85 %	
Market, certification and standardisation unit	%	Annual	Objectives 2021	22 %	
Executive directors office	%	Annual	Objectives 2021	47 %	
Corporate support services	%	Annual	Objectives 2021	38 %	
10.3. Exceptions in the risk register	Number	Annual	Internal control	16	
Deviation from financial regulations	Number	Annual	Internal control	14	
Deviation from staff regulations	Number	Annual	Internal control	2	
10.4. Number of complaints filed against ENISA, including number of inquiries/complaints submitted to the European Ombudsman	Number	Annual	See below	19	
To European Ombudsman	%	Annual	ENISA functional mailbox	16 % of 19	
Under Article 90	%	Annual	Internal control files	79 % of 19	
Under Article 24	%	Annual	Internal control files	0	
To EDPS	%	Annual	Internal control files	5 % of 19	
10.5. Results of the annual risk assessment exercise					
10.6. Observations from external audit bodies (e.g. ECA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings)	Number	Annual	See below	4	
IAS	Number	Annual	IAS Section 2.7.1	Three important recommendations	
ECA	Number	Annual	ECA Section 2.7.2	One critical observation	
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)				Results 2020	Results 2021
Percentage of staff seeing a positive atmosphere within ENISA since the reorganisation	%	Annual	Staff satisfaction survey	70 %	58 %
Percentage of staff feeling confident working within the new organisational culture	%	Annual	Staff satisfaction survey	61 %	68 %
Percentage of staff satisfied with their work	%	Annual	Staff satisfaction survey	74 %	80 %
Percentage of staff indicating their line manager provides sufficient feedback on their performance	%	Annual	Staff satisfaction survey	68 %	76 %

KPI Metric	Unit (of measurement)	Frequency	Data source	Results	
Percentage of staff indicating their line manager sets clear objectives	%	Annual	Staff satisfaction survey	66 %	76 %
Percentage of staff that feel well informed by ENISA leadership regarding important matters	%	Annual	Staff satisfaction survey	80 %	73 %
11.2. Quality of ENISA training and career development activities organised for staff					
Percentage of staff trusting that ENISA will support them in acquiring the necessary skills and capabilities to successfully manage the reorganisation	%	Annual	Staff satisfaction survey	49 %	
Percentage of staff indicating that courses match their training and development needs	%	Annual	Staff satisfaction survey	58 %	
Percentage of staff finding that their line manager dedicates enough time during the CDR dialogue for mapping training and development needs	%	Annual	Staff satisfaction survey	55 %	
Percentage 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	47 %	
Percentage of staff finding that they have had the opportunity to grow in their careers at ENISA since the reorganisation	%	Annual	Staff satisfaction survey	35 %	
11.3. Reasons for staff departure (exit interviews)	Scale 1-10	As required	HR files	7.1	
On a scale of 1 to 10, did the job you were employed for meet your expectations?	Scale 1-10	As required	HR files	7.5	
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	6.6	
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	7.75	
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	6.5	
On a scale of 1 to 10, what was your working relationship with your manager like?	Scale 1-10	As required	HR files	7.25	
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	8.4	
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	6.8	
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	6.6	
On a scale of 1 to 10, how would you rate your employee experience in the agency?	Scale 1-10	As required	HR files	6.6	
Turnover rates	%	Annual	HR files	3 %	

KPI Metric	Unit (of measurement)	Frequency	Data source	Results
11.4. Resilience and quality of ENISA IT systems and services				
Critical systems downtime	%	Annual	Uptime report of Fortimail appliance in Heraklion	99,38 %
Percentage of central IT infrastructure assessments with few (< 5) critical findings	%	Annual	Intranet repository of all proactive assessments and their findings	100 %
Percentage of central infrastructure patched to the last formal version of one year	%	Annual	Yearly IT maintenance plan in PDF	95 %
Percentage of major IT helpdesk requests resolved in a satisfactory way within two business days	%	Annual	Graph created from IT ticket repository (https://pbi.enisa.europa.eu/reports/powerbi/IT/IT%20Service%20Requests)	80 %
Percentage of staff indicating they were supported by ENISA's IT infrastructure for remote working	%	Annual	Staff satisfaction survey	76 %
Percentage of staff indicating that the IT help desk responds within a reasonable time	%	Annual	Staff satisfaction survey	75 %
Percentage of staff indicating that the IT central services are stable	%	Annual	Staff satisfaction survey	62 %
Percentage of staff finding the digital applications easy to use and that they cover job requirements	%	Annual	Staff satisfaction survey	67 %
Percentage of staff finding that digital applications for the job are supported in a timely manner	%	Annual	Staff satisfaction survey	65 %
Percentage of staff indicating that connectivity issues are resolved swiftly	%	Annual	Staff satisfaction survey	65 %

N/A, not applicable.

ANNEX 2

STATISTICS ON FINANCIAL
MANAGEMENT

Budget outturn and cancellation of appropriations (EUR)

Budget outturn	2019	2020	2021
Reserve from the previous years' surplus (+)			
Revenue actually received (+) ^a	16 740 086	21 801 460	23 058 211
Payments made (-)	- 11 980 352	- 15 050 421	- 17 989 374
Carryover of appropriations (-)	- 4 357 734	- 6 200 614	- 5 082 548
Cancellation of appropriations carried over (+)	62 522	180 023	209 385
Adjustment for carryover of assigned revenue appropriation from previous year (+)	116 393	10 403	125 622
Exchange rate differences (+/-)	- 1 802	- 1 291	- 428
Adjustment for negative balance from previous year (-)			
TOTAL	579 113	739 560	320 868

a Includes the contribution of EUR 219 110 received from the Greek authorities to cover office leasing expenditure

Execution of commitment appropriations in 2021 (EUR)

EUR	Chapter	Commitment appropriations authorised ^a	Commitments made	(%) Commitment rate
A-11	Staff in active employment	8 370 300	8 370 300	100.0%
A-12	Recruitment/departure expenditure	308 013	306 022	99.4%
A-13	Socio-medical services and training	1 375 038	1 371 493	99.7%
A-14	Temporary assistance	751 678	751 678	100.0%
	TITLE I	10 805 029	10 799 493	99.9%
A-20	Buildings and associated costs	1 322 229	1 312 041	99.2%
A-21	Movable property and associated costs	275 162	271 592	98.7%
A-22	Current administrative expenditure	692 222	686 263	99.1%
A-23	Information and communication technologies	1 614 011	1 585 422	98.2%
	TITLE II	3 903 624	3 855 317	98.8%
B-30	Activities related to outreach and meetings	535 859	504 740	94.2%
B-37	CSA Core operational activities	7 942 806	7 878 630	99.2%
	TITLE III	8 478 665	8 383 370	98.9%
	Total	23 187 318	23 038 179	99.4 %

a Commitment appropriations authorised include the budget voted by the budgetary authority, budget amendments and miscellaneous commitment appropriations for the period (e.g. internal and external assigned revenue).

Execution of payment appropriations in 2021 (EUR)

EUR	Chapter	Payment appropriations authorised ^b	Payments made	(%) Payment rate
A-11	Staff in active employment	8 370 300	8 370 300	100.0%
A-12	Recruitment/departure expenditure	308 013	257 056	83.5%
A-13	Socio-medical services and training	1 375 038	903 912	65.7%
A-14	Temporary assistance	751 678	559 667	74.5%
	TITLE I	10 805 029	10 090 935	93.4%
A-20	Buildings and associated costs	1 322 229	746 913	56.5%
A-21	Movable property and associated costs	275 162	9 116	3.3%
A-22	Current administrative expenditure	692 222	267 511	38.6%
A-23	Information and communication technologies	1 614 011	666 704	41.3%
	TITLE II	3 903 624	1 690 244	43.3%
B-30	Activities related to outreach and meetings	535 859	285 500	53.3%
B-36	CSA Core operational activities	7 942 806	5 921 696	74.6%
	TITLE III	8 478 665	6 207 195	73.2%
	Total	23 187 318	17 988 374	77.58 %

b Payment appropriations authorised include the budget voted by the budgetary authority, budget amendments and miscellaneous payment appropriations for the period (e.g. internal and external assigned revenue) (fund sources C1, C3, C4, R0).

Breakdown of commitments (with open amounts as of 31 December 2021) (EUR)

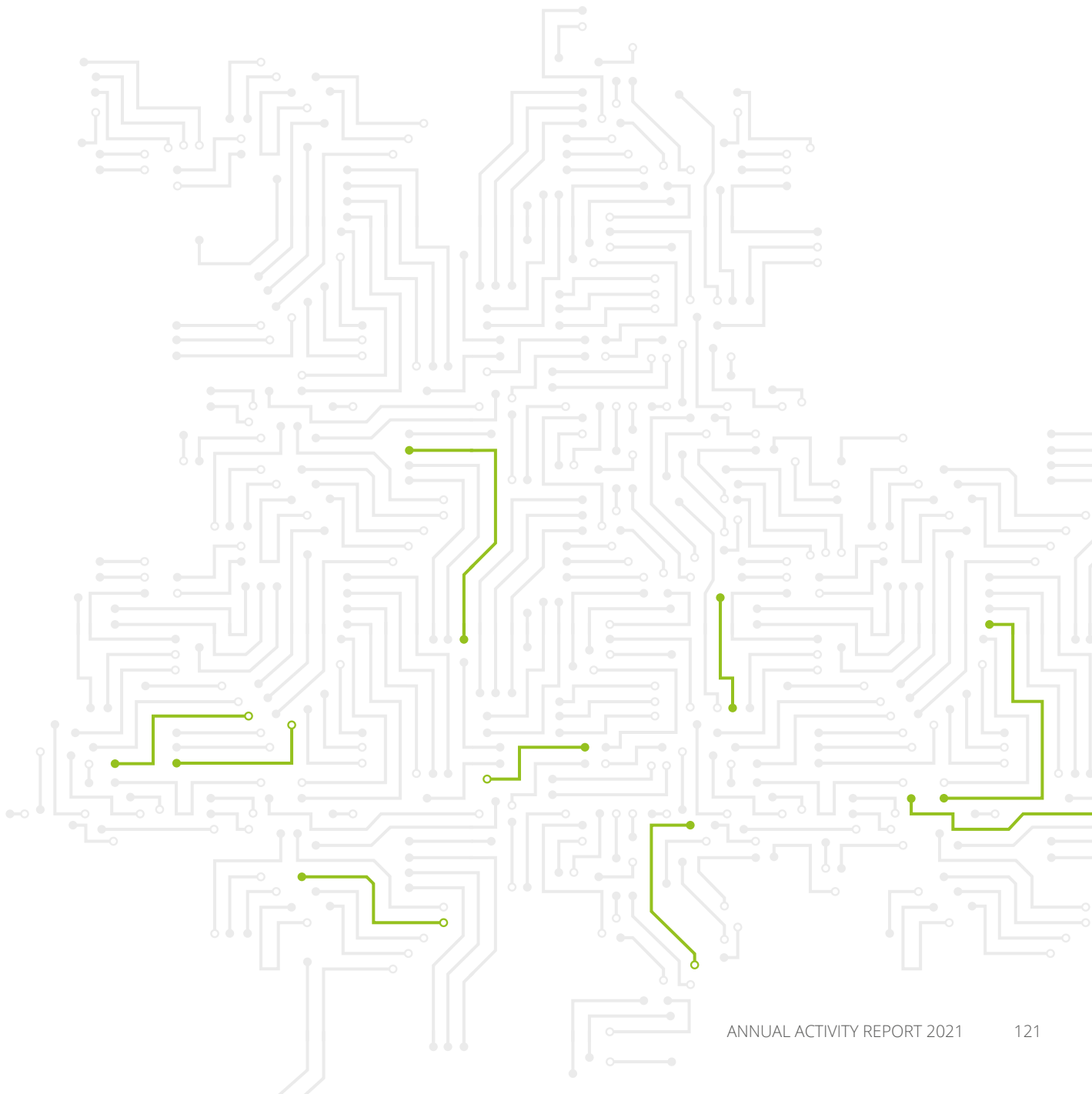
EUR	Chapter	Commitments made ^a	Payments made ^b	Amount to be paid in 2022	(%) Amount to be paid
A-11	Staff in active employment	8 370 300	8 370 300	-	0.0%
A-12	Recruitment/departure expenditure	306 022	257 056	48 966	16.0%
A-13	Socio-medical services and training	1 371 493	903 912	467 581	34.1%
A-14	Temporary assistance	751 678	559 667	192 011	25.5%
	TITLE I	10 799 493	10 090 935	708 558	6.6%
A-20	Buildings and associated costs	1 312 041	746 913	565 128	43.1%
A-21	Movable property and associated costs	271 592	9 116	262 476	96.6%
A-22	Current administrative expenditure	686 263	267 511	418 752	61.0%
A-23	Information and communication technologies	1 585 422	666 704	918 717	57.9%
	TITLE II	3 855 317	1 690 244	2 165 073	56.2%
B-30	Activities related to outreach and meetings	504 740	285 500	219 240	43.4%
B-36	CSA Core operational activities	7 878 630	5 921 696	1 956 934	24.8%
	TITLE III	8 383 370	6 207 195	2 176 174	26.0%
	Total	23 038 179	17 988 374	5 049 805	21.9%

a,b Commitments and payments made include the budget voted by the budgetary authority, budget amendments and miscellaneous commitment and payment appropriations for the period (e.g. internal and external assigned revenue) (fund sources C1, C3, C4, R0).

Revenue and income during 2021 (EUR)

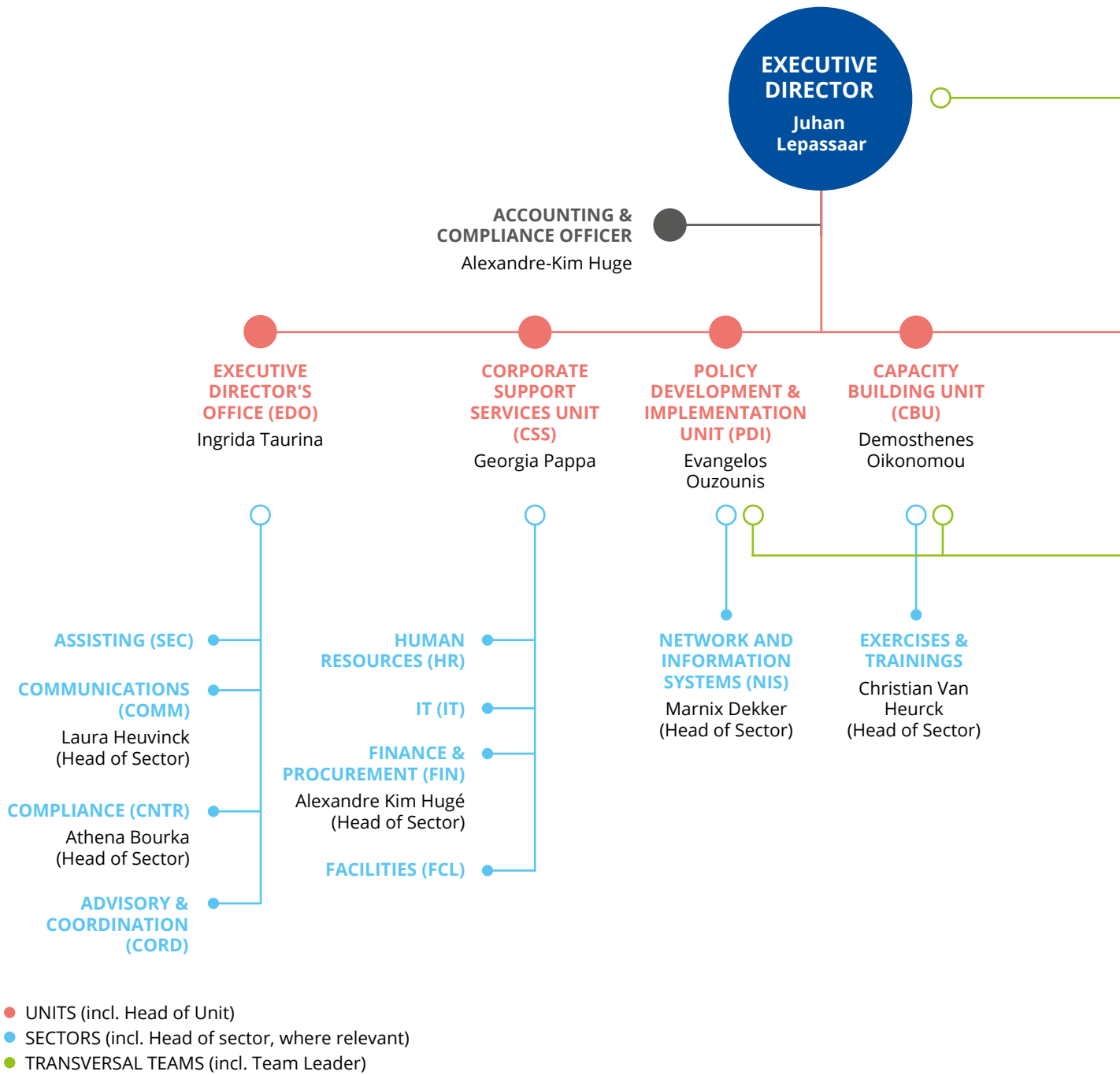
Type of revenue	Entitlements established	Revenue received	Outstanding at the end of the year
Subsidy from the EU budget	22 833 060	22 833 060	-
Subsidy from Greek authorities	219 110	219 110	-
Revenue from administrative operations	14 742	6 041	8 701
Total	23 066 912	23 058 211	8 701

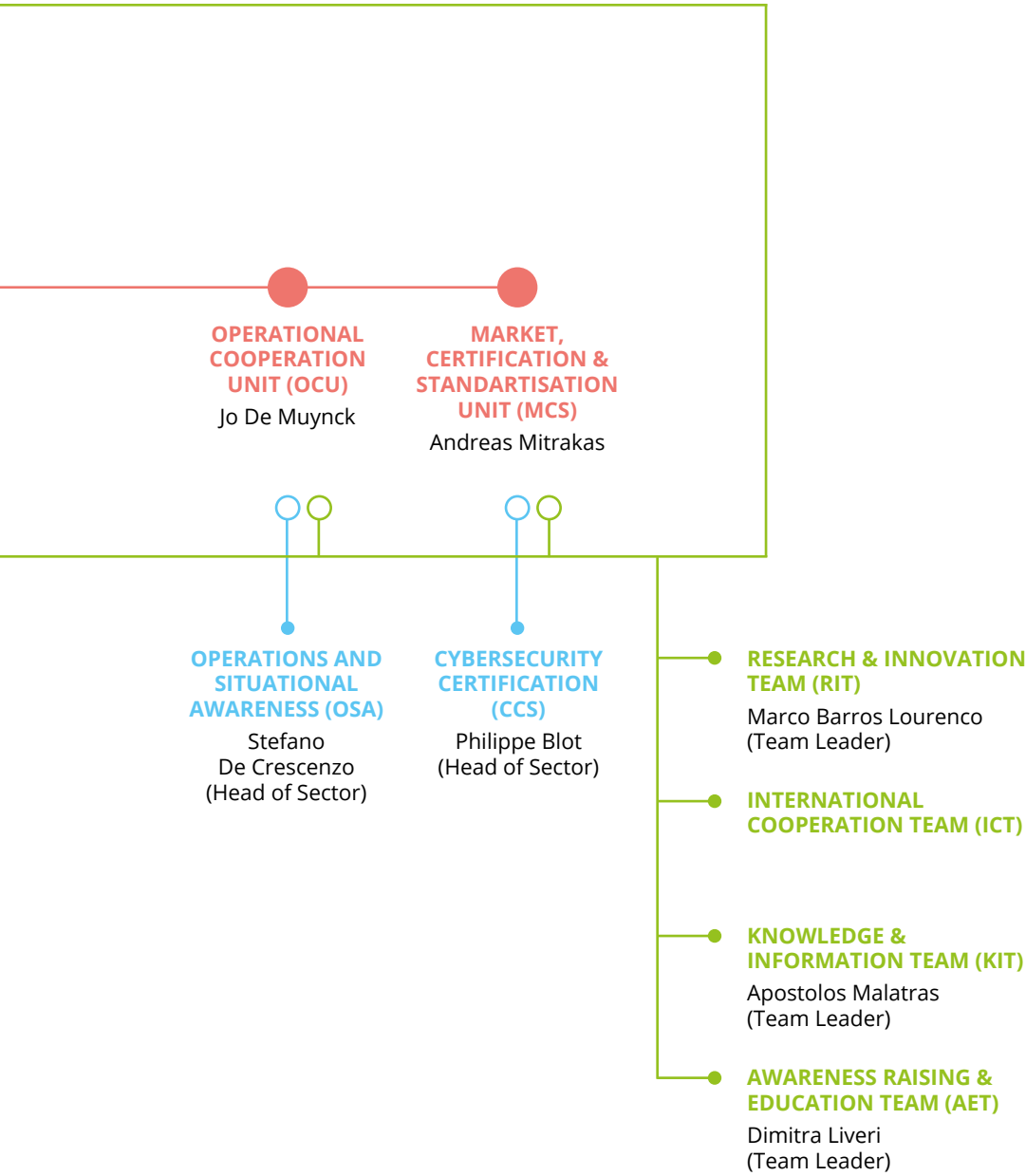
Total revenue may differ from commitment appropriations authorised, as total revenue is based on actual income whereas commitment appropriations may use estimates for other, minor administrative revenue.



ANNEX 3

ORGANISATIONAL CHART





ANNEX 4

2021 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT

2021 establishment plan

Functional group (administrator (AD) / assistant (AST) / assistant-secretary (AST/SC) and grade	Establishment plan in 2021 voted EU budget		Positions filled as of 31.12.2021 ^a	
	Officials	Temporary agents	Officials	Temporary agents
AD 16				
AD 15		1		
AD 14				1
AD 13		1		1
AD 12		5		5
AD 11		2		
AD 10		3		3
AD 9		12		9
AD 8		21		9
AD 7		8		12
AD 6		4		12
AD 5				
Total number of ADs		57		52
AST 11				
AST 10				
AST 9				
AST 8		1		1
AST 7		4		3
AST 6		8		2
AST 5		5		4
AST 4		1		4
AST 3				2
AST 2				1
AST 1				
Total number of ASTs		19		17
AST/SC 6				
AST/SC 5				
AST/SC 4				

Functional group (administrator (AD) / assistant (AST) / assistant-secretary (AST/SC) and grade	Establishment plan in 2021 voted EU budget		Positions filled as of 31.12.2021 ^a	
	Officials	Temporary agents	Officials	Temporary agents
AST/SC 3				
AST/SC 2				
AST/SC 1				
Total number of AST/SCs				
TOTAL		76		69

- a In addition, 1 AST offer was accepted in December 2021 and planned to start May 2022. This figure is not included in the breakdown of posts filled by 31 December 2021.

Information on entry level for each type of post¹⁰

Job title	Type of contract (official, temporary agent, contract agent or seconded national expert)	Function group (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	Operation
Spokesperson	Temporary agent	AD 6	Administrative
Legal adviser	Temporary agent	AD 7	Administrative
Data Protection Officer	Temporary agent	AD 7	Administrative
Information Security Officer	Temporary agent	AD 7	Administrative
Administrator	Temporary agent	AD 8	Administrative
Accounting	Temporary agent	AD 8	Administrative
Seconded national expert	Seconded national expert	N/A	Operations

N/A, not applicable.

¹⁰ The 2021 benchmarking exercise is based on entry grade per job title without taking into consideration the function. The Agency intends to align this as of 2022 onwards.

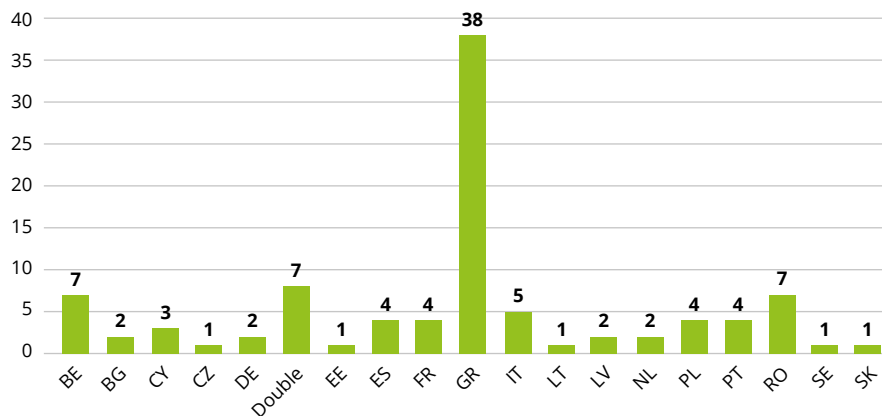
Information on benchmarking exercise

Job type	2021	2020	2019
Total administrative support and coordination	20.34	17.12	18.37
Administrative support	16.95	14.41	15.31
Coordination	3.39	2.70	3.06
Total operational	64.41	72.97	70.41
Total operational coordination	5.93	4.50	5.10
General operational	58.47	68.47	65.31
Total neutral	15.25	9.91	11.22
Finance and control	15.25	9.91	11.22

Human resources statistics

On 31 December 2021, the agency had a total of 96 statutory staff members in house.

Nationality

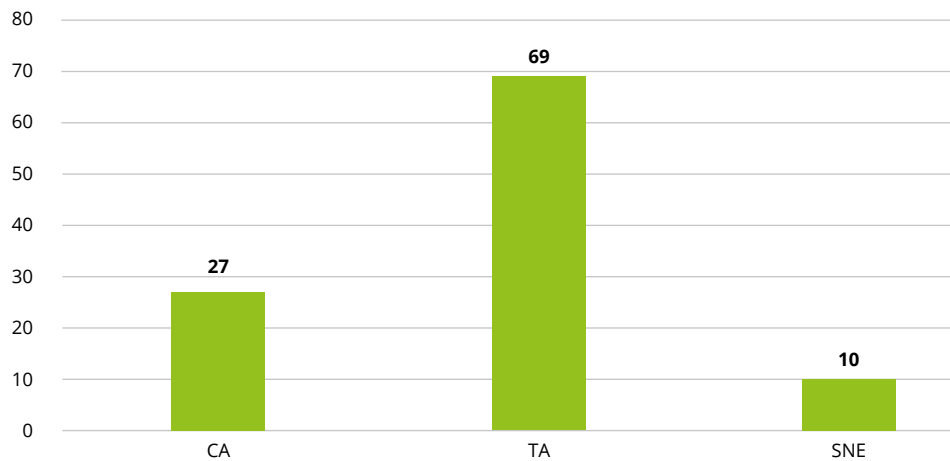


Looking back at 2020 and 2021 and the positive measures undertaken to improve the diversity of nationalities, the Agency can mention its broad outreach campaign on popular media across the EU, closer consideration of the nationality spread in relation to competencies requested and specific provisions on the vacancy notices.

Gender distribution – all departments



Number of employees by contract type



Managers by gender	2016		2021	
	Number	%	Number	%
Female	0	0	5	30
Male	10	100	12	70

The managers are the Executive Director (1), heads of units (6), team leaders (3) and heads of sectors (7).

Implementing rules

MB/2020/10 on procedure for dealing with professional incompetence

MB/2020/13 on laying down general provisions on the conduct of administrative inquiries and disciplinary proceedings

Appraisal and reclassification/promotions

Implementing rules in place

Topic	Number	Yes	No	If no, what 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)	Actual average over 5 years	Recommended average over 5 years according to Decision C(2015)9563
AD05	—	—	—	—	—	2.8
AD06	1	2	3	1	3.7	2.8
AD07	—	—	—	—	—	2.8
AD08	—	1	1	1	4.3	3
AD09	—	—	1	—	—	4
AD10	—	—	—	—	—	4
AD11	1	—	—	—	—	4
AD12	—	—	—	—	—	6.7
AD13	—	—	—	1	10	6.7
AST1	—	—	—	—	—	3
AST2	—	—	—	—	—	3
AST3	1	1	1	—	—	3
AST4	1	1	1	—	—	3
AST5	—	1	—	1	5.5	4
AST6	—	—	—	1	3.5	4
AST7	—	—	—	1	5	4
AST8	—	—	—	—	—	4
AST9	—	—	—	—	—	N/A
AST10 (senior assistant)	—	—	—	—	—	5

N/A, not applicable

Reclassification of contract agents

Function group	Grade	Staff members reclassified in 2021 (ref. year 2020)	Average number of years in grade of reclassified staff members	Recommended average number of years in grade of reclassified staff members according to Decision C(2015)9561
IV	17	—	—	Between 6 and 10
	16	—	—	Between 5 and 7
	15	—	—	Between 4 and 6
	14	5	3	Between 3 and 5
	13	—	—	Between 3 and 5
III	11	—	—	Between 6 and 10
	10	1	3	Between 5 and 7
	9	—	—	Between 4 and 6
	8	—	—	Between 3 and 5
II	6	—	—	Between 6 and 10
	5	—	—	Between 5 and 7
	4	—	—	Between 3 and 5
I	3	—	—	N/A
	2	—	—	Between 6 and 10
	1	—	—	Between 3 and 5

N/A, not applicable

Schooling

Agreement in place with the European School 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	For the 2021–2022 school year, a new decision of the Executive Director was put in place (EDD 2021/41) on financial support for the staff of ENISA in relation to the cost of schooling, which abolished the SLA system

ANNEX 5

HUMAN AND FINANCIAL RESOURCES BY ACTIVITY

Human resources by activity

The allocation of financial and human resources for 2021 for the operational and corporate activities described in Part I of this CAAR is presented in the table below. The allocation was determined according to the direct budget and number of FTEs reported for each activity, with the indirect budget being assigned based on drivers such as direct FTEs.

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

- The direct budget is the actual cost of each of the nine operational activities described in Part I of this CAAR in terms of services, goods, and missions.
- The indirect budget is the actual cost of salaries and allowances, buildings, IT, equipment and miscellaneous operating costs attributable to each activity. The indirect budget was allocated to activities based on drivers. The main driver for cost allocation was the number of direct FTEs used for each operational activity in 2021.
- 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 to all of the Agency's operational activities.
- For the purpose of the allocation of human and financial resources, a Corporate Support Service activity (Activity 11 as described in Part I), including HR, IT services, procurement and finance, facilities and logistics, was allocated to all of the Agency's operational activities.

Allocation of human and financial resources	Activities as referred to in Part 1	Budget allocation (EUR)	FTE allocation
Providing assistance on policy development	Activity 1	1 393 794.52	7.25
Supporting implementation of Union policy and law	Activity 2	3 395 688.26	16.62
Building capacity	Activity 3	3 907 076.25	16.93
Enabling operational cooperation	Activity 4	2 753 446.25	10.97
Contribute to cooperative response at Union and Member States level	Activity 5	2 044 536.29	6.40
Development and maintenance of EU cybersecurity certification framework	Activity 6	2 147 521.14	11.00
Supporting European cybersecurity market and industry	Activity 7	2 027 048.34	10.64
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	2 881 670.90	12.05
Outreach and education	Activity 9	2 170 368.01	8.35
TOTAL		22 721 149.95	100.20

ANNEX 6

GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENT

ENISA does not receive any form of grant.

In accordance with the provisions of the Seat agreement (Greek law 4627/2019) concluded with the Greek authorities, ENISA received a contribution of EUR 219 110 to cover the 2021 leasing expenditure on its offices.

Active service-level agreements in 2021:

- with Cedefop for the purposes of increasing cooperation and sharing services between the two agencies;
- with the Body of European Regulators for Electronic Communications for the provision of electronic data backup services;
- with the European Food Safety Authority for a shared support office under the EU Agencies Network;
- with the European Union Intellectual Property Office for disaster recovery services.

ANNEX 7

ENVIRONMENTAL MANAGEMENT

The normal activities of the Agency were materially affected by the fallout related to COVID-19 for the majority of 2021. ENISA continued to implement, to the greatest extent allowed by its infrastructure and location, its established greening measures such as recycling of office materials, reduction in electricity usage for lighting and heating/cooling, the use of videoconferencing equipment instead of face-to-face meetings involving travel, the use of teleworking, provision of bicycle racks to promote bicycling, the use of public transport and implementing green public procurement.

Owing to restrictions imposed for the best part of 2021, such as 50 % teleworking for staff and restricted travel for work, there were many areas in which significant benefits were realised with regard to adopting a more environmentally friendly workplace. With the majority of staff teleworking 50 % from home, the carbon footprint of each staff member was significantly reduced; they eschewed EU-wide business travel in favour of video conferencing meetings instead; printing at the office was substantially reduced.

The Greek authorities concluded a lease agreement on behalf of ENISA for its headquarters building in Athens, which was fully operational as of 1 July 2021. The building and office space are rented by the Greek authorities for ENISA's use. No longer occupying a shared building will enable a wider set of green measures to be implemented, as all electrical systems such as heating/cooling/lighting will be directly controlled by the Agency, therefore enabling it to directly monitor those systems and assess the impact of any greening measures implemented. During the set-up of the new office, the path to carbon neutrality was already visible. The Agency renovated the office space to better align with operational needs and incorporate considerations of more efficient energy savings and responsible energy consumption.

The European Commission has determined that all sectors of the economy, including all EU institutions and bodies, must contribute to making Europe become the first climate neutral continent by 2050. With this goal, ENISA embraced the EU's climate targets to ensure the climate neutrality of its operations by 2030.

ENISA will thus finally be able to commence assessment and initial planning for implementation of the eco-management and audit scheme certification (EMAS) for its new main office building.

2022 will be a milestone for the agency on the path to carbon neutrality as it engages in the eco-management and audit scheme for the first time, and expects to take action such as sourcing renewable energy and offsetting emissions from work-related travel by staff members and visitors to ENISA premises.

ANNEX 8

ANNUAL ACCOUNTS

Statement of financial position (EUR)

Assets and liabilities	Financial position on 31. 12. 2021	Financial position on 31. 12. 2020
I. Non-current assets	1 994 449	2 124 212
Intangible fixed assets	0	25 094
Tangible fixed assets	1 994 449	2 082 618
Guarantee for leased building	0	16.500
II. Current assets	5 772 118	7 256 337
Short-term receivables	378 897	347 054
Cash and cash equivalents	5 393 221	6 909 283
TOTAL ASSETS (I. + II.)	7 766 567	9 380 549
III. Non-current liabilities	0	0
Long-term provision for risk and charges	0	0
IV. Current liabilities	1 418 889	2 067 160
European Commission pre-financing received	320 867	739 560
Accounts payable	67 797	70 605
Accrued liabilities	1 030 225	1 256 995
TOTAL LIABILITIES (III. + IV.)	1 418 889	2 067 160
V. Net assets	6 347 678	7 313 389
Accumulated result	7 313 389	4 437 322
Surplus/(deficit) for the year	- 965 711	2 876 067
TOTAL LIABILITIES AND NET ASSETS (III. + IV. + V.)	7 766 567	9 380 549

Statement of financial performance (EUR)

Revenue and expenses	2021 financial performance	2020 financial performance
Revenue from the Union subsidy	22 512 193	20 409 560
Revenue from administrative operations	228 252	553 302
Total operating revenue	22 740 445	20 962 862
Administrative expenses	- 14 821 111	- 13 511 894
<i>Staff expenses</i>	- 10 252 970	- 7 796 310
<i>Fixed asset-related expenses</i>	- 836 573	- 347 811
<i>Other administrative expenses</i>	- 3 731 568	- 5 367 773
Operational expenses	- 8 883 259	- 4 573 301
Total operating expenses	- 23 704 370	- 18 085 195
Surplus/(deficit) from operating activities	- 963 925	2 877 667
Financial expenses	- 1 358	- 309
Exchange rate loss	- 428	- 1 291
Surplus/(deficit) from non-operating activities	- 1 786	- 1 600
Surplus/(deficit) from ordinary activities	- 965 711	2 876 067
Surplus/(deficit) for the year	- 965 711	2 876 067

ANNEX 9

LIST OF ABBREVIATIONS

ABAC	Accrual Based Accounting
ACER	European Union Agency for the Cooperation of Energy Regulators
AD	administrator
AHWG	ad hoc working group
AI	artificial intelligence
ARES	Advanced Records System
ARET	Awareness Raising and Education Team
AST	assistant
AST/SC	assistant-secretary
Blue OLEx	Blueprint Operational Level Exercise
BMC	Budget Management Committee
CDR	career development report
Cedefop	European Centre for the Development of Vocational Training
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardisation
CERT-EU	Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSA	Cybersecurity Act
CSIRT	computer security incident response team
CSPO	Cybersecurity Policy Observatory
CVD	coordinated vulnerability disclosure
CyberHEAD	Cybersecurity Higher Education Database
CyCLONe	Cyber Crisis Liaison Network
DG Connect	Directorate-General for Communications Networks, Content and Technology
DNS	domain name system
DSP	digital service provider
EC3	European Cybercrime Centre
ECA	European Court of Auditors
ECASEC	European Competent Authorities for Security of Electronic Communications
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECSC	European Cyber Security Challenge
ECSM	European Cybersecurity Month
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EECC	European Electronic Communications Code
EFTA	European Free Trade Association



eIDAS	electronic identification, authentication and trust services
ENISA	European Union Agency for Cybersecurity
ERA	European Union Agency for Railways
ETSI	European Telecommunications Standards Institute
EU	European Union
EUCC	European common criteria
EUCS	European cloud services
EUIBAs	European Union institutions, bodies and agencies
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
HR	human resources
IAS	internal audit service
ICC	International Cybersecurity Challenge
ICT	information and communications technology
IoT	internet of things
IPR	intellectual property rights
ISAC	information-sharing and analysis centre
ISO	International Organization for Standardization
IT	information technology
ITMC	Information Technology Management Committee
JCU	Joint Cyber Unit
KPI	key performance indicator
LE	law enforcement
MeliCERTes	Name of a project funded by the EU to connect CSIRTs around the Member States
MoU	memorandum of understanding
NCSS	national cybersecurity strategy
NIS	network and information security
NIS CG	Network and Information Security Cooperation Group
NISD	network and information security directive
NISD2	revised network and information security directive
NLO	national liaison officer
OES	operator of essential services
O-RAN	open radio access network
OSINT	open-source intelligence
PQC	post-quantum cryptography
SCCG	Stakeholder Cybersecurity Certification Group
SLA	service level agreement
SMEs	small and medium-sized enterprises
SOP	standard operating procedure
SPD	single programming document
VAT	value added tax



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

enisa.europa.eu



Publications Office
of the European Union

ISBN 978-92-9204-577-7