EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONSOLIDATED ANNUAL ACTIVITY REPORT




2020

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 2020. The report is based on the 2020 amended work programme as approved by the Management Board of ENISA in **Decision No MB/2020/7.** The *ENISA Programming Document 2020–2022* 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

Print	ISBN 978-92-9204-503-6	ISSN 1830-981X	doi:10.2824/643018	TPAB-21-001-EN-C
PDF	ISBN 978-92-9204-502-9	ISSN 2314-9434	doi:10.2824/2917	TPAB-21-001-EN-N

CONSOLIDATED ANNUAL ACTIVITY REPORT 2020

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

FOREWORD

2020 will be a year to remember.

The digital transformation we saw emerging in 2020 as a result of the COVID-19 pandemic was both unexpected and unprecedented. The measures to contain the epidemic imposed on the world new ways to operate and tested our efficiency and flexibility. As the dependence on digital services started to rise rapidly, cyber threats and attacks increased proportionally in the EU and in the rest of the world, and demonstrated the need for more cybersecurity. ENISA remained at the forefront of this battle to give the support needed to the European Union, to the Member States and the EU citizens in these exceptional circumstances to prevent and mitigate threats and ensure business continuity in all spheres of our society.

I am very proud to report the success of the Agency in responding to these challenges. We managed to sail the storm, and made the most of our work programme to ensure the best possible outcomes.

In relation to Covid-19, the Agency was called upon to help coordinate the activities of the EU Member States and bodies at the very start of the pandemic. ENISA therefore issued recommendations to the critical infrastructure industry, and supported the EU tracing apps toolbox. The Agency also provided advice to SMEs and guidance to the healthcare sector to enable them to respond to the increase of phishing campaigns and ransomware attacks. Such preventive actions, although in relation to the pandemic, still fall into the mandate of the Agency to raise the cybersecurity resilience of the EU.

It is important to underline the significant progress made in 2020 by the Agency in developing the new areas foreseen by the Cybersecurity Act, especially in relation to the implementation of the Cybersecurity Certification Framework. This progress included the development of a methodology to enable the implementation of key requirements of the CSA, the candidate European Common Criteria Scheme (EUCC) on ICT products and the candidate European Cloud services scheme (EUCS).

We also supported the EU in relation to the cybersecurity challenges of the 5G networks, and updated the technical guidelines on security measures under the EECC and the 5G threat landscape. ENISA also contributed to the development of the 5G toolbox in cooperation with the Commission services.

This proactive stance of ENISA is part of the new strategy established in the course of the year and adopted by the management board in June 2020. This document sets the foundation of our strategic objectives and priorities and serves the purpose the purpose of mapping out the annual work programme, fulfilling the Agency's permanent mandate and moving towards « A trusted and cybersecure Europe ».

The Management Board of ENISA also approved the amendment of the 2020 work programme made necessary by the pandemic. The objective of this amendment was to allow us to resort to the online environment for those activities delivered in presence before the emergence of COVID-19. In parallel, an amending budget was adopted in August to re-direct funding to new projects as a replacement of activities which could not take place because of the pandemic.

With the new strategy designed to integrate the provisions of the Cybersecurity Act, came the need to change the organisational structure of the Agency. To achieve this ambitious goal, the Agency mapped its human competences, changed or created new internal processes and formed new teams to trigger better internal dynamics. The reorganisation was approved by the Management Board in June 2020 and was implemented as of 1st January 2021.

To strengthen the existing human resources and increase the capacity of the Agency to meet the requirements of its extended mandate, a large-scale recruitment exercise was also launched in 2020. The widespread promotional campaign enhanced the visibility of the vacancies resulting in the submission of more than 1200 applications coming from all Member States. Thanks to this initiative the Agency was able to use a pool of 84 shortlisted candidates to fill the open positions it had in 2020. The purpose of this pool was also to facilitate the recruitment process for openings in the operational units in 2021 and 2022.

Highlights of ENISA's work in the area of expertise included the 4th annual IoT security conference on operational IoT, Artificial Intelligence (AI) and Supply Chain for IoT. Our experts developed security recommendations addressed to the professionals of the Connected and Automated Mobility sector.

Artificial Intelligence was also under scrutiny and resulted in the AI threat landscape published in December 2020. ENISA started to cooperate with the new working group on AI as soon as it was established in May.

As for cybersecurity exercises, due to the « force majeure » of the situation, it was generally agreed to postpone the European Cybersecurity Challenge to 2021 and to also postpone the pan-European cyber exercise, Cyber Europe 2020.

I am proud to report that the Capture-the-Flag (CTF) event « ENISA Hackfest 2020 » went ahead in a virtual setting and successfully attracted 250 participants from 17 EU and EFTA Member States. In addition, I am glad to report the likewise successful digital edition of the 2020 European Cybersecurity Month campaign demonstrated by a three-fold increase in outreach.

Other works of particular interest included the development of a cyber-threat assessment methodology and impact assessment model designed to help the EU assess the overall impact of cyberattacks. The work allows ENISA to support the cooperation among EU institutions on cyber crises management.

ENISA has taken on board the new Security Union Strategy released in July 2020 and included these parameters to address digital risks.

I am glad to see that ENISA has successfully endeavoured to raise the resilience of the EU critical infrastructures and to strengthen the EU's capabilities while maintaining the synergies needed for an effective operational cooperation.

This of course could not have been achieved without the unrelenting support and commitment of all our stakeholders and I seize this opportunity to thank each one of them warmly and express how grateful I remain to our communities, to the European institutions and bodies and to all the Member States.

I understand the anxiety and pressure we all experienced in these difficult times. This is why I would like to also express my sincere gratitude to the Agency's staff for displaying such resilience and commitment to ENISA. Only such collective efforts can lead to the success of our endeavours.

Juhan Lepassaar
Executive Director, ENISA

ENISA MANAGEMENT BOARD ASSESSMENT

The analyses and assessment by the Management Board of ENISA of the consolidated annual activity report for the year 2020 of the authorising officer of ENISA

The Management Board takes note of the Consolidated Annual Activity Report (CAAR) for the financial year 2020, 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 CAAR 2020 produced by the Executive Director of ENISA in his quality of Authorising Officer for the implementation of the annual budget on 1st June 2021 and the Management Board received a copy of the 2020 AAR on the same date.

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

- The challenging circumstances which emerged as a result of the COVID 19 pandemic led to the adoption of a number of amendments to the work programme 2020 and associated budget. The amendments allowed the Agency to adjust its meetings to the online environment. They also made it possible to postpone some of its deliverables requiring physical presence.
- Despite these challenges, the Agency was able to meet the objectives set in the work programme 2020 as shown by the results presented in this report.
- The CAAR presents key results of the implementation of the ENISA work programme 2020 thus demonstrating how the Agency successfully completed all deliverables as agreed with the Management Board in the amended work programme 2020.
- The new strategy of ENISA was adopted by the Management Board in June 2020. The programming of the Agency's work will be based on the strategic objectives and priorities defined in this new strategy. The activities of the Agency will be planned accordingly using a multi-annual framework covering the years to come.
- Furthermore, the Agency embarked on the reorganization of its internal structures, adopted by the MB in June 2020. The new organisational structure aligns the tasks and functions of the Agency's structural set-up with the Cybersecurity Act.
- ENISA produced 45 reports and engaged in various activities according to the provisions of its mandate in the Cybersecurity Act and pertaining to the current cybersecurity environment. These reports provided assistance to many sectors listed in the NIS Directive, but also in evolving areas such

as Artificial Intelligence. Impact indicators show that the Agency's results exceeded the targets established in the work programme 2020, against the framework of the ENISA Strategy 2016-2020.

- In 2020 the Agency began to fulfill its role in the area of Cybersecurity certification framework, in particular for candidate schemes on common criteria and cloud services. This work will be continued in 2021, by preparing candidate schemes for other areas in response to the requests received from the Commission services.

- Overall, the AAR is in line with the ENISA work programme 2020 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 2020 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 2020, the Agency operated with a budget of EUR 21.6 million equivalent to a 28 % increase compared to the 2019 budget (EUR 16.9 million). The amending budget was adopted by the Management Board by written procedure on 28 August 2020. The purpose of this amending budget was to re-direct funding made available through the cancellation of projects and forecasted expenditures due to the COVID-19 pandemic to finance new projects and activities up to an amount of EUR 2.5 million, from which EUR 1.6 million were under operational activities.

- During 2020, ENISA committed a total amount of EUR 20 588 320 representing 97.35 % of the total budget for the year. Payments made during the year amounted to EUR 14 513 329 representing 68.62 % of the total budget. The budgetary execution was high despite of the restrictive circumstances imposed by COVID-19.

- As compared to 2019, there has been a slight increase in commitment execution – 97.35 % in 2020 as compared to 96.80 % in 2019, and a slight decrease in payment execution – 68.62 % as compared to 70.12 % in 2019. The target of 95 % for commitment rate set by the Commission (DG Budget) was reached.

- In 2020, the Executive Director reviewed the delegation of authorising authority powers and on 12 February 2020 adopted a new decision on a framework of the financial delegation of the authorising officer and of a budgetary management committee to ensure a sound financial executive of the Agency's budget.

- The AAR also provides a follow up of the 2019 Discharge and control results. This section also notes the main categories of deviation that led to exceptions reported. In 2020 the agency recorded 31 exceptions: 28 of these were below the relevant materiality level (less than EUR 15 000) and of a minor administrative nature with no financial impact.

- In 2020, ENISA undertook an ex post evaluation of 2019 activities within the ENISA work programme from Deloitte Consulting and Advisory. This work resulted in a final report and a case study on Procurement Guidelines for Cybersecurity in Hospitals. Recommendations included to revise key performance indicators (KPIs), balancing and tailoring the Agency's activities and outputs, and finally to reinforce the position of the Agency within the cybersecurity ecosystem.

- The turnover of staff was greatly reduced in 2020. The ratio was only of 2 percent 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. It is worth noting that vacant posts for seconded national experts were fulfilled as well.

- ENISA adopted the revised internal control framework at the end of 2019. The AAR 2020 shows the adequate management of risks, a high level of transparency, well managed data protection rules and business continuity activities.

- The Management Board notes that infringement of the use of delegation powers and weaknesses in internal controls framework were identified by the European Court of Auditors. The Board concludes that necessary actions were undertaken 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 2020. The Management Board notes with satisfaction that ENISA could deliver the work programme 2020 despite the unforeseen 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.

The Management Board notes the reservations made by the Executive Director which do not affect the validity nor the accuracy of the annual accounts for the financial year 2020 to the discharge authority.

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: 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. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cyber policies.

The aim of the Agency is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. ENISA aspires to be an agile, environmentally and socially responsible organisation focused on people.

In a world that has become hyper-connected, cybercriminals pose a significant threat to the internal security of the European Union and security of its citizens online. The COVID-19 pandemic has highlighted the need for more security in the digital world. People have increased their presence online to maintain personal and professional relations, while cybercriminals have taken advantage of this situation, targeting in particular e-commerce and e-payment businesses, as well as the healthcare system. At the same time, the Agency also needed to deal with the challenges of the pandemic and remote working.

THE YEAR IN BRIEF

In June 2019 the new Cybersecurity Act (CSA) came into force giving ENISA a new and permanent mandate. The tasks assigned to ENISA under this regulation are meant to help achieve achieve a high common level of cybersecurity across the Union, including actively supporting Member States, Union institutions, bodies, offices, and agencies in improving cybersecurity.

Such were the circumstances presiding over the implementation of the ENISA Programming Document 2020- 2022, the first programming year falling under the full scope of the new mandate.

The strengthened and expanded tasks of the Agency in the field of operational cooperation were tested in 2020 because of the need to ensure adequate cybersecurity throughout the corona virus (COVID-19) crisis. The Agency faced multiple challenges as a consequence. Acting in the context of Article 7 of the CSA, ENISA engaged in a number of activities[1] that played an important role in helping EU Member States

1 Including initiating contacts with the European Commission, the European Union Agency for Law Enforcement Cooperation's (Europol) European Cybercrime Centre (EC3) and the Computer Emergency Response Team for the EU (CERT-EU) to establish an information exchange network, which subsequently attracted the participation of the European External Action Service (EEAS) and the Council of the European Union; contributing to the technical annex of the Commission's recommendation on contact tracing apps.

and bodies coordinate their activities throughout the initial phases of the pandemic and in raising the resilience of the EU. These practical steps and actions are not expected to be one-off endeavours, but will continue to be pursued through the evolving Blueprint and future operational cooperation activities.

KEY ACHIEVEMENTS OF THE YEAR

The Agency took a very proactive stance in the CSA and made significant progress in developing the new areas of work foreseen by the act. In this respect, ENISA laid the groundwork to fully implement the Cybersecurity Certification Framework. In parallel, the Agency supported the European Union to respond to cybersecurity challenges connected to 5G. Additionally, ENISA engaged additional efforts to integrate the concepts of the 'blueprint' into the cyber-crisis management approach by unveiling an innovative tool for knowledge management in this area.

In addition 2020 marked the establishing of the In addition, 2020 marked the establishiment of the new strategy of ENISA, adopted by the management board in June 2020 and used as a baseline to set the strategic objectives and priorities for programming the Agency's work using a multiannual framework, for the years to come. The new strategy outlines the Agency's strengthened path in view of achieving a high common level of cybersecurity across the Union. The strategy was developed to fulfil the Agency's permanent mandate and takes on the vision of 'A Trusted and Cyber Secure Europe' and enhanced mission: *'to achieve a high common level of cybersecurity across the Union in cooperation with the wider community."*

In parallel, the Agency was the object of a reorganisation engaged in order to align its structure and organisational capabilities with the needs of the CSA. The Management Board agreed with the principles guiding the reorganisation in February 2020. The new organisational structure was adopted in June 2020 and was implemented on 1 January 2021.

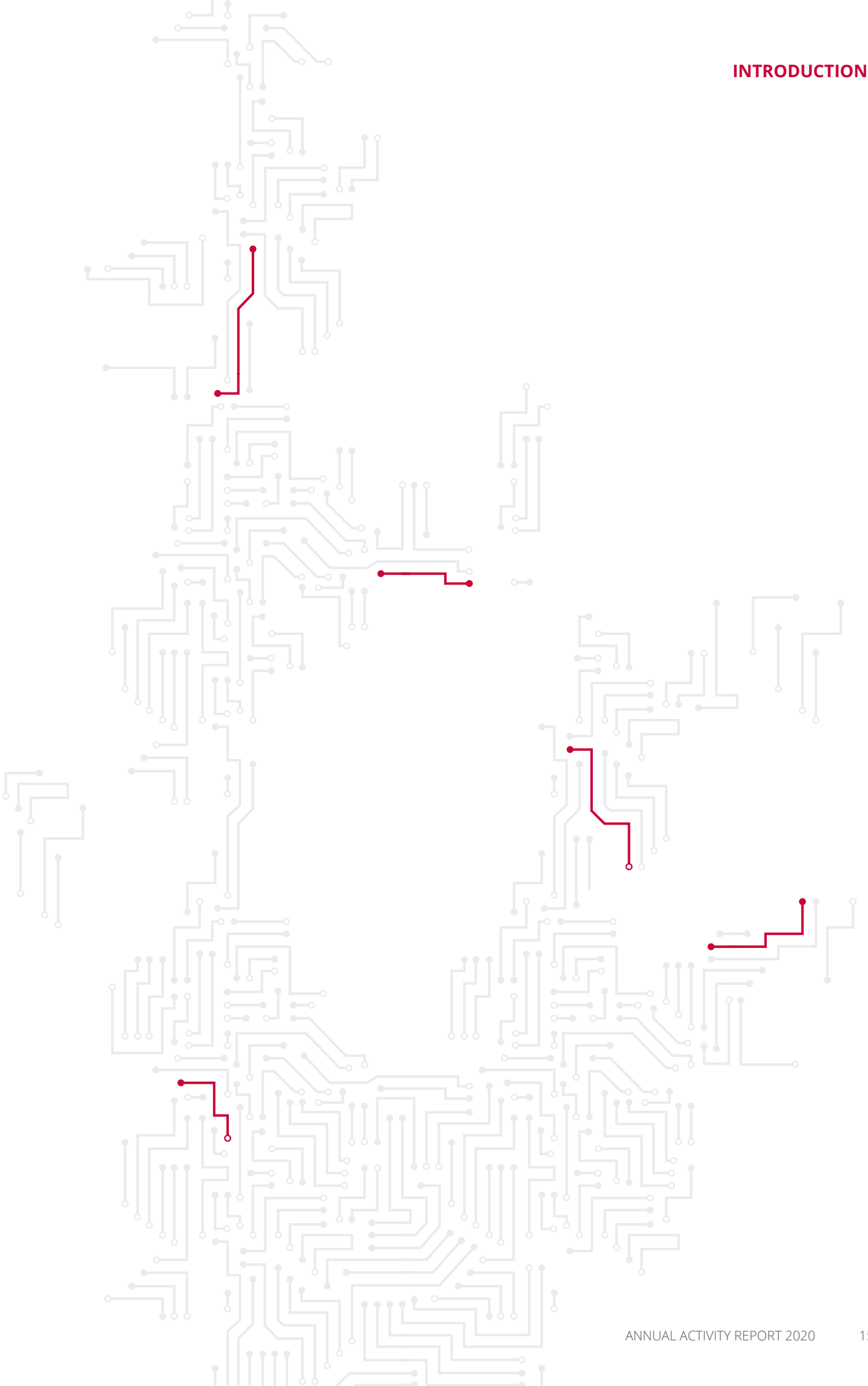
The CSA provides for a framework for European cybersecurity certification schemes with a view to creating a digital single market for ICT products, services and processes. The Agency began to fully execute this function in 2020, in particular for candidate schemes for common criteria and cloud services. In 2021, the Agency will initiate the work meant to raise the competitiveness of the European cybersecurity market and industry. This work includes advising and assisting EU bodies (including the Cybersecurity Competence Centre and Network[2] in setting cybersecurity research and innovation priorities, as well as by providing regular insights into how both the supply side and the demand side of the market function. Such activities will remain in the years to come and are expected to grow.

The Agency continued to support EU decision-making institutions in relation to the EU Cybersecurity Strategy and the announced review of the security of networks and information systems (NIS) directive. This renewal and strengthening of a key pillar of the EU's regulatory framework. It underpins the cybersecurity of critical sectors across our society. It could also further make use of the expanded and permanent mandate given to the Agency and is expected to influence the development of the ENISA work programme in the years to come as a result.

Finally, ENISA negotiated a lease agreement for a new building in Athens and startedpreparations to move into the new premises during the summer of 2021.

While being in full telework regime since March 2020 in response to restrictions due to the pandemic, the Agency remained operational and implemented its work programme, recruitment, procurement, and managed to ensure staff wellbeing. Following the duty of care principle, the Agency allowed staff to carry out their duties remotely, and from outside their place of assignment as appropriate, with regular information being provided to the Executive Board and the Management Board.

2 In September 2018, the European Commission proposed a regulation setting up a European Cybersecurity Competence Centre and Network. The (draft) regulation ensures cooperation and complementarity with ENISA. In particular, ENISA will have an important role in contributing to the Centre's strategic role in coordinating cybersecurity technology-related investments by the EU, Member States and industry. The Council agreed its negotiating position in June 2020 and the trilogies with the European Parliament began in summer 2020.



PART I
ACHIEVEMENTS OF THE YEAR

The following sections of the Annual Activity Report are based on the structure of the ENISA Programming Document 2020-2022[3] with specific amendments on work programme 2020, PART III. After the description of the specific results for each activity and output, the achievements against indicators and the detailed results for each output are presented in tables, followed by the list of publications together with relevant links.

1 ACTIVITY 1: EXPERTISE

Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges

1.1 Key results in implementing Activity 1: EXPERTISE

1.1.1 Objective 1: Improving knowledge on the security of digital developments

O.1.1.1. Building knowledge on the security of Internet of Things (IoT)

Main achievements:

- Study on securing IoT
- Annual IoT Security Conference

ENISA delivered guidelines for securing IoT based on the study addressing challenges related to the security of the supply chain for IoT. It analysed the different stages of the IoT supply chain and explored all the important security considerations to be taken into account in each stage. The guidelines issued included input and validation from IoTSec EG[4], EICS EG[5], NLOs[6] and other industry stakeholders.

The 4th annual IoT Security Conference series raised awareness on the security challenges facing the Internet of Things (IoT) ecosystem across the European Union. The series spanned three weeks, with each week exploring a different cybersecurity topic: Operational IoT, Artificial Intelligence (AI) and Supply Chain for IoT, respectively.

In 2020, bilateral discussions took place with relevant stakeholders on IoT security. ENISA also engaged in the topic during related events.

3 https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2020-2022-with-amendments

4 ENISA Internet of Things (IoT) Security (IoTSEC) Experts Group

5 ENISA Industry 4.0 Cyber Security (EICS) Experts Group

6 National Liaison Officers Network (https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office)

O.1.1.2. Building knowledge on Connected and Automated Mobility (CAM)

Main achievements:

- Reports on the security of CAM and on CAM ecosystem

The ENISA Deliverable: *'Recommendations for the security of CAM'* is a report providing a high-level overview of the cybersecurity challenges in the CAM sector. It defines both the concerned CAM actors and introduces associated recommendations. The report benefited from the input and validation from CAMSEC EG[7], and other industry stakeholders.

Additionally, ENISA produced another report providing a comprehensive understanding of the CAM cybersecurity ecosystem. In particular, it includes the mapping of the key stakeholders and relevant bodies and organisations in the European Union, and provides an overview of the critical services and systems and infrastructures.

O.1.1.3. Building knowledge on Artificial Intelligence security

Main achievements:

- Report on AI Cybersecurity Challenges and Threat Landscape
- AI security webinar co-hosted with MEP Kaili
- Report 'Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving' in collaboration with Commission services (DG JRC)

ENISA published the deliverable 'AI: Cybersecurity Challenges – AI Threat Landscape' in December 2020. This was a seminal piece of work mapping the AI Threat Landscape. This report presents the Agency's active mapping of the AI cybersecurity ecosystem and its Threat Landscape, realised with the support of the Ad-Hoc Working Group on Artificial Intelligence Cybersecurity. The ENISA AI Threat Landscape not only laid the foundation for upcoming cybersecurity policy initiatives and technical guidelines, but also stressed relevant challenges.

In October 2020, ENISA hosted an AI security webinar together with MEP Kaili to explore the cybersecurity challenges of AI. Speakers and panellists discussed the current risks and offered ways forward in view of establishing a secure ecosystem for AI across the Union. The event – attended by more than 550 stakeholders – highlighted the role of cybersecurity in establishing the reliable and trustworthy deployment of AI – a principal area of work by the EU Agency for Cybersecurity.

In May 2020, ENISA formed an ad hoc Working Group (AI WG) composed of 15 members and 6 observers (EU institutions) in order to best satisfy the objectives of this Output. Together with the Working Group, ENISA mapped the threat landscape concerning AI, provided support to the Commission services on relevant policy initiatives, and held events to raise awareness on AI cybersecurity. The ENISA ad hoc Working Group on AI held 5 plenary sessions throughout the year, as well as a validation plenary session to discuss and validate the results presented in the study.

Together with the Commission services (DG JRC), ENISA worked on a report titled 'Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving'. The report was published in February 2021 and looks at cybersecurity risks connected to Artificial Intelligence (AI) in autonomous vehicles and provides recommendations for mitigating them.

O.1.1.4. Building knowledge on the security of healthcare services

Main achievements:

- Report on 'Cloud security for Healthcare services'
- Tool development for procurement in hospitals
- Online sessions of the annual eHealth Security Conference
- Toolkit development in collaboration with Commission services (DG CNECT and DG Health and Food Safety)

ENISA published the report 'Cloud security for Healthcare services'. This report identified the cybersecurity and data protection challenges that healthcare organisations faced when trying to move services to the cloud and detailed the key aspects that should be considered when conducting the relevant risk assessment. The report focused on three relevant case studies and detailed a set of 17 security measures to support healthcare organisations in addressing the relevant challenges. It was validated by the eHealth Security Experts Group and additional stakeholders from the healthcare sector.

ENISA also developed an online tool for procurement in hospitals. Based on the procurement guidelines deliverable published by ENISA in February 2020, the tool provides a simple way for hospitals to identify good practices of relevance to them based on context

7 ENISA Connected and Automated Mobility Security (CAMSec) Informal Expert Group

(e.g. type of procurement, cybersecurity threats/ challenges etc.).

Furthermore, ENISA organised three online sessions of the annual eHealth Security Conference. The Danish Health Data Authority, co-organiser of this year's conference, together with ENISA redesigned the eHealth Security Conference this year to focus on three areas of healthcare's most pressing cyber challenges with in-depth online sessions taking place over a period of three months.

By working closely with Commission services (DG CNECT and DG Health and Food Safety) ENISA supported the COVID-19 tracing and monitoring mobile apps Toolkit development.

Finally, ENISA also supported the creation of the NIS Cooperation Group Work stream for Healthcare.

O.1.1.5. Building knowledge on maritime security

Main achievements:

- 'Cyber risk management for ports' report
- Support to SafeSeaNet project
- Contribution to the development of a Transport Cybersecurity Toolkit for Commission services (DG Mobility and Transport)

ENISA published the deliverable: *'Cyber risk management for ports'*. This report intends to provide port operators with guidelines and good practices to tackle the oft-cited issue of cyber risk management. Port operators are meant to find in the report the support they need in adopting the risk assessment methodology of their choice. The maritime work stream of the TRANSSEC Experts Group, Commission services (DG Mobility and Transport) and additional stakeholders from the maritime sector all validated the report.

Moreover, ENISA provided support to EMSA as an opinion for the security requirements of the SafeSeaNet project.

ENISA contributed to the development of the "Transport Cybersecurity Toolkit" for the Commission services (DG Mobility and Transport) and provided input on the sectorial specificities in maritime. ENISA supported the creation of a Cyber Work Group in the European Coastguard Function Forum (ECGFF) and took part in the activities of the work group as member.

ENISA contributed also to the ongoing project of CESNI/TI on Cybersecurity for Inland Ports as a member of the informal Advisory Board.

O.1.1.6. Building knowledge on cryptographic algorithms

Main achievements:

- Set of the Ad hoc stakeholders group on cryptographic algorithms
- Research on 'Post-Quantum Cryptography: Current state and quantum mitigation'
- Study on 'Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies'

The Agency set up an ad hoc stakeholders group on cryptographic algorithms, comprised of EU institutions. The group met only once physically in 2020 because of the Covid crisis. Further interactions (i.e. review of outputs, requests for support, feedback) happened in an asynchronous mode.

Research on Post-Quantum or Quantum-safe Cryptography were conducted with top experts in the field. ENISA presented the outputs in a publication, *'Post-Quantum Cryptography: Current state and quantum mitigation'* study. The study provides a concise overview of the current progress of the standardisation process of post-quantum cryptography (PQC) schemes. It introduces a framework to analyse existing quantum-safe solutions, classifying them into families and discussing their advantages and shortcomings. With contributions from top experts in the field, it helps readers navigate an overly complex but also fascinating topic for the future of cybersecurity. The study aims to help decision-makers and system designers to take up actions as soon as possible. It includes useful quantum resistant techniques that can be implemented in today's systems until PQC algorithms become standardised and generally available. NLO & the stakeholders' group reviewed the output and issued no negative comments. As an exceptional summary of the current PQC landscape, this deliverable is regarded as a useful mapping of the current situation. This is substantiated by the high-level information included on the ideas behind the algorithms and on the mitigation instructions for the transition period to actual standardised PQC algorithms.

ENISA performed an extensive research in cryptographic building blocks of crypto-assets. The outputs were presented in thepublication: *'Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies'* (DLTs). The study aimed to further increase the understanding of theunderlying cryptographic components. Such components are the ones forming the blockchain. and by extension are also part of crypto-assets, digital currencies and of a host of other possible applications. As a continuation of an earlier report on the security and

challenges of DLTs, this report provides an in-depth explanation of the technical components involved and illustrated their uses in popular deployed instances. By focusing on crypto-assets, it intends to support policymakers by explaining the underling cryptographic mechanics used and thus raised awareness on foreseen security, financial, legal and data protection issues.

1.1.2 Objective 2: Cybersecurity threat landscape and analysis – outputs

O.1.2.1. Annual ENISA threat landscape report

Main achievements:

- 22 reports on new visual and digital e-book format of Threat Landscape

This year's ENISA Threat Landscape Report summarises top cyber threats assessed for the period covering 2019 to April 2020. Divided into 22 different reports, ENISA released it in an e-Book form. The provided material presents the assessed changes of the threat landscape from the 2018 report, further to the transformation of the digital environment triggered by the COVID-19 pandemic. Moreover, it provides information on various aspects of cyberthreats, major incidents, advancements in Cyberthreat Intelligence, sectoral threat analysis, research issues and threat trends.

ENISA introduced a new visual and a digital e-book format., The new threat landscape includes seven strategic reports, along with 15 in-depth reports on the top cyber threats:

- **The Year in Review** report provided a general overview of the threat landscape, including the most important topics, and the top 15 threats, conclusions and recommendations.
- **Cyberthreat Intelligence Overview** summarised the most important topics relevant to the cyberthreat intelligence (CTI) community.
- **Sectoral and Thematic Threat Analysis** reviewed the threat landscape for specific sectors and technologies, including specifically ENISA's work on 5G, the Internet of Things (IoT) and smart cars.
- **Major Incidents in the EU and Worldwide** provided an overview of major cybersecurity incidents happening in the EU and worldwide, and highlighted the lessons we can learn from them.
- **Research Topics** presented key aspects related to the research and innovation in cybersecurity focused in the Cyberthreat Intelligence domain.
- **Emerging Trends** focused on the challenges and opportunities for the future in the cybersecurity domain.

A List of the top 15 Threats was followed by a series of reports describing each of the top 15 threats. The threat reports, of technical nature, include findings, major incidents, and statistics.

Last but not least, ENISA organised the annual event on Cyberthreat Intelligence EU (CTI EU), which took place in Brussels in January 2020.

O.1.2.2. Restricted and public info notes on cybersecurity

Main achievements:

For the year 2020, this deliverable was reprioritised to support the collaboration with CERT EU. The work was partially covered through Output 0.1.2.1.

O.1.2.3. Support for incident-reporting activities in the EU

Main achievements:

- Brussels' one-day workshop of telecom security authorities group
- Report on good practices in telecom sector: 'Telecom Security during a Pandemic'
- Annual incident report of EU's trust services sector

ENISA supported the Member States with implementing EU Incident Reporting, by working with the following working groups.

The European Competent Authorities for Secure Electronic Communications (ECASEC) is the group of telecom security authorities from 32 countries, formerly known as the Article 13a group. ENISA provided the secretariat and organised one physical workshops and 2 online ones.

- The first ECASEC group of the year was combined with an open day for industry, gathering 160 telecom security experts in Brussels for a one-day workshop on a wide range of topics related to telecom security (including talks on quantum crypto, zero trust networks, emergency communications, and the impact of solar flares on telecom equipment).

- ENISA also published a short paper on '*Telecom Security during a Pandemic*' giving an overview of the initiatives and good practices of the telecom sector to mitigate the impact of the pandemic. The report highlights the resilience of telecom networks and services during the pandemic, which sustained major fluctuations in usage and traffic, but also points to the need for increased cooperation between the public and private sector.

The ENISA Article 19 expert group is the group of supervisory bodies for eIDAS trust services. ENISA organised one online and one physical workshop and published the annual incident report aggregating incidents from 27 EU countries and 2 EFTA countries. This report was the fourth annual report for the EU's trust services sector. The group also delivered a position paper with input for the upcoming eIDAS review, including several suggestions for improvements regarding the supervision of security requirements in Article 19 of the eIDAS.

For the NIS Cooperation group Work Stream 3, on NIS Directive incident reporting, ENISA compiled 2 reports, published in 2020[8]. These papers focused on synergies in incident reporting and on the first NISD annual report. ENISA adapted its CIRAS reporting tool for the NISD reporing. It is important to note that, the group decided to use this NISD reporting tool in the future. Such successful outcome shows the efficiency of the work ENISA performed in the area in 2020 it will speed up and improve incident reporting and analysis going forward.

O.1.2.4. Supporting PSIRTs and NIS sectoral incident response expertise

Main achievements:

This activity was postponed because of the pandemic. Initiated in November 2020, the work will resume in 2021.

1.1.3 Objective 3: Research, development and innovation – outputs

O.1.3.1. Supporting EU research and development programmes

Main achievements:

- Research Roadmap for supporting the EU strategic digital autonomy
- Development of cybersecurity higher education Database

Research Roadmap for supporting the EU strategic digital autonomy: The mission-driven roadmap presented seven prioritised challenges in order to support research, development and innovation for the EU strategic digital autonomy. Based on our findings, strategic digital autonomy would require an overarching vision of the ICT landscape, driven by ambitious policies that aim (i) to protect European values and (ii) to satisfy European needs for advanced and resilient services.

ENISA published a short paper on 'Telecom Security during a Pandemic' giving an overview of initiatives and good practices in the telecom sector to mitigate the impact of the COVID-19 pandemic.

A virtual workshop was organised with the Commission services (DG CNET) in order to create inter-pilots cooperation. ENISA acted as a trusted independent partner by facilitating the process. In the meeting, the pilots of the European Competence Network (Concordia, CyberSec4Europe, Echo and Sparta) briefed the stakeholders on the cross-pilot activities and synergies – in the context of cybersecurity education and skills – with the goal of promoting further collaboration opportunities across the pilots and other stakeholders. Two focus groups – one on the cyber education database and the other on the skills framework – were created and ENISA's role was to act as enabler and facilitator.

ENISA added the cybersecurity higher education Database (CyberHEAD) it developed in its website to support more people opting forcybersecurity degrees. This crowd-sourced database – populated by academic institutions – lists more than 120 cybersecurity degrees in the EU and in EFTA countries and became the main point of reference for all citizens who intend to upskill their knowledge in the cybersecurity field through academic programmes.

8 NIS Cooperation Group | Shaping Europe's digital future (europa.eu)

1.2 Outputs and performance indicators for Activity 1: EXPERTISE

Summary of outputs from Activity 1: EXPERTISE – Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges		
Outputs	**Performance indicator**	**Results achieved**
Objective 1.1. Improving knowledge on the security of digital developments		
Output O.1.1.1. Building knowledge on the security of Internet of Things	Engagement of 10 IoT stakeholders from 5 EU Member States in the preparation of the study (P).	29 IoT stakeholders from seven (7) EU Member States, US and Israel were involved in the preparation of the study. 15 out of the 29 IoT stakeholders had been interviewed and 20 IoT stakeholders participated in the validation workshop.
Output O.1.1.2. Building knowledge on Connected Automated Mobility (CAM)	Engagement of 10 CAM stakeholders from 5 EU Member States in the preparation of the study (P).	42 stakeholders from six (6) EU Members States. 18 interviews were conducted with the stakeholders. Validation workshop held on 15 October 2020 with 15 stakeholders.
Output O.1.1.3. Building knowledge on Artificial Intelligence security	Engagement of 10 stakeholders in the preparation of the publication (P) and of at least 20 stakeholders participating in the workshop (E).	22 AI stakeholders were engaged in the preparation of the publication (15 members and 7 observers of the ENISA ad hoc Working Group on AI). 527 registered participants to the Cybersecurity for Artificial Intelligence online workshop (on 30 September 2020).
Output O.1.1.4. Building knowledge on the security of healthcare services	Engagement of healthcare stakeholders from at least 12 EU Member States in this activity, i.e. the publication (P) and/or workshop (E) and/or support (S).	Advice provided for two CSIRTs on how to evaluate and enhance team's maturity. Together with CSIRTs Network Maturity Working group prepared guidelines for remote maturity peer review process for CSIRTs network members.
Output O.1.1.5. Building knowledge on maritime security	Engagement of 10 maritime sector stakeholders from 5 EU Member States in the preparation of the study (P).	18 maritime sector stakeholders from 11 EU Member States were interviewed in preparation of the study. An additional 49 maritime stakeholders from 16 EU Member States participated in the online survey.
Output O.1.1.6. Building knowledge on cryptographic algorithms	Publication of 2 news items or dissemination materials covering public documents and activities of the groups/ meetings attended.	One news item covering two public studies: Crypto Assets: Introduction to Digital Currencies and Distributed Ledger Technologies Post-Quantum Cryptography: Current state and quantum mitigation Publications reviewed by NLO with no negative comments. As an exceptional summary of the current PQC landscape, this deliverable is regarded as a useful mapping of the current situation. This is substantiated by the high-level information included on the ideas behind the algorithms and on the mitigation instructions for the transition period to actual standardised PQC algorithms.
Objective 1.2. Cybersecurity Threat Landscape and Analysis		
Output O.1.2.1. Annual ENISA Threat Landscape report	Engagement of more than 10 Member States in discussions related to the structure and content of the ENISA Threat Landscape report. More than 5 000 downloads of the ENISA Threat Landscape report. Engagement of more than 80 CTI experts from industry, academia and Member States.	More than 20 experts from EU Member States engaged in discussions about the structure and content of the ENISA Threat Landscape 2020. This was achieved by contributions of the ENISA Cyber threat Intelligence Group (ca. 13 experts from 8 EU Member States) and contributions to the content by means of reviews from experts of the ENISA Advisory Group and NLOs (8 experts communicating their comments). During the first two months of publication, ENISA registered over 25 000 downloads of reports from the ENISA website and 300 000 reactions in social media. In 2020, CTI EU event was attended by ca. 180 from EU and 11 international vendors who had showed presence in the exhibition space.

Summary of outputs from Activity 1: EXPERTISE – Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges		
Outputs	**Performance indicator**	**Results achieved**
Output O.1.2.2. Restricted and public Info notes on cybersecurity	Coverage of all major incidents relevant to EU NIS policy priorities. Expanding of coverage to all key ENISA's key stakeholder groups.	No results to be disclosed regarding ENISA public info notes in 2020, due to reprioritization of the ENISA work.
Output O.1.2.3. Support incident reporting activities in the EU	Contribution of more than 20 national regulatory authorities / EU Member States to the preparation of the report (Article 13a) (P). Contribution of more than 10 EU Member States to the preparation of the report (Article 19) (P). Engagement of more than 10 Member States in discussions and work related to implementing particularities of the NISD incident-reporting framework (S).	For the telecom security incidents, 25 EU Member States, as well as two (2) EEA/EFTA countries), participated in the annual summary reporting and the final annual report was approved by the entire Article 13a expert group before it was published by ENISA. For the trust services security incidents, 26 EU Member States, as well as one EFTA country, participated in the annual summary reporting and the final report was approved by the entire Article 19 expert group, before it was published by ENISA. The work stream 3 of the NIS Cooperation group, with 26 EU Member States, contributed to a report on synergies in incident reporting, and, for the first time, an annual report covering NISD incidents. The synergies paper as well as the annual report were approved by 26 EU Member States in the work stream and were ultimately published on the NIS Cooperation group portal.
Output O.1.2.4. Supporting PSIRTs and NIS sectoral incident response expertise	Engagement of sectoral CSIRTs and PSIRTs in Member States.	In 2020 a desk research was conducted on the subject matter and its result was handed over to ENISA. Based on the findings, a survey was drafted and sent to the different organisations having role as a PSIRT or CSIRT
Objective 1.3. Research & Development, Innovation		
Output O.1.3.1. Supporting EU research and development programmes	No papers to be produced.	ENISA issued the Research Roadmap for supporting the EU strategic digital autonomy. The validation included comments from 25 experts. A virtual workshop (by invitation only) organized with the Commission services (DG CNECT) had an active participation of 30 research and innovation organisations involved in education on the pilots of the European Cybersecurity Competence Centre and Network (CCCN).

1.3 Publications and Deliverables[9] for Activity 1: EXPERTISE

List of deliverables for Activity 1: EXPERTISE – Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges
Objective 1.1. Improving knowledge on the security of digital developments
Output O.1.1.1. Building knowledge on the security of Internet of Things Guidelines for securing IoT Status: Published
Output O.1.1.2. Building knowledge on Connected and Automated Mobility (CAM) Cybersecurity Stocktaking in the CAM Status: Published Recommendations for the security of CAM Status: Published
Output O.1.1.3. Building knowledge on Artificial Intelligence security Artificial Intelligence Cybersecurity Challenges Status: Published
Output O.1.1.4. Building knowledge on the security of healthcare services Cloud Security for Healthcare Services Status: Published (January 2021)
Output O.1.1.5. Building knowledge on maritime security Guidelines – Cyber Risk Management for Ports Status: Published
Output O.1.1.6. Building knowledge on cryptographic algorithms Crypto Assets, Digital Currencies and Distributed Status: Published Good Practices in Cryptography Status: Published – Restricted Study on Post-Quantum Cryptography state of the art Status: Published
Objective 1.2. Cybersecurity Threat Landscape and Analysis
Output O.1.2.1. Annual ENISA Threat Landscape report Annual ENISA Threat Landscape 2020 report Status: Published
Output O.1.2.3. Support incident reporting activities in the EU Annual Report NIS Directive Incidents 2019 Status: Published Technical topic article 13a Telecoms during a pandemic Status: Published Annual Incident Analysis Report for the Trust Service Providers Status: Published Annual Incident Analysis Report for the Telecom Sector Status: Published
Output O.1.2.4. Supporting PSIRTs and NIS sectoral incident response expertise PSIRTs and NIS sectorial incident response policy and expertise Status: Delayed
Objective 1.3. Research & Development, Innovation
Output O.1.3.1. Supporting EU research & development programmes

9 https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

2 ACTIVITY 2: POLICY

Promote NIS as an EU policy priority

2.1 Key results in implementing Activity 2: POLICY

2.1.1 Objective 1: Supporting EU policy development – outputs

O.2.1.1. Supporting policy developments in NIS Directive sectors

Main achievements:

- Energy Sector: Mapping exercise of ES-C2M2 to controls of ISO/IEC 27001:2013 and position paper to Commission services in development of network codes on cybersecurity for electricity
- Railway Sector: Report on 'Railway Cybersecurity: Security measures in the Railway Transport Sector' and online webinar co-organised with European Agency for Railways
- Finance Sector: Position paper to the consultation by European Commission

Energy sector

In 2020 ENISA's activities concerning energy sector cybersecurity revolved around two main areas:

1. Maturity Framework for the energy sector and mapping of ES-C2M2 to controls of ISO/IEC 27001:2013. In order to address these two issues,

   ENISA compiled a study by:

   - Conducting a stock taking exercise with 35 stakeholders from the sector during a workshop. Key findings and recommendations in order to establish an EU maturity framework are provided in the final report.
   - Mapping the widely used US ES-C2M2 to well-known standards (including ISO 27001). This outcome is planned to be further consulted and be published as a joint product with key energy stakeholders such as ENTSO-E, ACER and E.DSO.

2. Electricity network code on cybersecurity: According to Article 59(3) of the Electricity Regulation (EU) 2019/943 the Commission has to establish a priority list (every three years in electricity) identifying the areas to be included in the development of network codes for electricity. Cybersecurity has been identified as one of the key areas in which network codes and guidelines could be developed. ENISA contributed to this consultation by providing a position paper which identifies key challenges and provides recommendations in six main areas: governance, security measures, supply chain security, coordination and crisis management, early warning capability and situational awareness as well as cross border risks and dependencies.

Railway sector

ENISA issued the report on *'Railway Cybersecurity: Security measures in the Railway Transport Sector'*. This ENISA study assesses the level of implementation of cybersecurity measures in the railway sector, within the context of the enforcement of the NIS Directive in each European Member State. It presents a thorough list of essential railway services accompanied by a high-level overview of the railway systems they support. Finally, the European Railway Traffic Management System was presented together with some key cybersecurity considerations and recommendations.

In November 2020, ENISA and the European Agency for Railways jointly organised an online webinar on rail cybersecurity. The webinar showcased the agencies' joint activities on rail cybersecurity and stressed the importance of cybersecurity to railway stakeholders.

Finance sector

In the finance sector, ENISA developed an EU map of European cybersecurity policy initiatives in the finance sector. It was a first depiction of the complex landscape of initiatives related to cybersecurity at an EU level. The document was created in an effort to shed light to the initiatives and to guide interested parties in engaging with them and benefit from their produced results. Furthermore, it aimed to make the cooperation between the initiatives and their different groups work more seamless.

Additionally, ENISA contributed to a consultation by the European Commission on the digital resilience Act (DORA) by providing a position paper to the consultation. The paper identified key challenges and provided recommendations in three main areas: risk management and resilience, information sharing and cooperation, and on interaction with the NIS directive.

2.1.2 Objective 2: Supporting EU policy implementation – outputs

O.2.2.1. Recommendations supporting implementation of the eIDAS Regulation

Main achievements:

- Six reports on the implementation of Electronic Identification and Trust Services
- Annual Trust Services Forum co-organised with Commission services

In 2020 the Agency completed a package of six reports to boost the implementation of the eIDAS regulation and to promote the uptake of Electronic Identification and Trust Services.

ENISA published a set of four reports to provide technical guidance and security recommendations for the implementation of trust services. These reports provide a conformity assessment framework for Qualified Trust Service Providers (QTSPs), security recommendations for QTSPs based on standards, a security framework for trust service providers and also a security framework for QTSPs in order to achieve compliance with Article 19 of the eIDAS Regulation.

ENISA also published a report on the analysis of methods used to carry out remote identity proofing. The report provides an overview of the most common methods for identity proofing. ENISA illustrated this using examples received from the different stakeholders. The report also includes a presentation of the supporting standards at the international and EU level and provided the current status quo in the EU Member States in relation to their identity proofing laws, regulations and practices. Besides, the report also includes a preliminary gap analysis on existing standards and regulations followed by legal and technical recommendations.

In implementing the Cybersecurity Act, ENISA supported the eID efforts of the Member States and the Commission services in 2020 by working towards the formulation of an eID maturity model (MM), focusing on the security of eID schemes, in the form of a questionnaire. It was envisaged that the model would allow stakeholders to indicatively measure the maturity level of security of eID schemes on multiple topics, as well as the maturity of Member States in this area. Besides, ENISA organised the 6th annual Trust Services Forum in collaboration with the Commission services. The forum served as a platform for stakeholders to share their good practices on the implementation of trust services, stood as an opportunity to review the standards, implementing acts and technical guidelines within the eIDAS. It also allowed to to discuss strategies to promote the adoption of qualified trust services. The event attracted more than 500 participants and brought together trust service providers, conformity assessment bodies, supervisory bodies and experts to discuss the practical and emerging issues under the eIDAS Regulation across Europe.

O.2.2.2. Supporting the implementation of the work programme of the Cooperation Group under the NIS Directive

Main achievements:

- Support to Commission services (DG CNECT) with the review of the NISD
- Gap analysis report on the existing national security measures
- Knowledge building session on auditing frameworks for the energy sector national competent authorities
- Study on good security practices for Digital Infrastructures
- Technical deep dive report on 'Security of Country Code Domains in Europe'
- Participation to the activities of the group of national health competent authorities
- Report on NIS investments

In 2020, ENISA supported Commission services (DG CNECT) with the review of the NISD via:

- Internal interviews, a survey for the CSIRT network and drafting of an ENISA position paper which was submitted to COM as input to the consultation process.
- Input to the consultations through e.g. interviews, organising meetings with experts from COM, or active participation to workshops and conferences.
- Telecommunication security review after an extraordinary request by COM.

ENISA also provided support to the Member States and the COM by taking stock of the existing national security measures and drafting a gap analysis report. The purpose of this activity was to analyse the different national approaches to the security measures adopted by the Cooperation Group, identify gaps as well as common good practices.

This year ENISA launched a series of knowledge building sessions with the purpose of increasing the awareness as well as the knowledge of the energy sector competent authorities concerning energy and industrial control systems cybersecurity.

Furthermore, ENISA supported the NIS Cooperation group WS10, authorities for Digital infrastructure, with a wide-ranging security analysis of the Digital Infrastructure sector, assessing criticality, threats and good practices. This security analysis was used by the Commission services as input for the NIS2 proposal, which proposes to extend the scope of this sector. The security analysis also helps the authorities with developing guidelines, by providing the high priorities, and giving an overview of industry good practices.

ENISA supported the creation of the NIS Cooperation Group Work Stream for Healthcare as well. This group includes the participation of members of the eHealth Network (national competent authorities for eHealth).The Agency contributed to the discussions for determining the priorities and initial deliverables of the work stream (security measures, incident reporting).

Lastly, ENISA published a report on NIS investments Lastly, ENISA published a report on NIS investments in order to document how Operators of Essential Services (OES)/Digital Service Providers (DSPs) invest in cybersecurity. The report also provides insights on how the NIS Directive influenced this investment, and provides useful data for policymakers to reflect upon and identify future policy initiatives. This report aims to serve as a reference point offering policymakers at an EU and National level sufficient data to better understand the investments across the sectors in scope of the NIS Directive as well as the relevant impact of the NIS Directive and its implementation.

O.2.2.3. Contribute to the EU policy in privacy and data protection with technical input on cybersecurity related measures

Main achievements:

- Report on pseudonymisation techniques and advanced use cases
- ENISA co-organised online the 8th edition of the Annual Privacy Forum

In 2020, the Agency published a report on pseudonymisation techniques and advanced uses cases. The report aims to support data controllers and processors in implementing pseudonymisation by providing possible techniques and use cases that could fit different scenarios. It was a continuation of the work conducted in the area since 2018 and provided an analysis of state-of-the-art solutions in the field of data pseudonymisation, as new research and business models broke new ground.. ENISA also published a report on the analysis of methods used to carry out remote identity proofing. The report provides an overview of the most common methods for identity proofing. ENISA illustrated this using examples received from the different stakeholders. The report also includes a presentation of the supporting standards at the international and EU level and provided the current status quo in the EU Member States in relation to their identity proofing laws, regulations and practices.

Furthermore, ENISA organised the 8th edition of the Annual Privacy Forum (APF), in order to bring together research and policy practitioners in the cutting edge of privacy, data protection and information security. The event was co-organised with the Commission services (DG CNECT), Catolica University of Lisbon with the support of the European Data Protection Supervisor (EDPS) and the Portuguese Data Protection Authority. The two-day event took place online and welcomed renowned policymakers and speakers fromindustry, research and academia. The event attracted over 650 participants. Dedicated panel sessions covered the work of the Agency in the area of pseudonymisation as well as challenges in the area of tracking. The proceedings were published with Springer Lecture Notes in Computer Science (LNCS)[10].

O.2.2.4. Guidelines for the European standardisation in ICT security

Main achievements:

- ENISA co-organised the Annual Standardisation Conference 2020 and prepared the conference edition of 2021

ENISA co-organised the Annual Cybersecurity Standardisation Conference 2020, together with its partners – the European Standards Organisations – the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). The conference aimed to foster the dialogue among policymakers, industry, research, standardisation organisations, certification organisations and those involved in the development of the ICT certification framework in Europe, in view of an effective implementation of the Cybersecurity Act.

ENISA also prepared in 2020 the 2021 edition of the Conference (online event).

10 http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0

O.2.2.5. Supporting the implementation of the European Electronic Communications Code

Main achievements:

- Security analysis of the Over-The-Top services
- Development of new reporting guidelines for the European Electronic Communications Code
- Open day event with telecom stakeholders in Brussels

ENISA supported the group of national telecom security authorities, namely the European Competent Authorities for Secure Electronic Communications (ECASEC) with the transposition of the European Electronic Communications Code (EECC). This support translated into the performance of a security analysis of the so-called Over-The-Top (OTT) services. This set of services was new in the scope of the EU telecom security legislation. This work was partly background material (criticality, risks) and partly input for the OTT security profile (measures) which would be developed by the group.

ENISA also developed new reporting guidelines for the EECC. The new reporting thresholds were needed because the EECC extended the scope of reporting to new services and new types of incidents. The EECC reporting guideline, together with the EECC security measures guideline (see O.2.2.5), formed the minimum basis for implementing the security provisions in the EECC. ENISA will continue supporting the group with transposition by analysing specific new EECC topics.

To facilitate the discussions with the industry, ENISA organised an open day event at the start of 2020 inviting telecom providers, suppliers, and also the new OTT providers like Facebook and Microsoft. This (yearly) open day was a success The open day – which takes place yearly - was considered an important action in order to create mutual understanding and enable the exchanging of views between the authorities and the sector. With a total of 160 participants attending in Brussels, the event was therefore considered a success.

O.2.2.6. Support the MS in improving the cybersecurity of 5G networks

Main achievements:

- Update the technical guideline on security measures under the EECC
- Updated version of the 5G Threat Landscape report
- Study on security controls in 3GPP and other 5G specifications
- Knowledge building webinar on 5G security
- Toolbox implementation progress report

In 2020; ENISA continued to provide an active support in the area of cybersecurity of European 5G networks, in particular to assist Member States in implementing provisions from the EU 5G Toolbox on risk mitigation measures. Two key achievements in this domain were the new Guideline on Security Measures under the EECC[11] (with the added 5G supplement[12]), aligned with the Toolbox and with the new European Electronic Communication Code that came into force in December 2020, and a new version of ENISA Threat Landscape for 5G networks[13].

In addition, jointly with the Commission services (DG CNECT) ENISA actively supported the work of the NIS Cooperation Group Works Stream on 5G cybersecurity, and was one of the key contributors in preparation and publication of the 5G Toolbox implementation report[14], published in July 2020.

The Agency had also regular discussions with BEREC on 5G security (also in the context of ECASEC group) and co-organised a major workshop on 5G security with the participation of the private sector.

ENISA supported European Competent Authorities for Secure Electronic Communications (ECASEC), the group of national telecom security authorities with the transposition of the European Electronic Communications Code (EECC).

11 https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

12 https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc

13 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

14 https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

2.2 Outputs and performance indicators[15] for Activity 2: POLICY

Summary of outputs from Activity 2: POLICY – Promote NIS as an EU policy priority		
Outputs	**Performance indicator**	**Results achieved**
Objective 2.1. Supporting EU policy development		
Output O.2.1.1. Supporting policy developments in NIS Directive sectors	Engagement of at least 10 relevant stakeholders (P and S). Participation of at least 20 stakeholders in workshops (E).	In the energy sector, 35 stakeholders (i.e. energy operators, vendors, regulators, energy associations and energy sector consultants) took part in the stock taking activity concerning the electricity maturity frameworks. 28 experts participated and validated the work done in the workshop that ENISA organised. In railway sector, 41 stakeholders from 21 Member States contributed to the survey and validated the published report. The ERA-ENISA Webinar gathered around 350 live participants (575 views). In the finance sector, 15 stakeholders contributed to the survey, as well as in the document's validation.
Objective 2.2. Supporting EU policy Implementation		
Output O.2.2.1. Recommendations supporting implementation of the eIDAS Regulation	Engagement of at least 5 representatives from different bodies / Member States in the validation of the recommendations. Review and acceptance by at least 10 stakeholders (trust service providers, conformity assessment bodies and supervisory authorities) from at least 5 Member States. Participation of more than 50 stakeholders in the activity.	The report concerning guidelines on trust services was scrutinized by a broad range of stakeholders (around 80 in total from across the 27 Member States); Moreover, FESA, Article 19 EG and Commission services (DG CNECT) provided valuable comments. The guidelines on trust services passed through the review of many stakeholders (around 80 from across the 27 Member States); Moreover, FESA, Article 19 EG and Commission services (DG CNECT) provided valuable input. Experts from 10 Member States that participate in the eIDAS Cooperation Network, as well as Commission services, reviewed the maturity model and provided input for its design and validation. The report on identity proofing analysed rich data from elaborated answers though questionnaires from 80 key stakeholders from all 27 Member States including public and private sector. The report was further validated by the Article 19 EG, FESA, Commission services (DG CNECT) and ETSI STF 588. The Trust Services forum was attended by more than 500 participants from relevant stakeholders.
Output O.2.2.2. Supporting the implementation of the work programme of the Cooperation Group under the NIS Directive	Engagement of at least 12 Member States in ENISA's contributions to the implementation of the NIS Directive (S).	Representatives of national as well as sectorial (energy, digital infrastructures and health) competent authorities in NIS CG, from 27 Members States, were actively involved in scoping, review and validation of deliverables.
Output O.2.2.3. Contribute to EU policy in privacy and data protection with technical input on cybersecurity related measures	Participation of at least 5 representatives from different bodies/ Member States in preparing the recommendations. Attendance of more than 60 participants from relevant communities to the APF.	Nine (9) representatives from research, academia and regulatory bodies took part in the drafting and preparing of the recommendations and in the editing of the associated report. The APF was an online two-day event that over 650 participants from relevant stakeholders' communities attended.

15 https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

Summary of outputs from Activity 2: POLICY – Promote NIS as an EU policy priority		
Outputs	**Performance indicator**	**Results achieved**
Output O.2.2.4. Guidelines for the European standardisation in ICT security	Participation of at least 5 representatives of European Standard Developing Organisations (SDOs) and relevant services of the European Commission and/or agencies in drafting and reviewing the guidelines. Participation of more than 60 participants from relevant communities.	Six (6) representatives from European SDOs took part in the drafting of the ENISA strategy paper and approximately 50 standardisation experts and representatives of the Commission and Member States participated in the review process. The standardisation conference attracted 450 registered participants (400 participants were online) and it was co-organized by ENISA, CEN CENELEC and ETSI as a physical event which took place before the outbreak of the pandemic.
Output O.2.2.5. Supporting the implementation of the European Electronic Communications Code (EECC)	Participation of at least 10 Member States and 5 providers in the activities/workshop (P, E) related to the new EECC.	Authorities from 27 EU Member States and several EEA/EFTA countries, together with more than 60 participants from the sector joined the ENISA workshop. This was the last major telecom security event in Europe before the COVID lockdown started.
Output O.2.2.6. Support the Member States in improving the cybersecurity of 5G networks	Engagement of stakeholders from at least 10 Member States in the activity (P).	Stakeholders (i.e. representatives of cybersecurity authorities in NIS Cooperation Group and of telecom security NRAs in Article 13a EG) from 27 Members States, were actively involved in scoping, review and validation of deliverables.

2.3 Publications and deliverables for Activity 2: POLICY

List of deliverables for Activity 2: EXPERTISE – Promote NIS as an EU policy priority
Objective 2.1. Supporting EU policy development
Output O.2.1.1. Supporting policy developments in NIS Directive sectors Railway Cybersecurity – Security measures in the Railway Transport Sector Status: Published EU Cybersecurity Initiatives in the Finance Sector Status: Published (March 2021)
Objective 2.2. Supporting EU policy implementation
Output O.2.2.1. Recommendations for technical implementation of the eIDAS regulation Conformity Assessment of Qualified Trust Service Providers Status: Published Security Framework for Qualified Trust Service Providers Status: Published Security Framework for Trust Service Providers Status: Published Recommendations for Qualified Trust Service Providers based on Standards Status: Published Remote ID Proofing - Analysis of Methods to carry out identity proofing remotely Status: Published A Maturity Model Framework for eID Schemes Status: Published internally to stakeholders only due to confidential data included in the report.
Output O.2.2.2. Supporting the implementation of the work programme of the Cooperation Group under the NIS Directive NIS Investments Report Status: Published
Output O.2.2.3. Contribute to the EU policy in privacy and data protection with technical input on cybersecurity related measures Data Pseudonymisation: Advanced Techniques and Use Cases Status: Published

List of deliverables for Activity 2: EXPERTISE – Promote NIS as an EU policy priority
Output O.2.2.4. Guidelines for the European standardisation in the field of ICT security Taxonomy of Cybersecurity (Approach to ENISA strategy towards standardisation) Status: Delivered (no publication)
Output O.2.2.5. Supporting the implementation of the European Electronic Communications Code Technical Guideline on Incident Reporting under the EECC Status: Published (2021)
Output O.2.2.6. Support the MS in improving the cybersecurity of 5G networks Update of 5G Threat Landscape Status: Published Telecom security guidelines under the EECC Status: Published Security in 5G standards Status: Published (Feb 2021) 5G supplement to telecom security guidelines under EECC Status: Published

3 ACTIVITY 3: CAPACITY

Support Europe in maintaining state-of-the-art NIS capacities

3.1 Key results in implementing Activity 3: CAPACITY

3.1.1 Objective 1: Assisting Member States in capacity building – outputs

O.3.1.1. Technical trainings for Member States and EU bodies

Main achievements:

- Development of two new trainings on ransomware scenario, DoS attack and APT intrusion on a victim network.

ENISA updated the technical training material and developed two new trainings sessions in 2020.

ENISA added two elaborate use cases to the training that was developed the year before(Orchestration of CSIRT Tools). The two use cases are: a ransomware scenario and a Denial of Service (DoS) attack. The focus was on using the set of orchestrated tools for investigation and mitigation of incidents, emphasising aspects of automation and information sharing. The initial modular approached to the 'Orchestration of CSIRT Tools 'allowed to integrate these new use case scenarios with little extra effort.

The other training developed had a very high focus on supporting operational practices. The training was called: 'Defending Against Adversary Actions' and the scenario was an Advanced Persistent Threat (APT) intrusion on a victim network. Both the attacker and victim infrastructure were emulated and the training was developed and delivered in an online virtual lab environment. It aimed more experienced CSIRT members and could be considered as an ENISA flagship technical/operational training. ENISA presented the training in a near final version to the CSIRTs Network (CNW) members, to whom an advanced demo/dry-run and access to all the documentation and manuals were given. The feedback was very positive and some comments were taken into account and integrated in the final version.

O.3.1.2. Support EU Member States in the development and assessment of national cybersecurity strategies

Main achievements:

- A National Capabilities Assessment Framework (NCAF) was produced
- NCSS workshop to validate the results of the NCAF study

ENISA produced a National Capabilities Assessment Framework (NCAF) to measure the level of maturity of MS cybersecurity capabilities. This framework was developed to serve as a self-assessment, it used the national strategy as a starting point and covered 5 maturity levels for 17 strategic objectives that are structured around four main clusters.

The Agency organised the annual National Cyber Security Strategies (NCSS) workshop that took place on the 6th of October to validate the results of the study on the NCAF. In this workshop 60 experts from 26 EU Member States participated and provided feedback.

ENISA started a study to increase the resilience of SMEs against cybersecurity risks and threats in

case of crisis such as COVID19. The results will be published in 2021.

Furthermore, a workshop took place on the 17th of November in collaboration with EASME to present the preliminary results on the study performed on Cybersecurity for SMEs. Participants from 120 private and public sector organisations coming from all EU Member States and several other countries attended the online workshop.

ENISA supported Greece in the evaluation of their NCSS by providing guidance, support and input and by sharing of good practices. This led to the development of the new GR NCSS (2020 – 2025) that was published in December 2020.

O.3.1.3. Support EU Member States in their incident response development

Main achievements:

- Study conducted on 'How to set up CSIRT and SOC'
- Report on Sectoral CSIRT Capabilities – Energy and Air Transport

ENISA conducted a study that was a results-driven guidance for establishing a computer security incident response team (CSIRT) and a security operations centre (SOC). The study includes a guidance on possible improvements for different types of CSIRTs and SOCs currently active.

ENISA also developed and published a report focusingon trends in Energy and Air Transport Incident Response Capabilities, procedures, processes and tools., This report also includes insights on current challenges and gaps facing IR communities.

The CSIRT inventory was updated in June and December 2020. Currently, there are 583 teams in the inventory.

The development of the online tool for ENISA CSIRT maturity assessment started in 2020 and was made available online in 2021[16].

O.3.1.4. ISACs for the NISD sectors in the EU and Member States

Main achievements:

- Toolkit for ISACs
- Supported 5 EU ISACS, Financial ISAC, Rail ISAC, Maritime ISAC, Healthcare ISAC and Energy ISAC

Specification for a toolkit[17] for ISACs – ENISA developed the comprehensive toolkit "ISAC in a BOX", following studies on the ISAC concept, to address the need to facilitate community building and collaboration across ISACs. The toolkit is intended to providepractical guidance and the means to empower industry for the creation of new ISACs and to further develop existing ones.

ENISA supported the Financial ISAC, RAIL ISAC, Maritime IS AC, Healthcare ISAC and the Energy ISAC. In the Finance ISAC, ENISA hosted two meetings virtually. The meetings engaged an average of 25 participants, and included the participation of the European Central Bank (ECB), and Europol. In the Railway ISAC, ENISA hosted two meetings virtually hosted , engaging an average of 50 participants, including the European Railway Agency (ERA). In the Energy ISAC, ENISA supported three meetings with an average of 25 participants. Additionally, ENISA organised three webinars based on the interest of the ISAC members.

In February 2020 the Maritime ISAC was founded. ENISA participated in 4 meetings with an average of 10 participants and contributed to the formalising of the ISAC. Finally, ENISA supported the inception and inaugural discussion of the European Healthcare ISAC.

3.1.2 Objective 2: Support EU institutions in capacity building – outputs

O.3.2.1. Liaison with the EU agencies on operational issues related to CERT-EU's services

Main achievements:

- Workshop between CERT-EU and ENISA

CERT-EU and ENISA organised a workshop in February 2020 which concluded that information sharing between staff of both entities need to be further strengthened. In addition it became clear thatboth entities should cooperate in building synergies on various areas of activities to contribute to cybersecurity incident response or event response in the European Union. ENISA established a task force which mandate is to strengthen the structural cooperation with CERT-EU, in order to benefit from synergies and to avoid the duplication of activities.

16 https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-survey

17 https://www.enisa.europa.eu/news/enisa-news/isac-in-a-box

ENISA attended the CERT-EU Steering Board meetings in 2020. ENISA and CERT-EU signed a Memorandum of Understanding in 2021 on a strategic cooperation model between ENISA and CERT-EU.

O.3.2.2. Cooperation with relevant EU institutions, agencies and other bodies on cybersecurity initiatives

Main achievements:

- ENISA participation in the EU Cyber Forum

At the September 2020 second edition of the EU Cyber Forum, the Executive Director of ENISA participated in the panel 'Digital society after COVID-19: building a global cyber resilience regime'. ENISA also co-organised and moderated the working session 'Cybersecurity certification: EU and global outlook'.

3.1.3 Objective 3: Awaren ess raising– outputs

O.3.3.1. European Cyber Security Challenges

Main achievements:

- Launched the International Cybersecurity Challenge activity
- Planning and execution of 'ENISA Hackfest 2020'

ENISA launched the International Cybersecurity Challenge activity. This decision was based on the success of the European Cybersecurity Challenge, and it involved the help of other regional and international organisations, decided to design and host the International Cyber Security Challenge (ICSC). To that end, a steering committee was formed in 2020. Formed by government, regional institutions, universities and research centres, the steering committee started to design a competition between teams from different regions. Teams from as far as South East Asia, Oceania, US, Latin America and Africa started to express vivid interest in participating. ENISA completed the setting up of the steering committee early in the year.

The Agency planned and executed the 'ENISA Hackfest 2020' on the 16-18th of November. This was a Capture the Flag (CTF) event between cybersecurity professionals and students in order to connect and train the teams taking part in the 2021 European Cyber Security Challenge (ECSC).

O.3.3.2. European Cyber Security Month deployment

Main achievements:

- ESCM went fully digital and online with 6 more Members States participating

In 2020 the ECSM went fully digital and online with no in-person meetings due to the circumstances of the COVID-19 outbreak. Notwithstanding these circumstances, metrics built into the ECSM show a three-fold increase in outreach, from 2.7 million citizens that the campaign had reached in 2019, to 9.8 million in 2020.

The 2020 campaign followed the same format as in 2019. The activities were developed around two themes: digital skills and cyber-scams. The overwhelming majority of partners gave ECSM a rating from good to excellent and believed that the campaign supported, added value and improved their national campaigns and that it promoted sharing ideas between Member States. Another important improvement compared to previous years was the fact that Member States' participation increased by 22 %, with six more Member Sates actively engaging in the campaign compared to 2019. Moreover, the ECSM team received very positive feedback with respect to the provision of promotional and security awareness materials translated in all official EU languages, especially forthose Member States having limited resources for such production.

O.3.3.3. Support EU Member States in cybersecurity skills development

Main achievements:

- Policy recommendations for the implementation of ECSC roadmap

ENISA performed an analysis of the key factors enabling the success of a national cybersecurity competition and gave a snapshot of the current situation in the European Union and European Cyber Security Challenge (ECSC) partner countries. This analysis helped provide policy recommendations for both the short-term and the long-term implementation of this common ECSC roadmap, with the goal to place the ECSC in a primary position to support the objectives of the EU Security Union Strategy for the period 2020–2025.

3.2 Outputs and performance indicators[18] for Activity 3: CAPACITY

Summary of outputs in Activity 3: CAPACITY – Support Europe in maintaining state-of-the-art NIS capacities		
Outputs	**Performance indicator**	**Results achieved**
Objective 3.1. Assisting Member States in capacity building		
Output O.3.1.1. Technical training for Member States and EU bodies	Development of at least 1 training material to support operational practices of CSIRTs in Europe. Contribution of at least 5 CSIRTs in the training material validation. Support for at least 3 TRANSITs events.	Two (2) trainings updated/developed, both with an operational focus but one of them with a very high focus on operational practices. Training material positively evaluated in advanced demo by over five CSIRTs Network members No TRANISTS events took place because of COVID-19 restrictions.
Output O.3.1.2. Support EU Member States in the development and assessment of NCSSs	Support for at least 3 Member States in the implementation of NCSS lifecycle (S). Support for stakeholders from at least 12 small-medium sized enterprises engaged in the activity (S). Engagement of stakeholders (national competent authorities or the private sector) from at least 12 EU Member States. (E).	ENISA supported three EU Member States in the evaluation of their NCSS through the dissemination of best practices and distribution of related guidelines and tools. ENISA also supported one EFTA by providing input and comments in the draft document of their national cybersecurity strategy.[19] Member States were engaged in the development of the National Capabilities Assessment Framework (acknowledgments included in the study). ENISA engaged 16 small-medium sized enterprises in interviews for a study, 249 SMEs through a survey and 120 public and private organisations that participated in an online workshop. ENISA's NLOs were also engaged in this activity and provided input and comments. ENISA also engaged 26 Member States from NCSS expert group and NIS CG, EC3, Council of Europe and Oxford University have registered to attend the NCSS Workshop. Overall, about 60 participants attended the online NCSS annual workshop.
Output O.3.1.3. Support EU Member States in their incident response development	Identification and report on the number of Member States supported and the type of support provided. 2 CSIRT inventory updates. Updated report on CSIRT and IR landscape in Europe. Support or advisory to at least 2 CSIRTs to enhance their teams' maturity. Support from ENISA for at least 2 international CSIRT or task force initiatives in community forums like the Forum of Incident Response and Security Teams, TF-CSIRT-TI ([19]) or the Global Forum on Cyber Expertise.	The updating of the CSIRT inventory took place in June and in December 2020. Report on Sectoral CSIRT Capabilities – Energy and Air Transport prepared and published. Study on *How to set up CSIRT and SOC* prepared and published. Advice provided for two CSIRTs on how to evaluate and enhance team's maturity. Together with CSIRTs Network Maturity Working group prepared guidelines for remote maturity peer review process for CSIRTs network members. ENISA is in TF-CSIRT steering committee as a member. ENISA provided continuous support of TF-CSIRT Reference Security Incident Taxonomy Working Group and three WG meetings a year. FIRST (Global forum of Incident Response and Security Teams) supporting global CSIRT and PSIRT communities by participating in variety of special interest group activities such as CSIRT services framework (https://www.first.org/standards/frameworks/)
Output O.3.1.4. ISACs for the NISD Sectors in the EU and Member States	Support for at least 3 ISACs (S). Engagement of at least 12 organisations representing at least 3 sectors from at least 8 Member States in this activity (P).	Three ISACs were supported, Financial ISAC, Rail ISAC and Energy ISAC. Three different sectors Finance, Rail and Energy were covered from all Member States, as well as EFTA Member States.

18 https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

19 https://tf-csirt.org/trusted-introducer/

Summary of outputs in Activity 3: CAPACITY – Support Europe in maintaining state-of-the-art NIS capacities		
Outputs	**Performance indicator**	**Results achieved**
Objective 3.2. Supporting EU institutions in capacity building		
Output O.3.2.1. Liaison with the EU agencies on operational issues related to CERT-EU's activities	Consultation with EU agencies and representation of their views at the level of CERT-EU Steering Board.	ENISA attended all foreseen meetings and agreed on a strategic cooperation model with CERT-EU Steering Board.
Output O.3.2.2. Cooperation with relevant EU institutions, agencies and relevant bodies on cybersecurity initiatives	Engagement of the relevant EU stakeholders (including EASA, CERT-EU, EDA (including civil/ defence cooperation), etc.). Engagement of 10 stakeholders in the workshop and in the preparation of the recommendations.	At the September 2020 second edition of the EU Cyber Forum, ENISA Executive Director participated in the panel 'Digital society after COVID-19: building a global cyber resilience regime'. The collaboration was focused on responding to the pandemic, therefore other activities did not go ahead as planned, and consequently no report was produced. ENISA co-organised and moderated the working session 'Cybersecurity certification: EU and global outlook'.
Objective 3.3. Assisting in improving private sector capacity building and general awareness		
Output O.3.3.1. Cybersecurity challenges	Organisation by at least 2 additional EU Member States of national cybersecurity challenges in 2020 and their participation in the ECSC final. Promotion from at least one contact from Non EU country of the international engagement.	Four new EU/EFTA countries engaged in the ECSC Steering Committee during 2020. Two (2) of them confirmed their participation on the ECSC 2021 edition. During 2020, ENISA completed the creation of an international Steering Committee to support the setting up of the International Cyber Security Challenge Teams from as far as South East Asia, Oceania, US, Latin America and Africa engaged, more than 60 contacts from different organisations around the world are currently engaged. The ECSC final for 2020 was cancelled due to the pandemic. In its place an online Hackfest was organized by ENISA with the participation of 20 National Teams from the EU.
Output O.3.3.2. European Cyber Security Month deployment	Participation/support of all 28 EU Member States and at least 10 partners and representatives from different bodies / Member States in/for ECSM 2020 (private and public sectors).	Six (6) more EU Member States and one (1) EFTA country participated actively at the campaign, compared to previous year, bringing about the desired outcome. More than 10 partners from different bodies coming from different bodies and Member States took part in the online ECSM 2020.
Output O.3.3.3. Support EU Member States in development of cybersecurity skills	Engagement of at least 15 organisations representing academia, public institutions and private companies from at least 10 Member States.	ENISA concluded 14 in-depth, semi-structured interviews with organisers of national cybersecurity competitions from 12 Member States. Conducted 20 surveys from different organisations involved in national competition.
Objective 3.4. Response to Article 14 requests under capacity activity and associated outputs are removed following amendment 11 to the 2019 work programme		

3.3 Publications and Deliverables for Activity 3: CAPACITY

List of deliverables for Activity 3: CAPACITY – Support Europe in maintaining state-of-the-art information security network and capacities
Objective 3.1. Assist Member States' capacity building
Output O.3.1.1. Technical trainings for MS and EU bodies Update of CSIRT training material in the area of operational trainings Status: Published – Restricted
Output O.3.1.2. Support EU Member States in the development and assessment of NCSS National Capabilities Assessment Framework Status: Published
Output O.3.1.3. Support EU Member States in their incident response development Sectoral CSIRT Capabilities – Energy and Air Transport Status: Published How to set up CSIRT and SOC Status: Published
Output O.3.1.4. ISACs for the NISD Sectors in the EU and Member States ISAC in a Box Status: Published
Objective 3.3. Awareness raising
Output O.3.3.1. European Cyber Security Challenges ECSC 2020 Analysis Report Status: Published (in March 2021)
Output O.3.3.2. European Cyber Security Month deployment ECSM Deployment Report – 2020 Status: Published (in April 2021)
Output O.3.3.3. Support EU MS in cybersecurity skills development Towards a Common ECSC roadmap Status: Published (in March 2021)

4 ACTIVITY 4: COOPERATION

Foster the operational cooperation within the European cybersecurity community

4.1 Key results in implementing Activity 4: COOPERATION

4.1.1 Objective 1: Cyber-crisis cooperation – outputs

O.4.1.1. Planning of Cyber Europe 2020

Main achievements:

Due to the pandemic, the Cyber Europe exercise execution was initially postponed for June 2021, and is now tentatively planned for June 2022 depending on the evolution of the circumstances of the pandemic.

O.4.1.2. Support activities for cyber exercises

Main achievements:

- Updates and security assessment exercise on the CEP platform
- Support Netherlands and eu-LISA on exercises

ENISA has been developing the cyber exercise platform (CEP) since 2014.

CEP hosts a number of services ENISA offers to Member States and EU institutions, such as: exercise organisation and management, technical incidents. During 2020, ENISA performed major updates to the platform, redesigning for instance the Regeneration Logic and user interface.

The CEP platform opened new opportunities for ENISA to enlarge the user base and thus to offer to the operational cybersecurity communities opportunities to exercise and to gain experience and

knowledge. An in-depth security assessment including a penetration testing took place (as per yearly schedule) to ensure the security of the platform. ENISA didn't identify any major issues and used the results to further improve the infrastructure..

In 2020, ENISA was asked to support the Netherlands with the scenario of the BlueOLEX exercise. The exercise consisted in a discussion-based table top exercise held online. ENISA supported eu-LISA in organising and executing a cyber-exercise together with participating Member States.

O.4.1.3. Support activities for cybersecurity collaboration with other EU institutions and bodies

Main achievements:

- Organised a tabletop exercise for the 36th meeting of ITAC
- Development of cyber threat assessment methodology
- Development of an impact assessment model

In 2020, the EU Agencies ICT Advisory Committee (ICTAC) asked ENISA to organise a tabletop exercise for the 36th meeting of ICTAC. The mission of ICTAC is to promote inter-agency cooperation on issues of common interest in the area of Information and Communication Technologies, through knowledge and experience sharing and exchange of good practice. ENISA co-organised the tabletop cyber exercise with the ICTAC and CERT-EU.

Furthermore, ENISA produced a draft on a new threat assessment methodology. This methodology was to be mainly used by Blueprint stakeholders, but could also be employed by any related bodies who wanted to take advantage of it. It is based loosely on an existing approach by the NATO Cyber Threat Assessment Cell (CTAC). The new methodology is based more on a reproducible mathematical approach with less 'wiggle room' for the quantitative assessments to facilitate comparisons of assessment results by different organisations.

Lastly, ENISA designed a model EU institutions can use to assess the impact of cyberattacks. The model was designed based on relevant existing literature, on input from various experts, and on current practices within theEU institutions. The final result provided the basis for a fully functional and operational framework to be developed in 2021. This work will support collaboration between EU Institutions regarding cyber crises management as described in the Blueprint recommendation.

O.4.1.4. Supporting the implementation of the information hub

Main achievements:

- Development of new functionalities of OpenCSAM

ENISA launched the Open Cyber Situational Awareness Machine (OpenCSAM) 3rd round of development in 2020 and will be concluded in 2021.

The development of new functionalities for the tool was based on stakeholders inputs gathered in May 2020. Among those new functionalities are included the integration with SHODAN and Twitter enterprise APIs and a collaboration capability based on user-defined circles of trust. As a result, the tool is now used by over 90 analysts from EUIs, CSIRTs and other Member States' Agencies/Organisations.

O.4.1.5. Supporting the EU Cyber Crisis Cooperation Blueprint

Main achievements:

- Support the EU Cyber Crisis Cooperation Blueprint
- Development of a cooperation portal for the Cyber Crises Liaison Network (CyCLONe)

To support the EU Cyber Crisis Cooperation Blueprint, ENISA developed a Standard Operating Procedures document for the Operational level cooperation of EU Institutions. The document integrated into a joint SOP document of the Commission services (DG CNECT) and is currently under discussion by relative stakeholders from EUIs in two separate working groups.

ENISA also developed and maintained a cooperation portal for the Cyber Crises Liaison Network (CyCLONe) in June 2020, following its appointment as the Secretariat of this group.

4.1.2 Objective 2: Community building and operational cooperation – outputs

O.4.2.1. EU CSIRTs Network support

Main achievements:

- Weekly report during pandemic on cyber threats to EU Member States
- CSIRTs Network Secretariat support
- Annual trust exercise

Second Report to the Cooperation Group in line with the NIS Directive requirements

The NIS Directive established the CSIRTs Network 'to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation'. To date, there are 39 appointed Members to the CSIRTs Network covering all Member States and CERT-EU. ENISA supported the operations of the Network as the Secretariat and the Commission services participated as an observer. The COVID-19 related cybersecurity situation of the significant general security event was a pivotal moment for the growth of the Network. The CSIRTs Network moved to remote escalated cooperation and, at the same time, the ENISA CSIRTs Network Secretariat strengthened the underlying infrastructure to support this new normal operational mode. The Network is ready to respond to COVID-19 related cyber threats. From March to May 2020, the Network issued a weekly report to the EU and MS higher levels/and their constituencies, providing summaries and recommendations on how to face the cyber threats related to the outbreak.

The NIS Directive established the CSIRTs Network 'to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation'. To date, there are 39 appointed Members to the CSIRTs Network covering all Member States and CERT-EU.

The CSIRTs Network Secretariat supported the functioning of the Network in full virtual mode since March 2020. This included supporting the governance in the Trio handover, from Romania, Finland, Croatia to Germany, Portugal and Slovenia; and change of the Chair in July 2020, from Finland to Slovenia. Moreover, the CSIRTs Network Secretariat facilitated the update of the Network's Work Programme for 2020-2023, the NIS Directive review process initiated by the Commission services, the Working Groups cooperation and dedicated ad hoc calls.

Furthermore, the CSIRTs Network managed to have the 11th meeting in Stockholm in February but moved to virtual for the 11th under Croatian Presidency including a shared session with the Cooperation Group (CG) and 12th under German Presidency. The annual trust / team building exercise took place online in parallel with the 12th meeting and tested the CSIRTs Network members' technical skills and knowledge of the Terms of reference (ToR), Rules of Procedure (RoP) and Standard operating procedure (SOP).

The CSIRTs Network also successfully completed the second Report to the Cooperation Group in line with the NIS Directive requirements. The report covers the period from 1st of July 2018 to 1st of February 2020. During the reporting period, the CSIRTs Network held four meetings (Vienna, Brussels, Bucharest and Helsinki), three of the meetings also provided the opportunity ofa shared session with the Cooperation Group (CG). Activity of the Working Groups is detailed in the report as well as the infrastructure and tools usage. The report assesses the experience gained with the operational cooperation, including conclusions and recommendations.

O.4.2.2. Support the fight against cybercrime and collaboration across CSIRTs, Law Enforcement Agency and other operational communities

Main achievements:

- 2020 Report on CSIRT-Law Enforcement Cooperation
- Training material on CSIRT-Law Enforcement Cooperation
- Annual ENISA-EC3 Workshop for national and governmental CSIRTs and their LEA counterparts

ENISA compiled and published the 2020 Report on CSIRT-LE Cooperation[20]. The report proposes a methodology to analyse the legal and organisational framework shaping the CSIRTs and law enforcement (LE) cooperation as well as their interaction with the judiciary. It also identifies synergies and potential interferences.

20 https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation

ENISA also developed and published training material (a handbook and a toolset) focused on Aspects of Cooperation between CSIRTs and Law Enforcement Agencies[21]. This training material, which mainly stems from the 2020 Report on CSIRT-LE cooperation, is based on three case studies (theft of confidential data, ransomware DDOS and malware blended attack).

The workshop[22] allowed a discussion on ways to cooperate effectively to respond to cybercrime and the sharing of success stories. This event, by invitation only, took place as a virtual event due to the pandemic.

ENISA invited CERT-EU for the production of deliverables and to the workshop.

21 https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training material/legal-cooperation#Aspects

22 https://www.enisa.europa.eu/news/enisa-news/ninth-enisa-ec3-workshop-on-csirt-le-cooperation-standing-shoulder-to-shoulder-to-counter-cybercrime

O.4.2.3. Supporting the operations of the MeliCERTes platform

Main achievements:

- Support 21 CSIRTs network members in usage of MeliCETes

ENISA provided support to 21 CSIRTs network members in their usage of MeliCETes Platform including on boarding new teams, support of interoperability tests, necessary communication between CSIRTs network members and MeliCERTes consortium.

ENISA provided support for MeliCERTes 2.0 requirements collection and approval by CSIRTs network members in close cooperation with MeliCERTes consortium. This included also participation in MeliCERTes steering board, CEF governance board and tri-partial meetings between Consortium, ENISA and the Commission services.

4.2 Outputs and performance indicators for Activity 4: COOPERATION

Summary of outputs in Activity 4: COOPERATION – Foster the operational cooperation within the European cybersecurity community		
Outputs	**Performance indicator**	**Results achieved**
Objective 4.1. Cyber-crisis cooperation		
Output O.4.1.1. Planning of Cyber Europe 2020	Confirmation of support from at least 80 % of EU Member States / EFTA countries for Cyber Europe 2020.	Due to the pandemic the planned Cyber Europe 2020 exercise was postponed and is currently planned for June 2022. Nevertheless the planning of the Cyber Europe exercise continued to the extend possible involving all EU MS and EFTA countries.
Output O.4.1.2. Support activities for cyber exercises	Organising in 2020 of at least one exercise with two different entities.	Organised BlueOLEX cyber exercise with one (1) of the Member States. ENISA also supported eu-LISA in Multi-System Exercise (MSE).
Output O.4.1.3. Support activities for cybersecurity collaboration with other EU institutions and bodies	Achieving at least 3 major collaboration tasks from the roadmap.	ICTAC cyber exercise planned, organised and executed in collaboration with CERT-EU. EUISOPs exercise planned in collaboration with CERT-EU, and the EC3, but postponed later on. Cyber Diplo TTX planned in collaboration with CERT-EU, EC3, however, exercise cancelled due to COVID-19 this exercise. The objectives of the MoU for the next two years (2020-2021) included the development of an impact assessment model and a Cyberthreat assessment methodology under the context of the MoU of the EU Agencies (EDA, Europol, EEAS, CERT EU, ENISA)
Output O.4.1.4. Supporting the implementation of the information hub	Establishing communication. Evaluation of the tool by at least 3 EU bodies/agencies. Publishing on a quarterly basis EU Cybersecurity Technical Situation Reports.	EU survey sent to OpenCSAM users and conducted in May 2020 to receive inputs and requirements for the 3rd spiral of development (evaluation). At least four (4) EU bodies/agencies participated. Publication of eight (8) EU situation reports in relation to the COVID-19 crisis. Publication of weekly OSINT Situational Awareness reports (44 reports in 2020) CTI Reports were published on a weekly basis throughout the year.
Output O.4.1.5. Supporting the EU cyber crisis cooperation blueprint – replaced by O.4.1.3 following amendment 13 to the 2019 work programme.	Consulting at least 3 stakeholders of the Blueprint.	Two (2) rounds of consultation for the EUIs Operational SOPs between Blueprint stakeholders (ENISA, DG CNECT EEAS, DG Migration and Home Affairs, DG ECHO, Secretariat-General of Commission, CERT-EU).

Summary of outputs in Activity 4: COOPERATION – Foster the operational cooperation within the European cybersecurity community		
Outputs	**Performance indicator**	**Results achieved**
Objective 4.2. Community building and operational cooperation		
Output O.4.2.1. EU CSIRTs Network support	Organising at least 1 CSIRT Network meeting. Participation of 90 % of Member States' standing CSIRT representatives and CERT-EU in CSIRTs Network regular meetings. Provision of support to CSIRT Network chair in preparation of the next evaluation report for the cooperation group. Provision of conference call facility backup for the need of the CSIRT Network operations. Completion of at least 2 penetration tests and necessary security and functionality improvements to the Cooperation portal. Holding of at least 1 team-building event during regular CSIRT Network meeting. Completion of at least 4 communications checks to test CSIRT Network communication channels readiness. Provision of active secretariat support during crisis and escalated cooperation modes.	Three (3) meeting of the CSIRTs Network Organised: one (1) physical and two (2) virtual, 11th Meeting, under Croatian Presidency, and 12th Meeting, under the German Presidency, with all CSIRTs Network Members Participation. Supported the finalisation of the Second Report to the Cooperation Group Conference and tools facilities provided in support of the operation of the CSIRTs Network in default and alert cooperation modes. Two (2) penetration tests and necessary security and functionality improvements to the Cooperation portal. Trust / team building exercise ran online in parallel to the 12th CSIRTs Network virtual meeting aimed at testing the CSIRTs Network technical skills and knowledge of the Terms of reference (ToR) Rules of Procedure (RoP) and Standard operating procedure (SOP) One communication check completed (two planned on working group leader request) and all CSIRTs Network Communications channels fully utilised during the escalated cooperation mode from 19 March to May 2020 during COVID-19 related cyber security situation and default cooperation mode till December 2020 (both cooperation mode fully relied on the communications tools.) Active support to enable the escalated cooperation mode from 19 March to 6 May 2020 during COVID-19 related cyber security situation.
Output O.4.2.2. Support fight against cybercrime and collaboration across CSIRTs, Law Enforcement Agency and other operational communities	Participation of at least 5 Member States' CSIRT representatives, 5 Member States' law enforcement representatives and EC3 in the roadmap's preparation. Participation of at least 15 Member States in ENISA/EC3 annual workshop. Engagement with CERT-EU on structured cooperation.	In 2020, ENISA produced a Report on CSIRTs and LE cooperation. The preparation of the report mobilised the participation of seven (7) Member States' CSIRT representatives, six (6) Member States and one (1) EFTA country law enforcement representatives, EC3 plus five (5) Member States' judiciary representatives. They all provided input during the data collection phase and/or during the review phase. Representatives from 18 Member States, plus three (3) EFTA countries, the UK, EU Institutions, Bodies and International Organisations took part in the 9th ENISA/EC3 Workshop that took place on 16 September 2020.
Output O.4.2.3. Supporting the operations of MeliCERTes platform	Provision of tool integration and support to at least 10 CSIRTs using MeliCERTes according to agreed operational procedures.	21 teams installed MeliCERTes 1.0. ENISA supported on boarding of teams and interoperability tests.
Objective 4.3. Response to Article 14 requests under community activity and associated outputs are removed following amendment 16 to the 2019 work programme		

4.3 Publications and Deliverables[23] for Activity 4: COOPERATION

List of deliverables for Activity 4: COOPERATION – Foster the operational cooperation within the European cybersecurity community
Objective 4.1. Cyber-crisis cooperation
Output O.4.1.1. Planning of Cyber Europe 2020 CE2020 After Action Report Status: Delayed
Objective 4.2. Community building and operational cooperation
Output O.4.2.1. EU CSIRT Network support Proactive detection – Measures and information sources Proactive detection – Good practices gap analysis recommendations Proactive detection – Measures and information sources Status: Published
Output O.4.2.2. Support the fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities 2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries Status: Published (January 2021) Aspects of Cooperation between CSIRTS and LE - Handbook, Document for trainers Status: Published (January 2021) Aspects of Cooperation between CSIRTS and LE - Toolset, Document for trainees Status: Published (January 2021)

23 https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

5 ACTIVITY 5: CYBERSECURITY CERTIFICATION

Developing security certification schemes for digital products, services and processes

5.1 Key results in implementing Activity 5: CYBERSECURITY CERTIFICATION

Objective 1: Support activities related to cybersecurity certification – outputs

O.5.1.1. Support the European Cybersecurity Certification Group, potential subgroups, and the Stakeholder Cybersecurity Certification Group

- ENISA supports the European Commission in the chair's role of ECCG

Main achievements:

ENISA supported the European Commission in its role as chair of the ECCG, and the subgroups thereof, by providing content and organisational support. ENISA also carried out its tasks as co-chair with the Commission of the SCCG, and provided secretariat services.

O.5.1.2. Research and analysis of the market as an enabler for certification

- Proposed set of methodological steps to allow for a market analysis

Main achievements:

A study was undertaken on identifying an initial set of methodological steps to allow for a market analysis on cybersecurity certification of ICT products, ICT services, and ICT processes. The performance of a market analysis on cybersecurity certification aimed at contributing to the EU cybersecurity certification framework and the planning activities of the Commission services, the ECCG and the SCCG by identifying future areas for cybersecurity certification. The proposed steps identified in the study cover:

- the identification of the context of the market analysis;
- the scope of the target of analysis;
- an assessment of the impact of a cybersecurity certification initiative;
- the identification of the available options and possible initiatives.

O.5.1.3. Set-up and maintenance of a certification portal and associated services

Main achievements:

- Development of public cybersecurity certification website

ENISA opted for a CIRCA BC solution, offered by DIGIT, in order to establish a certification management of IT system (CerMIT) to provide securely a cooperation platform for its certification stakeholder community, including the ad hoc Working Groups.

The Agency also launched the development of a public cybersecurity certification website in accordance with article 50 of the CSA in 2020 and reached the phase of initial process definition, technical set up, and consultations with Member States.

Objective 2: Developing candidate cybersecurity certification schemes – outputs

O.5.2.1. Hands on tasks in cybersecurity certification of products, services and processes

Main achievements:

- The Risk Assessment and Assurance Level definition project (RA&AL)

ENISA drew a 'Methodology for consistent, risk based definition of cybersecurity certifications schemes', (hereinafter called, 'Methodology') to determineassurance levels in cybersecurity certification particularly in sectoral schemes. Examples ofsuch sectoral systems are mobile networks and services, health telematics, payment or mobility infrastructures.

This Methodology can be combined with common ISO/IEC 27005-conformant risk assessment tools and can generate a sound understanding of the sectoral system concerning cybersecurity at business process and at component level.

The Methodology enables the implementation of key requirements of the EU Cybersecurity Act and has the potential to promote the market acceptance of cybersecurity certification. This methodology was presented to CEN CENELEC in relation to European standardisation activities.

ENISA organised the Cybersecurity Certification Conference virtually and from Brussels on 18 December 2020.

O.5.2.2. Tasks related to specific candidate schemes and ad hoc working groups

Main achievements:

- The candidate European Common Criteria Scheme (EUCC)
- The candidate European Cloud Services Scheme (EUCS)

Following the Commission request ref ARES(2019)4895286 dated 20/07/2019, ENISA prepared the candidate EUCC scheme on ICT products, to serve as a successor of the Senior Officials Group on Information Systems Security Mutual Recognition Agreement (SOG-IS MRA). This candidate European cybersecurity certification scheme focuses on certification of ICT products. ENISA, and the dedicated Ad Hoc Working Group of experts and stakeholders, in close collaboration with the ECCG, worked on finalising the first draft.

This draft version was made public for consultation in July 2020. ENISA invited all relevant stakeholders to bring forward their recommendations, remarks, or share their concerns in an open, transparent and inclusive consultation process. Both the ECCG and the SCCG participated in the public consultation as well.

Based on the ECCG Opinion finalised in December 2020, ENISA will transfer the candidate scheme to the Commission, as to serve as a reference for the Implementing Act for the scheme.

ENISA continued providing its support to the Commission for follow up activities. Such activities include the development of the the necessary guidance to facilitate transition between current SOG-IS practices and the new rules set by the scheme, and the contribution to the work related to the establishment of a scheme maintenance organisation.

Following the Commission request ARES (2019)7197658, dated 21/11/2019, ENISA also prepared a candidate European cybersecurity certification scheme on cloud services (EUCS). The work on this candidate scheme started in the beginning of 2020 after the Ad Hoc Working Group of experts and stakeholders was constituted.

Together with the Ad Hoc Working Group, ENISA drafted the first version of the EUCS candidate scheme following the advice and close cooperation of the ECCG members. The draft EUCS candidate scheme produces a coherent approach on the security of cloud services taking into account the EU regulatory framework, international standards, best industrial practices, as well as with existing (national) certification schemes in EU Member States.

The diverse set of market players, complex systems and constantly evolving landscape of cloud services, along with different schemes in Member States, represent challenges to the development of cloud services in general. The draft EUCS candidate scheme tackles these challenges by calling for cybersecurity best practices across three levels of assurance and by allowing for a transition from current national schemes to the EU-level. By defining a security baseline for every assurance level, the draft EUCS candidate scheme is a horizontal and technological scheme that intends to provide cybersecurity assurance throughout the cloud supply chain, and forms a sound basis for sectoral schemes. The structuring principles of the scheme were submitted to the SCCG members and to a limited pool of experts over the summer, and the first consolidated version was presented for public consultation in December 2020.

Following the Commission request, ENISA prepared a candidate European cybersecurity certification scheme on cloud services (EUCS). This candidate scheme started its work in the beginning of 2020 after an Ad Hoc Working Group of experts and stakeholders was appointed.

5.2 Outputs and performance indicators[24] for Activity 5: CYBERSECURITY CERTIFICATION

Summary of outputs in Activity 5: CYBERSECURITY CERTIFICATION – Developing security certification schemes for digital products, services and processes		
Outputs	**Performance indicator**	**Results achieved**
Objective 5.1. Support activities related to cybersecurity certification		
Output O.5.1.1. Support the European Cybersecurity Certification Group, potential subgroups and the Stakeholder Cybersecurity Certification Group	Planning and execution of tasks related to meetings; European Commission feedback	ENISA supported both the ECCG along with its subgroup as well as the SCCG. From June to December three (3) meetings were organised in close cooperation with the Commission. ENISA provided the secretariat, organised the meetings, supported the written procedures and the process of the Opinion on the URWP for the Commission. An additional six (6) ECCG meetings were held.
Output O.5.1.2. Research and analysis of the market as an enabler for certification	Provision of input by eight Member States and ten industry representatives.	ENISA focused on an analysis method concerning the cybersecurity market. Representatives of 27 Member States (under the ECCG) and 50 representatives from across the industry, research, European Standards Organisations and private sector associations (under the SCCG) provided input during the preparation of the methodological steps.
Output O.5.1.3. Set-up and maintenance of a Certification portal and associated services	Meeting milestones, in terms of implementation and usability of the resources provided; available portal for the existing European certification schemes	CERMIT: A multi-stakeholder collaboration platform developed for internal use of the Ad Hoc Working Groups and their subgroups to exchange, work out and store data related to their tasks (e.g. developing certification schemes, and other project task related work. The platform is based upon a Commission based exchange environment (CIRCA BC) in close collaboration with DIGIT for implementation and maintenance. A co-editing tool was added in cooperation with DG DIGIT to allow for multiple users to support the Ad Hoc Working Groups concurrently. Regarding the EU Cybersecurity Certification Website: Technical basis with the baseline functionalities for the website was ready by the end of 2020.
Objective 5.2. Developing candidate cybersecurity certification schemes		
Output O.5.2.1. Hands on tasks in the area of cybersecurity certification of products, services and processes	Identification of number of stakeholders and actively participating in the drafting, preparation and consultation process of the scheme; Engagement at least 10 private and or public organisations. Event participation of at least 60 relevant stakeholders.	For the EU Common Criteria scheme:ENISA presented the report to the ECCG (representatives of 27 Member States and SCCG (50 Members of the Stakeholder Cybersecurity Certification Group). ENISA finalised on time the Risk Assessment and Assurance Level definition project (RA&AL). The Agency addressed the planned scope.The creation of the main deliverable, the 'Methodology for consistent, risk based definition of cybersecurity certifications schemes' was accompanied by the ad-hoc working group (20 external experts). The draft report will be presented to the ECCG (27 Member States representatives). Its publication is planned as soon as the result has been implemented in a new revision. The deliverable is planned for re-use for the preparation of the EU 5G candidate scheme as well as other schemes that ENISA may assist with. ENISA organised a Cybersecurity Certification Conference in December, to provide an update on the current state of play on the development of the candidate EU Common Criteria Scheme and the candidate EU Cloud services scheme. The event gathered a total of about 500-600 participants including Commission stakeholders.

24 https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0

Summary of outputs in Activity 5: CYBERSECURITY CERTIFICATION – Developing security certification schemes for digital products, services and processes		
Outputs	**Performance indicator**	**Results achieved**
Output O.5.2.2. Tasks related to specific candidate schemes and ad hoc working groups	Production drafts of at least 2 schemes per year or 50 % of the ones requested and prioritised by ECCG and the European Commission for 2020.	Publication of the draft candidate EUCC scheme v1.0 for review, and update of the scheme v1.1 for the ECCG opinion, following kick off in December 2019 and delivery as foreseen in June 2020. Development of a first set of guidance to support the EUCC scheme. The candidate Cloud services scheme started in March and ENISA delivered THE first draft in December. ENISA presented both draft candidate cybersecurity certification schemes in a timely manner.

5.3 Publications and Deliverables for Activity 5: CERTIFICATION

List of deliverables for Activity 5: CERTIFICATION – Developing security certification schemes for digital products, services and processes
Objective 5.1. Support activities related to cybersecurity certification
Output O.5.1.2. Research and analysis of the market as an enabler for certification Market_Analysis_Methodology Status: Published (2021)
Output O.5.1.3. Set-up and maintenance of a certification portal and associated services Status: Collaboration portal CermIT now in use in scheme preparation collaboration. Development of a public ENISA cybersecurity certification website started.
Objective 5.2. Developing candidate cybersecurity certification schemes
Output O.5.2.1. Hands on tasks in cybersecurity certification of products, services and processes RA- AL – Method for consistent risk-based definition of CS certification schemes Status: Delivered (Publication in 2021)
Output O.5.2.2. Tasks related to specific candidate schemes and ad hoc working groups EUCS – Cloud Services Scheme Status: Published Cybersecurity Certification: EUCC Candidate Scheme Status: Published

6 ACTIVITY 6: ENABLING

Reinforce ENISA's impact

6.3.1 Objective 1: Management and compliance

a) MANAGEMENT

This topic is covered in Part II.1, 'Management Board.

The Resources Department

The Resources Department administered a range of services across finance and procurement, ICT, facilities management, health and safety physical security, and liaison with local authorities.

TheOut of a total of 24 posts assigned to the Resource Department, 15 staff members contributed to the tasks of internal controls and risk management (including Head of department), Finance and Procurement Unit, and Corporate support services.

The Accounting and compliance officer acted as Head of Finance and Procurement unit and not calculated in the total number of staff members.

Also, as of March 2020 Human Resources reported directly to the Executive Director. The Unit was managed by the Head of Data Security and Standardisation as acting Head of Unit. The unit had 4 staff members.

ENISA resorted to external staff to allow for the full execution of tasks of the department. A total of 10 interim agents was assigned to the Resources department and 5 interim agents assigned to Human Resources to cover vacant posts and extra workload.

In March 2020 the Executive Director established the Executive Director's support team to strengthen internal coordination capacity at ENISA, among other tasks previously in Resources Department's remit.

As a result of the problem analysis endorsed by the Management Board in February , the Agency started a reorganisation process coordinated by the Executive Director's support team and the Human Resources unit, both reporting directly to the Executive Director.

The objective of the Resources Department is to equip the agency with state-of-the-art strategies, programmes and tools to optimise the use of resources across ENISA, enabling it to deliver on the work programme and statutory commitments. The department initiated specific projects to support the delivery of the work programme, such as the update of the Business Continuity Plan and ENISA internal IT Strategy but the agency could not provide them.

The Core Operations Department

The Core Operations Department coordinated the delivery of ENISA's core activities. As such, its main role is to deliver the work pertaining to Activities A1–A5 of the work programme. The Policy Office and the Public Affairs Team also reported to the Department. The support The Core Operations Department also supported the ENISA Advisory Group and the National Liaison Officers (NLO) Network.

With 61 staff members and 11 posts unfilled in 2020, the Core Operations Department counted a total of 72 posts. In addition, the department had the support of 16 external staff, covering the functions of vacant posts and extra workload.

b) POLICY OFFICE

The Policy Office reported to the Head of Core Operations Department. Through the Policy Office, the Agency initiated and developed strategic cooperation with active relevant stakeholders from the cybersecurity community, and managed Public Access to Documents (PAD) requests pursuant to Regulation (EC) No 1049/2001.

The Public Affairs Team (PAT) reported to the Head of the Policy Office and coordinated all communication activities, including media and press activities such as press releases, news items and interviews to enhance the reputation, visibility and the public image of the Agency. It supported the entire Agency regarding publications, social media promotion, website management, public affairs activities and awareness campaigns. PAT was also responsible for establishing ENISA's corporate visual identity and branding.

Due to pandemic in 2020, limited number of physical events took place, however the team supported events taking place online. PAT also managed the ENISA website.

Besides, additional information on the activities delivered by the Policy Unit and Public Affairs team are listed in Objective 6.2 Engagement with stakeholders and international activities.

In March 2020 the Executive Director established the Executive Director's support team to strengthen internal coordination at ENISA, and perform other tasks previously in the Policy Office's remit.

c) INTERNAL CONTROL

This topic is covered in Part III – 'Assessment of the effectiveness of the internal control systems'.

In 2020, ENISA successfully hosted and evolved the central component of MeliCERTes. MeliCERTes is the primary collaboration platform for the CSIRTs of participating Member States.

d) INFORMATION TECHNOLOGY

TheAgency migrated to a new fully operating datacentre in the course of the year and, in cooperation with another EU Agency it synergised to use the latter as a Disaster Recovery (DR) site for some of its critical corporate IT services.

TheAgency followed up with actions to strengthen its own cybersecurity standing in the CIA triad (confidentiality, integrity, availability). The Agency upgraded its entire email system to the latest version, provisioning for load balancing to enhance availability and removal of older protocols. The Agency also successfully reinforced its directory services and strengthenedits security filtering and antispam polices.

IT supported all internal digital infrastructure in the Agency, this includes but is not limited to core applications for business use and operation systems. Due to the pandemic, the Agency's methods had to extend to new services; to address such shortcomings as identified in terms of electronic signatures orvideoconferencing for large conferences for instance. Mitigation measures were proposed and started being implemented in late 2020, allowing the Agency to continue operating remotely.

ENISA successfully hosted and developed the central component of MeliCERTes. MeliCERTes was the primary collaboration platform for CSIRTs of participating Member States. The platform standsas a means to improve EU Member States preparedness, cooperation and coordination to improve cyber threat and cross-border incident response. ENISA IT incorporated the MeliCERTes support service delivery structure into its own on-premises JIRA ticketing system, creating a solid structure for incident response.

Task	Objective	Level of completion in 2020
Keep ENISA systems safe from cybersecurity incidents (from exterior) – detect, prevent, react and recover from threats	Security	100 %
ENISA IT managed servers patched in time	Security	100 %
Exchange server availability	Efficiency	100 %
Availability of internal applications	Availability	95%
Help desk, reply with success to all service requests	Efficiency	99 %

e) FINANCE AND PROCUREMENT

This topic is covered in Part II.3, 'Budgetary and financial management'.

f) LEGAL AFFAIRS, DATA PROTECTION AND INFORMATION SECURITY COORDINATION

Legal Affairs

Legal affairs continued supporting the legal aspects associated with the operation of the Agency; thus ensured the efficient legal support within the spectrum of activities of ENISA. This included dealing with matters such as (indicatively) contracts, procurement, employment related matters, data protection in collaboration with the Data Protection Officer, access to documents and corporate governance matters. The Legal Affairs function also included dealing with complaints to the European Ombudsman. In general the Legal Affairs ensured also the interpretation and implementation of primary and secondary legislation to ENISA activities, provided legal advice and drafted reports on ad hoc legal issues. ENISA resorted to external Legal counsel only to assist in the resolution of staff matters.

Data Protection Compliance tasks and Data protection Office

ENISA is subject to Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by EU institutions, bodies, offices and agencies (EUDPR)[25]. A Data Protection Officer was appointed according to EUDPR and relevant ENISA implementing rules[26].

Within 2020, ENISA complied with all requests for information/reporting, as well as relevant recommendations of the European Data Protection Supervisor (EDPS), including in particular:

- EDPS monitoring exercise on registers under Art. 31(5) EUDPR, which involved the publication of ENISA's online register of data processing activities[27].
- EDPS Strategy to comply with Schrems II ruling, which encompassed an Agency-wide stock taking exercise and reporting on cases of transfers of personal data to third countries (following CJEU Schrems II Judgment)[28].

25 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0039.01.ENG&toc=OJ:L:2018:295:TOC (EUDPR).

26 ENISA MB Decision 2019/2, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB %20Decision %20MB_2019_2_implementing %20data %20protection %20regulation.pdf/view

27 https://www.enisa.europa.eu/about-enisa/data-protection/enisa2019s-central-register-of-data-processing-activities

28 https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en

In this context, the DPO's activities within 2020 included:

- Provision of various data protection opinions and advice in accordance with EUDPR and on different topics across the Agency, including on records of processing activities, Data Protection Impact Assessments and security of processing;
- Maintenance of the ENISA's central register of data processing activities;
- Data protection compliance monitoring, especially through contract monitoring and monitoring of international transfers of personal data;
- Awareness raising through the provision of data protection training to ENISA's staff members;
- Collaboration with the EDPS and the EU Institutions and Agencies (EUIs) DPOs network, including the co-chairing of the joint EUIs DPOs-ICTAC Working Group and participation in the DPOs Working Group on procurement;
- Provision of data protection advice to CEDEFOP, in the context of the standing co-operation between ENISA and CEDEFOP and the relevant SLA that has been established between the two Agencies.

Information Security coordination

The Chief Information Security Officer (CISO) coordinates the Information Security Management System on behalf of the Authorising Officer. In particular, the CISO advises the ICT Unit to develop and implement information security policies, standards, guidelines and baselines that seek to secure the confidentiality, integrity and availability of the information systems of the Agency. The CISO is instrumental in incident handling and incident response and security event monitoring. The CISO also leads the security training for the Agency's staff and he provides security guidance on all IT projects, including the evaluation and recommendation of technical controls. For the referenced year, the ENISA CISO contributed to the following activities and objectives:

- Conducting an annual risk assessment exercise and follow-up actions.
  - Monitoring and reporting the following to ENISA Internal IT Advisory Committee (ITAC).
  - Performed regular vulnerability assessments and penetrations tests.
  - Network security monitoring and incident response.
  - Implemented the security awareness policy and improved the IT Security training
- Non-compliances with policy identified and addressed
  - Advising on security policies and updating existing ones in line with the evolution of threats and risks
  - Implementing new systems and tools that can support improvements on Information Security. All these activities where conducted in the context of a re-organisation process that eventually changed the governance model and implicitly the roles and responsibilities.

6.3.2 Objective 2: Engagement with stakeholders and international activities

a) STAKEHOLDER COMMUNICATION AND DISSEMINATION OF ENISA'S DELIVERABLES[29].

In 2020, ENISA maintained its efforts to improve its focus on key activities and to engage the highest possible number of stakeholders. This includes the different groups of stakeholders from Member States, EU Institutions, bodies and agencies as well as academia, industry, the public, etc. In its engagement with the stakeholders, ENISA is guided by principles such as balanced representation, openness, transparency and inclusiveness. This is evidenced by organising open calls for expression of interest for various groups that contribute to ENISA work programme implementation.

Anew strategy was adopted for the Agency in 2020. The first objective of this strategy is to achieve 'Empowered and Engaged Communities across the Cybersecurity Ecosystem' striving for a cross sectoral, all-inclusive cooperation with our stakeholders.

The Management Board appointed the Advisory group in the course of the year. The appointment was based on a proposal of the Executive Director, with balanced numbers between female and male representatives. The group represents 14 countries with a mixture of old and new EU Members.

29 Work delivered by ENISA such as reports, recommendations, info notes, opinion papers, tools, platforms, training material or contents, etc.

Dissemination and outreach

ENISA further engaged in developing tools and using channels, including its website, for the dissemination of ENISA's deliverables and for outreach, with a strong emphasis on social media. ENISA saw an increase in all relevant social media metrics: The Agency's audience (followers) increased by 33% compared to 2019. In addition, there was a 27.4% increase in published posts, a 59.4% increase in post impressions and a 121% increase in engagements. ENISA's website also received 12% more visits compared to 2019 while the number of downloads of ENISA's publications was increased by 30%.

Early on in 2020, ENISA conducted regular press interviews during events. In January 2020, ENISA gave 5 interviews organised at the FIC conference in France and 3 interviews organised at the DLD conference in Germany. This trend was interrupted by the pandemic and the total number of spokesperson interviews in 2020 for ENISA ENISA dropped to 15, a total lower thank in 2019. In addition, ENISA was mentioned around 30 times in top-tier, Brussels-based and national media outlets.

During the initial phases of the pandemic, ENISA also provided tips and recommendations for cyber secure teleworking, videoconferencing and selling online etc. A Covid-19 information hub was created on the website to facilitate the outreach of this information to a wider audience.

Two other awareness and outreach activities were organised to reach stakeholders online. ENISA's campaign to generate awareness (1) about different types of online threats and (2) the promotion of ENISA Threat Landscape, achieved more than 1.2 million impressions in Twitter and LinkedIn. The campaign for the promotion of ENISA's work related to the EU Cybersecurity Package generated more than 1.5 million Twitter impressions and more than 16 thousand engagements.

Internal communications

- In 2020, ENISA took a step forward to enhance staff engagement and to exploit opportunities for pooling and sharing resources. The scope of this activity was limited on organisational and prioritisation grounds; main activities followed the pattern described hereinafter:
- Regular updates to staff by internal announcements on aspects concerning staff; particular attention was paid to aspects related to the pandemic in an effort to keep cohesion across the Agency staff.
- Regular sessions regarding the evolving reorganisation of recourses that were carried out at all layers of hierarchy and levels of involvement.
- Launching and utilising specific instruments such as staff interviews, to allow quicker integration of incoming staff.
- Adapting organisational frameworks to the Agency's corporate culture and practices, by shaping appropriately the competences framework.
- A staff survey activity in relation to the reorganisation in 2020 also took place.

With regards to the reorganisation, the Executive Director's Support Team supported a number of internal communications activities. In January 2020, a staff day was held to kick off the reorganisation with a staff consultation process. As of 15 April a weekly Question and Answer session (remotely) was also organised on various topics related to the reorganisation, to give staff the opportunity to ask questions. A new webpage was created on the Intraenisa to provide information to staff on the reorganisation.

The Executive Director sent regular emails and videos to all staff with updates on the reorganisation and other activities of relevance to staff.

Because of the pandemic, a number of events and team activities were cancelled or postponed . A few units still managed however to organise team building activities during the summer.

ENISA's internal communications objectives for 2020.

Task	Objective	Level of completion 2020
Maintain staff informed on ENISA Activities (internal communications)	Hold 10 staff meetings per year	27 Q&As[30] and 3 staff seminars meetings took place
Team-building activities	Events with participation of all staff	Impacted by the pandemic COVID-19

30 Due to the process of reorganisation of the Agency in 2020, Questions and Answers sessions were arranged online to all ENISA staff.

ENISA Advisory Group

The ENISA Advisory Group was established by the new CSA. It replaces the Permanent Stakeholder Group. ENISA published a call for expression of interest for the selection of the current Advisory Group early in 2020. Further to the call,ENISA proceeded with the selection and nomination of experts from all sectors specified in the CSA. The current group took office on 1 July 2020 with a mandate of two and a half years.

This group, composed of industry, academia and consumer organisation experts, continues to advise ENISA on drawing up a major part of the annual work programme except regarding the provisions of Title III ('Certification'), on the performance of its tasks and to engage effectively with stakeholder communities.

Two virtual meetings took place in July and November. New rules of procedure for the AG were adopted and activities where the group can assist ENISA with its work programme were identified as planned. ENISA ran a pilot with the Advisory Group to provide feedback on output finalisations. ENISA proposed three different outputs for feedback; output O.1.1.3, Output O.1.2.1[31] and Output O.2.2.4[32]. The result of the feedback received led to a number of changes within the outputs including clarifications and editorial changes, but it also provided valuable input on how to improve specific outputs in 2021.

National Liaison Officers Network

Set up in 2004 as a series of informal points of communications in the Member States, the NLO Network became a statutory body of the Agency via the 2019 Cybersecurity Act.

The NLO Network had 3 virtual meetings in the course of the year: in May, October and December. ENISA also developed, consulted and adopted new rules of procedure for the Network ENISA organised a training for NLOs interested in cloud security in December, after the NLO meeting.

A pilot was run with the NLO Network to provide feedback on output finalisations. Input was provided to 8 outputs of work programme 2020. The result of the input received led to a number of changes within the output and the outreach of the outputs.

b) INTERNATIONAL RELATIONS

Under the Executive Director's guidance and initiative and in line with the approach agreed by the Management Board, ENISA's main focus in 2020 was the implementation of its mandate in relation to the EU internal market. Some activities were carried out to strengthened contacts at an international level, in particular with the US partners to exchange on lessons learned in response to the pandemic.

31 Output 0.1.1.3 and 0.1.2.1 is listed in the table 1.2. Outputs and performance indicators for Activity 1: EXPERTISE

32 Output 0.2.2.4 is reflected in the table 2.2. Outputs and performance indicators for Activity 2: POLICY

PART II (A)
MANAGEMENT

1 MANAGEMENT BOARD

The Management Board had two ordinary meetings in the course of the year plus one extraordinary meeting. The extraordinary meeting took place to endorse the draft single programming document 2021-2023, the statement of estimates 2021 and the establishment plan 2021, among other decisions.

In total, the Management Board made 22 decisions during the year, which include the Agency's new strategy, the establishment of ENISA internal structures, as well as the setting up of the Advisory Group for the period 2020-2023.

In addition, the work programme 2020 was amended in response to the COVID -19 pandemic to shift to online environment for implementing the work programme outputs.

As part of its functions, the Management Board adopted its analysis and assessment of the 2019 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 opinion on the final annual accounts for 2019 and adopted the ENISA Programming Document 2021–2023, including the 2021 budget and the 2021 establishment plan.

Sharing information with the Management Board regularly, ENISA reported on the work programme, budget implementation, and audit and evaluation activities (by e.g. ECA, IAS), among other pertinent matters.

The Management Board endorsed the proposed reorganisation of the Agency's structure. The risks and/or issues identified in the Agency to potentially impact internal and quality controls in addition to the results of the problem analysis performed substantiated the endorsement by the Management Board. The board members remained committed to declaring their interests in order to avoid any conflicts of interest at meetings by providing their annual declarations of commitment and providing updated declarations of interest.

In addition, the Management Board, in agreement with the Commission, continued to engage in the adoption of the necessary implementing measures under the arrangements provided for in Article 110 of the Staff Regulations, namely on procedure for dealing with professional incompetence (MB 2020_10) and on the conduct of administrative inquiries and disciplinary proceedings (MB 2020_13).

The Management Board decisions were prepared by the Executive Board and adopted by the Management Board.

The Executive Board had one formal meeting per quarter.

2 MAJOR DEVELOPMENTS

The ENISA strategy, adopted by the Management Board in June 2020, sets concrete strategic objectives for the Agency and will guide the multiannual programming of the Agency in the coming years. These strategic objectives are as follows:

1. Empowered and engaged communities across the cybersecurity ecosystem;
2. Cybersecurity as an integral part of EU polices;
3. Effective cooperation amongst operational actors within the Union in case of massive cyber incidents;
4. Cutting-edge competences and capabilities in cybersecurity across the Union;
5. A high level of trust in secure digital solutions;
6. Foresight on emerging and future cybersecurity challenges;
7. Efficient and effective cybersecurity information and knowledge management for Europe.

The strategy's high-level objectives are directed at shaping a more digitally secure environment for Member States, EU Institutions, Agencies and Bodies, SMEs, academia and all of Europe's citizens. The European Union Agency for Cybersecurity will use the new strategy to map out its annual work programme to improve the level of cybersecurity across the Union, and specifically to:

- Direct the allocation of its human and financial resources;
- Develop the necessary capabilities under Article 3(4) of the CSA to maintain competitiveness and preparedness.
- Build on the Agency's trusted relationships with stakeholders and communities within the cybersecurity ecosystem across Europe.
- Guide ENISA communications within and beyond the Union, to non-EU countries and international organisations.
- Deepen the knowledge and information sharing of ENISA expertise to reach larger audiences and increase awareness of digital security.
- Provide cybersecurity stakeholders a clear understanding of the Agency's priorities and actions.
- Shape the future outlook of cybersecurity across the Union.

The strategy is both an aggregation of the tasks identified by the Cybersecurity Act and the developed synergies within Articles 5-12 of the CSA.

COVID-19

The second significant development that framed the 2020 work programme was the Agency's response to the global COVID-19 pandemic.

ENISA was called upon to support during these testing times by making recommendations to the critical infrastructure industry, supporting the EU Tracing Apps Toolbox, providing cybersecurity advice to SMEs and guidance to the healthcare sector against the increase of phishing campaigns and ransomware attacks. ENISA raised awareness of cybersecurity risks and recommendations on a variety of topics such as working remotely, shopping online and e-health; and with the support of its partners issued weekly situation reports of on-going cyber incidents. In addition, the CSIRTs Network was placed on high alert requiring increased support by the Agency. Through protecting critical infrastructure, public outreach and creating a common situational awareness, ENISA played a key role in preventing malicious cyber actors from taking advantage of the health pandemic and turning it into a large scale cyber pandemic.

Reorganisation

ENISA embarked on a journey to reorganise the organisation in light of the new strategy and the new mandate of the Agency under the Cybersecurity Act and on the basis of the problem analysis endorsed by its Management Board. The Management Board set out principles for preparing, deciding and implementing all the steps necessary for reorganising the Agency and establishing the new internal structures. The following principles guided the Executive Director in preparing and implementing the new organisation:

Purpose: the new organisation (including proposals regarding the Agency's internal structures) will be implementing the Agency's mandate, tasks and functions as outlined by Union law and the values and objectives as set by its Strategy.

Proportionality: the new organisation will ensure the Agency's continuous functioning, will aim to limit disruption to the Agency fulfilling its mandate, and will not go beyond what is necessary to address agreed problems and aims.

Synergies: the new organisation will aim to strengthen internal synergies and enhance cooperation with the Agency's strategic European partners as defined by the CSA.

Efficiency: the new organisation will aim to enhance the organisation's performance, the impact of ENISA and budgetary efficiency and sound budgetary management.

Agility: the new organisation should facilitate the Agency's potential flexibility in terms of its human and budgetary resources, as well as take into account the ever growing and changing nature of the cybersecurity ecosystem.

Transparency: all steps toward modifying or reforming the Agency's internal structure and the steps leading to the implementation of the reorganisation will be executed in an inclusive manner, discussed and consulted with the Agency's Executive and Management Board and staff.

Predictability: the new organisation will be implemented in a stage-by-stage approach allowing staff and partners to anticipate and adjust to changes.

Competences: development of staff will be based on their preferences, expertise, competences and talent, whilst taking due account of their current functions and career goals and the needs of the Agency.

Openness: new functions and posts within the Agency will be filled through open competitions or internal mobility organised on the basis of open calls and through a transparent assessment of merits and talent.

The Agency took different actions to initiate the changes needed. The first step consisted in identifying the problems of the current structure and look at how employees function together as a team and how they are equipped and empowered to deliver against the work programme. ENISA organised a 2-day workshop for staff to engage in the discussions.

The main problems identified were a) the imbalance between the talent, functions and aims of the two then departments, b) the limited synergies between both the departments and within the departments; c) weaknesses in internal controls framework. This problem analysis was endorsed by the Management Board.

In addition, ENISA created a competency framework to measure the future state of competencies needed for the new organisation. These competencies were grouped into four categories; Corporate DNA, Next Generation, Managerial and Functional competencies. The competency framework provided a profile based on specific sets of competencies and set levels of proficiency levels for each competency.

Interviews were arranged with a third party to assess the staff motivation and to give staff an opportunity to express their interest in transferring to a new job profile within the new organisation.

The Management Board established ENISA's new internal structure in June. The new organisational architecture introduced a number of structural elements to strengthen the Agency's ability to build internal and external synergies by introducing cross structural teams to lead the work on horizontal tasks (CSA Art 9-12) which require contributions from all vertical units and could not be efficiently managed within a unit. In addition, the role of the Management Team is to coordinate the activities of the constituent parts of the Agency in order to ensure efficient and effective implementation of the Work Programme (Art 20d) and sound budgetary management.

Four operational units were created:

- **the Policy Development and Implementation Unit** ensuring the performance of the tasks of the Agency as set out in Art. 5 of the CSA;
- **the Capacity Building Unit** ensuring the performance of the tasks of the Agency as set out in Art. 6 and Art 7(5) of the CSA;
- **the Operational Cooperation Unit** ensuring the performance of the tasks of the Agency as set out in Art. 7 (except for Art 7(5)) of the CSA;
- **the Market, Certification and Standardization unit** ensuring the performance of the tasks of the Agency as set out in Art. 8 and 22 and under Title III of the CSA.

Two internal new structural units were created **(Corporate Support Service and Executive Director's Office)** to ensure sound budgetary management and effective and efficient management of all its other resources, as well as compliance with the Agency's work and the regulatory and programming framework. The culmination of these

changes saw the ratio of administrative / neutral staff (40%) to operational staff (60%) that had historically been high at the Agency shift towards a greater balance in favour of operational activities.

A process was set in place to guide the transfer of staff into the new structure and to ensure a smooth and effective transition to the new organisation. This process included the creation of a Joint Committee, an advisory body to facilitate the decision-making of the Appointing Authority according to the principles outlined in Annex II Art 2 and 3 of the Staff Regulations.

Using an established methodology, the Joint Committee's final final assessment concluded whether a staff member's current tasks and/or job description matched to a great extent (e.g. at least 75% to the tasks of a new structural unit), then an offer letter was proposed for an automatic transfer to the new unit. Dedicated consultations were held with any staff member who refused the automatic transfer offer.

All staff members were transferred to the new structure by 01.01.2021 via individual 'transfer decisions' by the Appointing Authority acting solely in the interest of the service according to Article 7 of the Staff Regulations. All transfer decisions were prepared in a transparent and open manner towards staff members, taking into account their current functions and tasks, motivation, experiences and competences.

For managerial positions, the managers of units which managed at least 75% of the operational tasks (as outlined in Art 5-12 of Title I chapter II in the CSA) of a new structural unit, were offered a transfer to a new managerial position through internal mobility. Three managerial positions were transferred via internal mobility via this process. All other new managerial posts were fulfilled via open competitions.

In order to inform all staff on the various processes of the competency framework and staff transfers, since 15 April a weekly Questions and Answers session was organised by the Executive Director. Every week, a different aspect of the reorganisation would be discussed and staff could request information and provide feedback and input. A staff survey in June 2020 found that 89% of staff indicated that the amount of information received was just about right and that 94% of staff indicated that the timing of information was just about right.

The new organisational structure came into effect as from 1st January 2021.

Recruitment

In the beginning of 2020 the Agency embarked on a large-scale recruitment exercise to create a sufficiently diverse and broad reserve shortlist of 75 candidates with more transversal competences and skills. This reserve list was intended to be used to recruit staff into grades AD6–AD8 and functions and thus fill the gaps in the current establishment plan, as well as serve as a pool of candidates for the establishment plan of 2021 and 2022 if necessary, in line with the needs of the new organization. The TA call, which was supported by a widespread promotion campaign, attracted 1 235 candidates (who submitted more than 1 600 applications) across all Member States). This resulted in a reserve shortlist of 69 candidates. In addition, this selection came along with another call for contract agents , which attracted over 600 applications and resulted in a reserve shortlist of 15 candidates[33].

3 BUDGETARY AND FINANCIAL MANAGEMENT

a) FINANCIAL MANAGEMENT

The Agency operated with the budget of EUR 21.6 million equivalent to a 28 % increase in 2020 compared to the 2019 budget (EUR 16.9 million). The amending budget 1/2020 wasadopted by the Management Board by written procedure on 28 August 2020. The purpose of this amending budget was to re-direct funding made available through the cancellation of projects and forecasted expenditures due to the COVID-19 pandemic to finance new projects and activities up to an amount of EUR 2.5 million, from which EUR 1.6 million are under operational activities.

ENISA concluded a total of 35 public procurement procedures (two of which have been jointly done with Cedefop)

1. 18 were done through re-opening of competition under framework contract (51 %);
2. 10 were done through negotiated procedure for middle and low-value contracts (29 %); and
3. 7 were done through open procedure (20 %)

No interest was paid in 2020 to suppliers for late payments.

33 The establishment plan projected a staff increase over the period from 111 staff members in 2020 to 121 in 2023.

The table below shows ENISA's budget implementation targets and achievements in 2020, which remained high under restrictive circumstances imposed by COVID-19.

Area	Objective	Target 2020	Level of completion 2020
Budget implementation (appropriations committed through the year)	Efficiency and sound financial management	99 %	97.35 %
Payments against appropriations of the year (C1 funds)	Efficiency and sound financial management	85 %	68.62 %
Payments against appropriations carried over from previous year (C8 funds)	Efficiency and sound financial management	95 %	95.86 %

b) BUDGET EXECUTION OF EU SUBSIDY (C1 FUNDS OF CURRENT YEAR 2020)

During 2020, ENISA committed an amount of EUR 20 588 320 representing 97.35 % of the total budget for the year. Payments made during the year amounted to EUR 14 513 329 representing 68.62 % of the total budget.

The budgetary execution was high despite the restrictive circumstances imposed by COVID-19. As compared to 2019, there was a slight increase in commitment execution – 97.35 % in 2020 as compared to 96.80 % in 2019, and a slight decrease in payment execution – 68.62 % as compared to 70.12 % in 2019. The target of 95 % for commitment rate set by the Commission (DG Budget) was thus reached.

The payment rate was lower than expected but can be explained by the new challenges and priorities stemming from the COVID-19 pandemic and by the renewal of annual IT software licenses. Approved mid-year, the related commitments were therefore only concluded late in the year. Moreover, ENISA's budget increased by almost a third from 2019 to 2020 which required operational and administrative adjustments to absorb the substantial difference.

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

Table below summarises the execution of the budget in 2020.

2020 budget (C1)						
2020 area of budget allocation	**Appropriation amount (in EUR) (1)**	**Commitment amount (in EUR) (2)**	**Percentage committed (2)/(1)**	**Payment amount (in EUR) (3)**	**Percentage paid (3)/(1)**	**Amount carried forward to 2021 (in EUR)**
Title I (*)	10 753 483	10 488 532	97.54 %	9 278 773	86.29 %	1 209 759
Title II (**)	3 538 031	3 426 650	96.85 %	1 663 918	47.03 %	1 762 732
Title III	6 857 606	6 673 138	97.31 %	3 570 638	52.07 %	3 102 500
TOTAL	**21 149 120**	**20 588 320**	**97.35 %**	**14 513 329**	**68.62 %**	**6 074 991**

(*) Title I does not include revenue of EUR 97 920 from eu-LISA for provision of services
(**) Title II does not include the subsidy of up to EUR 640 000 from Hellenic Authorities for the rent of the building

Further details on budget execution are provided in Annex II.

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 of up to a maximum of 10 % of the appropriations for the financial year allocated to the title from which the transfer is made. Transfers within the same title are also permitted, without limit.

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

The Agency made three transfers in the reported year by the decision of the Executive Director (hereinafter – ED) on the initial budget, and four transfers by the decision of the Executive Director on the amended budget (in comparison, the Executive Director made four transfers on the initial budget and six transfers on the amended budget in 2019). The three transfers on the initial budget included only transfers within the title. The four transfers on the amended budget included two transfers within title and two transfers between titles. Because of COVID-19 restrictions funds were mainly redirected from salaries, meetings, conferences, other events and missions to support ICT projects, translations and interim services.

The table below summarises the changes to the budget in 2020.

2020 budget (C1) (in EUR)				
2020 area of budget allocation	**Initial budget**	**Amended budget**	**Transfers approved by the executive director**	**Final budget**
Title I	12 041 486	11 105 414 (*)	– 351 931	10 753 483 (*)
Title II (**)	2 346 000	2 714 724	823 306	3 538 031
Title III	6 761 633	7 328 981	– 471 375	6 857 606
TOTAL	**21 149 120**	**21 149 120**	**0**	**21 149 120**

(*) Title I does not include revenue of EUR 97 920 from eu-LISA for provision of services
(**) Title II does not include the subsidy of up to EUR 640 000 from Hellenic 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 2019 were carried forward to 2020 (C8 appropriations).

As compared to 2019, there was a 1 % increase in commitment execution (96.01 % in 2020 compared to 94.93 % in 2019) as well as a 1 % increase in payment execution (95.86 % in 2020 compared to 94.93 % in 2019) showing an improvement in financial management in this regard.

The following table shows the commitment execution and payment execution in 2020.

2020 budget (C8)				
2020 area of budget allocation	**Appropriations carried forward from 2019 to 2020 (in EUR)**	**Payment amount (IN EUR)**	**Percentage paid**	**Amount cancelled (in EUR)**
Title I	357 936	321 924	89.94 %	36 012
Title II	2 884 042	2 836 694	98.36 %	47 348
Title III	1 105 354	1 008 690	91.25 %	96 664
TOTAL	**4 347 332**	**4 167 309**	**95.86 %**	**180 023**

4 DELEGATION AND SUB DELEGATION

In the very beginning of 2020, the Executive Director reviewed the delegation of authorising authority powers and on 12 February 2020 adopted a new decision on a framework of the financial delegation of the authorising officer and of a budgetary management committee to ensure a sound financial execution of the Agency's budget.

This decision confirmed the overarching principle of financial delegations applicable to heads of department and heads of unit with a respective limit of EUR 500 000 and EUR 100 000 per transaction. ENISA didn't implement any further sub-delegations in 2020.

Controls on these delegation rights are done through a periodical revision of the rights granted in the main financial system, 'ABAC [34]'. ENISA set time limits to indicate the termination of the respective financial delegations.

In October 2020, the ECA identified a weakness in the delegation of financial rights whereas financial transactions were authorised without having proper financial delegation rights over the period prior to 12 February 2020.

The Agency took all the necessary steps to address this weakness properly: the Executive Director set up an independent task force to look into these transactions and concluded they were free of conflict of interest and did not jeopardise the Agency's financial interests. Moreover, a revision of the financial delegations, the related financial circuit and relevant internal controls took place in the last quarter of 2020 (see also section 2.7.2 European Court of Auditors).

5 HUMAN RESOURCES MANAGEMENT

ENISA HR took decisive targeted actions prior to the lockdown imposed by the Greek government, further to the COVID-19 outbreak, e.g. continuing to ensure high health and safety measures in place for its staff (ample supplies of disinfectants, disposable gloves, masks, basic medicine, and hand disinfectant).

Staff guidelines were drawn up and teleworking was authorised in lieu of working in the office for all staff as of March 11th 2020. Missions and public events were halted.

Since March 2020, 23% of staff teleworked outside the place of assignment for longer than 6 months. 6% of staff teleworked outside the place of assignment for less than 6 months. The Agency implemented this duty of care measure in order to allow staff members to take precautious measures based of numbers of available intensive care units per member state.

The management of the Agency processed a phased Return to the Office plan based on: the perception of the threat to the Agency staff, the assessment of risk by management, and the mitigation measures intended to keep staff from aggregating in the office. Staff safety was and still remains the guiding principle regarding the implementation of this plan.

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. The Agency also authorised reimbursement of all COVID-19 related tests (PCR, anti-gen, anti-body) for work-related reasons and for travel back to the place of employment. Human Resources also revised the core working hours, so as to provide for greater flexibility for colleagues working from various locations across Europe. A total of 5 Administrative Notices were published, as well as 17 intranet announcements, in addition to the bi-weekly updates from the Management Team meetings.

The Human Resources unit supported the operational and administrative goals of the agency in terms of staff acquisition and development. The planning of, execution of and accounting for the long- and short-term needs of the agency form the majority of the unit's regular activities. In this regard, the Human Resources unit carries out its tasks in relation to the management of ENISA's statutory staff along with its external staff (e.g. trainees) in line with the staff regulations / conditions of employment of other servants of the European Union, as appropriate.

In 2020, ENISA carried out tasks to support the deployment of the Commission's information management system for human resources ('Sysper'). Compliance remained a priority for the Human Resources 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.

34 ABAC (Accrual Based Accounting): the acronym of the European Commission's project to switch from cash-based to accrual accounting, and of the new accounting system introduced. https://ec.europa.eu/budget/library/biblio/publications/modern_accounts/modernising_EU_accounts_en.pdf

As previously mentioned, theAgency embarked on a large-scale call for expression of interest for temporary agents (TA) and contract agents (CA) following an adapted approach, to replenish its reserve lists with suitable candidates at various levels. This resulted in a reserve shortlist of 69 candidates for TA posts and for CA posts 15 in reserve shortlist, giving ample choice to the Appointing Authority.

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

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

6 STRATEGY FOR EFFICIENCY GAINS

ENISA is committed to continuously implementing measures to obtain efficiency gains in all activities. For this purpose, the agency launched coordinated initiatives notably with other EU institutions and bodies, namely CEDEFOP to create synergies and seek to rationalise its internal processes to improve its overall efficiency and to follow the benchmark best practices in the EU agencies. Such initiatives resulted in signing a contract with Cedefop.

In 2020 ENISA also engaged with EU LISA to seek such synergies as well. The process was concluded in early 2021.

ENISA also supported BEREC Office by providing back up services for storing BEREC's Office electronically data as per SLA agreement.

Similarly, in response to tasks provided for in Article 7 of the CSA, ENISA initiated the establishment of a structured dialogue with CERT EU (Commission services). The process was endorsed by the The Management Board of ENISA endorsed the process in a emorandum of Understanding.

In addition, further efficiency gains are planned for the future, based on the deployment and enhancing of IT tools and internal procedures (such as Sysper, the Missions Integrated Processing System, e-recruitment, etc.).

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

7.1 Internal Audit Service (IAS)

The IAS issued an audit report on stakeholder's involvement in the production of deliverables in June 2018. Five audit recommendations, two assessed as very important and three as important, were issued during this audit. ENISA set up a specific task force to ensure the adequate implementation of the action plan agreed with the IAS.

As of end of 2020, four recommendations were considered closed by the IAS. As for the pending important recommendation, the few remaining actions were carried out by the Agency in 2020 by strengthening its reporting process, notably on the information to be provided in the Annual Activity Report. The supporting documents were provided to the IAS to review its correct implementation in early 2021. Following its review, the IAS considered in May 2021 the controls put in place by the Agency as sufficient to close this recommendation.

Altogether, all five recommendations issued during the 2018 audit are now fully addressed by ENISA.

The IAS audit report on human resources management and ethics was issued in September 2019. Three very important and four important and recommendations were issued in this audit. An action plan was devised and agreed with the IAS. In the second half of 2020, one very important recommendation was considered as implemented and was closed by the IAS. Corrective actions were consequently implemented by ENISA for the

remaining six recommendations in 2020 and were submitted for IAS review in early 2021. Following its review, the IAS considered in May 2021 the sufficient the controls put in place by the Agency to further close another three recommendations.

Altogether, four audit recommendations were closed by the IAS while 3 recommendations remain open as further actions are required to be implemented by ENISA in 2021.

7.2 European Court of Auditors (ECA)

In October 2020, the ECA identified a weakness in the delegation financial rights whereas financial transactions had been authorised without proper financial delegation rights in place. The Agency welcomed this finding and a corrective action plan was immediately devised to address this legal issue and to reinforce relevant internal controls. A task force was constituted to evaluate whether these transactions jeopardised the Agency's financial interests. It is important to note that these financial transactions did not impact the reliability of the financial records: these transactions would have been processed by the Agency anyway as all of these were completed in the pursuance of the Agency's objectives and for its official use.

The corrective action plan also triggered an immediate revision of the financial delegation rights as well as of the financial circuit which took place in the last quarter of 2020 for effective implementation as from 1st January 2021. This also follows the recommendation issued by the task force in its January 2020 report on assessment on the Agency's organisational structure and internal control systems (see also Part III – Assessment of the effectiveness of the internal control systems).

The ECA issued in 2020 its report on the 2019 annual accounts of the Agency[35]. In their audit opinion, all revenue and payments underlying the accounts for the year ended 2019 are legal and regular in all material aspects. Moreover, 'the accounts of the Agency for the year ended 31 December 2019 present fairly, in all material respects, the financial position of the Agency at 31 December 2019, the results of its operations, its cash flows, and the changes in net assets for the year then ended'.

The ECA nevertheless identified non-critical weaknesses on the Agency's public procurement procedures[36]. In particular, selection and award criteria in the procurement notice could be improved and respect of publishing within the deadlines should be better monitored.

Acknowledging and welcoming these audit observations, the Agency immediately addressed these concerns by implementing corrective action through a reconsideration of its internal processes.

The ECA also observed an increase to the use of temporary workers and commented on specific legal provisions governing the use of interim staff[37]. As ENISA's activities are growing, the Agency does rely on interim staff to perform some of its tasks but only in case of unfilled vacant posts and of heavy workloads.

To mitigate risks linked to vacant posts, ENISA re-defined its recruitment strategy. The Agency indeed launched in 2020 two combined vacancy notices for Temporary Agents and for Contract Agents respectively likely to yield a large number of new recruits expected to reach the staff employment levels required under the Cybersecurity Act. ENISA therefore should see It the number of temporary workers significantly drop in.

To ensure that specific legal provisions governing the use of interim staff were complied with, the Agency updated the basic terms of employment in order to justify the category under which the interim worker is hired by among other adding a job description to the contract. ENISA also revised the extra-legal benefits granted to staff and the categories of staff who can benefit from them. This allowed the Agency to ensure that interim workers enjoyed the same working conditions as statutory staff.

In response to the Court recommendations and by following the above mentioned approach, the Agency is likely to remain a fairly attractive place to work, while mitigating any legal concerns of its interim agents and duly motivating its decision to dispense its appropriations accordingly.

All ECA's observations stemming from the previous years were duly addressed except for the adoption

35 https://www.enisa.europa.eu/about-enisa/accounting-finance/files/enisa-2019-annual-accounts-2013-eca-report

36 See paragraph 17 to 19 of ECA's Report on the annual accounts of the European Union Agency for Cybersecurity (ENISA) for the financial year 2019 – link to the report is disclosed in the footnote 31

37 See paragraph 20 to 21 of ECA's Report on the annual accounts of the European Union Agency for Cybersecurity (ENISA) for the financial year 2019 – link to the report is disclosed in the footnote 31

by the Agency of a policy on sensitive functions tobe made in 2021[38].

7.3 Ex-post evaluation results

ENISA performed *ex post* controls, as part of the internal control framework, for the 2019 financial year. A total of 266 financial transactions were scrutinised, representing 11.26 % of all the agency's financial transactions and 66.66 % of the agency's 2019 budget. As a result, recommendations were issued as follows.

Five recommendations were made pertaining to observations on administrative procedures for which corrective measures had already been implemented.

One recommendation was related to financial management, revealing a weakness in forecasting expenditures for non-fixed costs.

The final recommendation related to the late payment of the rent subsidy by the Hellenic authorities, as it delayed the payment from the agency to the property owner.

The agency recorded 31 exceptions in the reporting year: 28 of these were below the relevant materiality level (less than EUR 15 000). Two exceptions were linked to a posteriori commitments and the one remaining exception linked to a consumption that exceeded the available C8 funds. Reminders and additional information/training were delivered to the respective project managers and authorising officers by delegation on the applicable financial rules and ENISA will look into the accountability procedure for future events. In relation to the above, controls for the 2021 carry-forward will be improved.

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

One recommendation issued by OLAF was resolved in 2020. submitted to ENISA a report in December with recommendations to be addressed in the course of 2021.

38 See Annex of ECA's Report on the annual accounts of the European Union Agency for Cybersecurity (ENISA) for the financial year 2019 – link to the report is disclosed in the footnote 31

9 FOLLOW-UP OF OBSERVATIONS FROM THE DISCHARGE AUTHORITY

In relation to the 2019 discharge[39], 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 2019 financial year. The closure of the agency's accounts for the 2019 financial year was also approved by the discharge authority.

10 ENVIRONMENTAL MANAGEMENT

The normal activities of the Agency were materially affected by the fallout related to COVID-19 for the majority of the 2020 year, ENISA continued to implement its established greening measures such as; recycling of office materials, reduction in electricity usage for lighting and heating/cooling. ENISA also actively implements the EU GPP (green public procurement) award criteria in its tendering documentation, with relevant procedures launched in 2020 such as; Provision of Stationery and printing supplies; Laptop Computers and Docking Stations; and Production and supply of branded promotional material.

ENISA continued to implement its established greening measures such as; recycling of office materials, reduction in electricity usage for lighting and heating/cooling.

The restrictions imposed from March and for the best part of 2020, such as imposed teleworking and heavily restricted travel for work related missions, led to a number of benefits for the environment. With the majority of staff teleworking from home, the carbon footprint was significantly reduced per staff member as they did not drive their vehicles to the workplace; they replaced EU wide mission travel for video conference meetings instead; paper based printing at the office

39 https://www.europarl.europa.eu/doceo/document/A-9-2021-0085_EN.html

was substantially reduced, and heating/cooling/lighting of office space was largely not required.

Whilst it could be argued that the magnitude of these gains are not sustainable once life goes back to normal and staff return to their offices, there is a strong indication, backed by management, that the 'new normal' for staff working conditions will include a much higher level of voluntary teleworking, and an ongoing significant reduction in mission related travel. Furthermore, a carbon neutrality objective was introduced in the Single Programming document 2022-2024 targeting full implementation by 2030.

It is important to note that in consultation with ENISA, Hellenic Authorities ENISA found new headquarters building for ENISA in the reporting year. This will provide further impetus for implementation of measures which could not be undertaken in the current building due to the shared arrangement.

11 ASSESSMENT BY MANAGEMENT

2020 was a challenging year for ENISA for two reasons: the COVID-19 pandemic and fundamental changes in modus operandi.

Despite such circumstances, the report demonstrates that ENISA delivered as expected with the flexibility needed to reshuffle priorities in relation to its work programme.

Essential changes were implemented to reshape the organisational structure of ENISA from top to bottom and the way the Agency operates. In the transition actions deemed necessary were taken in order to increase the efficiency of the Agency including fulfilling its operational mandate, and address urgent shortcomings and needs.

Changes included the revision of the role of the Management Team. The practice of inceptions for every individual project undertaken to implement the work programme was introduced at the beginning of the year, to ensure better coordination within the Agency and guarantee more targeted and effective resource management.

The Agency also implemented a new system to validate the work programme deliverables piloted in 2020, which consisted in consulting the Advisory Group (AG), the National Liaison Officers network (NLO) and other statutory bodies.

Another essential development was the process engaged in view of the reorganisation of the structure of the Agency. This reorganisation also applied to the way ENISA's internal controls are now set up and addressed, and in relation to the work programme: the setting of key performance indicators and the implementation of new processes.

In addition, the Agency initiated the setting-up of the structured cooperation with CERT-EU, a statutory obligation foreseen in the CSA.

Besides, ENISA also launched a process to allow the handling of a higher level of the EU Classified Information and engaged in the administrative processes required for the set-up of the local office in Brussels, Belgium.

PART II (B)
EXTERNAL EVALUATIONS

ENISA contracted the services of Deloitte Consulting and Advisory to perform an ex-post evaluation of the activities of the Agency implementing the work programme of 2019. This work resulted in a final report and a case study on Procurement Guidelines for Cybersecurity in Hospitals. Deloitte aggregated the key findings of the report aggregated under the following criteria; effectiveness, efficiency, coherence and coordination, relevance, and EU added value). The contractor submitted an action plan composed of concrete recommendations to adjust and improve ENISA's activities. Recommendations included to redefine key performance indicators (KPIs), to balance and tailor the Agency's activities and outputs, and finally to reinforce the position of the Agency within the cybersecurity ecosystem.

PART III

ASSESSMENT OF THE EFFECTIVENESS OF THE INTERNAL CONTROL SYSTEMS

1 EFFECTIVENESS OF INTERNAL CONTROL SYSTEMS

ENISA adopted the revised internal control framework end of 2019. The revised framework follows the framework of the Committee of Sponsoring Organizations[40] of the Treadway Commission as adopted by the European Commission, and comprises five internal control components and 17 internal control principles.

The internal control system is designed to provide reasonable assurance of achieving effectiveness, efficiency and economy of operations, reliability of reporting, safeguarding of assets and information, and prevention, detection, correction and follow-up of fraud and irregularities.

In November 2019, the Executive Director created a task force to assess the Agency's organisational structure and internal control systems. A report was submitted by the task force in January 2020. One of the findings was that the previous Agency's organisation was not adequate to independently implement the principles of the internal control framework. This led to the re-organisation of the internal control function and underlying processes.

40 COSO

In order to assess all the components and principles of the Internal Control Framework, a set of 57 KPIs was designed and annexed to the MB Decision MB/2019/12[41]. All these KPIs are assessed individually using relevant supporting documents as evidence of the assessment.

1.1 Assessment of control environment component

The control environment component consists in five principles.

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

The Management strongly encourages all staff to follow annual mandatory trainings related to integrity and ethics (which is obligatory for all management team members).

To that purpose, a training on "Ethics and Integrity" was given by the European Commission to ENISA's staff during 2020. Moreover, different types of material are at disposal of the staff such as the training content and the most updated IDOC reports[42].

41 https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/MB%20Decision%202019-12%20on%20internal%20controls%20framework.pdf

42 Commission's Investigation and Disciplinary Office

Principle 2: ENISA's Management exercises oversight responsibility of 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 declaration of assurance covering their areas.

As a result of the assessment on the Agency's organisational structure and internal control systems by the task force initiated by the Executive Director, a revision of the internal controls function took place in 2020 to ensure its independency and to increase its effectiveness.

Moreover,ENISA fully re-assessed the financial circuit and financial delegation in 2020. The ECA preliminary finding (section 2.7.2.) further confirmed the need to review the financial delegations. ENISA fully implemented the revised financial circuit and financial delegation as from 1st January 2021. In particular, the financial processes were reviewed as well as the delegations and ceilings of each financial actor.

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

To ensure the comprehensive structure and clear reporting lines are communicated to all staff, the updated organisational chart is published every month on the ENISA intranet.

The task force set up by the Executive Director in November 2019 assessed ENISA's organisational structure, internal processes and internal controls systems. In this report issued in January 2020, recommendations included:

1. to fit ENISA's organisational structure to its purposes by better reflecting the new challenges arising from the Cybersecurity Act; and

2. to review the internal control function.

As a result, the Agency:

- reviewed the overall framework of financial delegation in February 2020, limiting the number of authorised officers and created a separate independent oversight body (Budget Management Committee) to monitor, among other tasks, the exercise of sub-delegated powers, with a more independent setup established in 2021 after reorganisation;
- started to design a new organisational structure (effective as of 01.01.2021), where the tasks of budgetary execution and internal controls (including monitoring) are structurally and functionally firm and well segregated, with a new 'compliance and control' section within the Executive Director's Office with 4 FTEs, separated from budgetary monitoring and execution (with the Finance and Procurement Section within the Corporate Support Service);

To ensure that the Agency has a comprehensive structure and clear reporting lines and that this structure is communicated to all staff, the updated organisational chart is published every month on ENISA intranet.

- in March 2020, further decisions restricted the financial impact of authorised expenditures to the Head of Resources Department and in November 2020 suspended the delegation of financial authority initially given to the Head of Resources Department, since the post was disbanded within the new organisation of the Agency;

As from the 1st January 2021, a single executive director decision covers all delegations of financial transactions streamlining the profiles and enhancing efficiency and effectiveness. Importantly, the new decision also includes a sunset clause to end all sub-delegated authority automatically 3 months after the change of the person of the Executive Director, unless the new Executive Director explicitly confirms the delegations in place.

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

The Agency made an enormous effort in the reporting year to widely disseminateENISA's vacancies using different channels. Vacancies were advertised internally through email and Intranet publications and externally through ENISA website, EPSO and social media. The extensive communication plan around these publications partly results from the new organisational structure and efforts done in the strategy on resources needed based on the priorities of the objectives of the Agency.

The agency managed to significantly reduce t staff turnover in 2020. The ratio was only of 2 percent which shows improvement in retaining staff members in the Agency

All staff performed their Career Development Report. The internal deadlines were respected and the exercise was successful.

In order to develop and retain competent individuals, a Learning and Developing policy is adopted every year. This policy is detailed and includes the training plan for the agency wide trainings, as well as the budgetary resources available for individual trainings.

Internal mobility was exercised during the reorganisation process in 2020.

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

The Agency defines clear roles and responsibilities for its staff members as well as sets annual objectives through annual appraisal exercise. Each of them are entrusted and accountable for the performance of the internal control at their level and based on their functions.

In order to pursue its objectives and to follow up on the actions taken, a mid-term review is performed by the Agency in order to evaluate the progress of the objectives (and their budgetary implementation). In 2020 this exercise led to amendments of the work programme 2020 and of the associated budget. Such exercise ensures that corrective actions can be taken in order to achieve the overall objectives.

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

1.2 Assessment of Risk Assessment component

The Risk Assessment component consists in 4 principles.

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

ENISA embarked on defining a new strategy with objectives allowing for the implementation of the mandate of the Cybersecurity Act and its mission statement..

The objectives of the work programme 2020 were based on the previous organisational structure and on the previous strategy. Also, the Agency established a template to incept the implementation of outputs. This template also includes a risk assessment.

ENISA also prepared an amending work programme to suggest several changes to the Management Board and the amended Single Programming Document (SPD) was approved by the Management Board on the 16th June 2020 by written procedure (MB/2020/7).

ENISA uses the objectives as basis for allocating resources to achieve policy, operational and financial performance goals. The Agency submitted its Amending Budget to the Management Board adjusting its financial resources allocation in response to the pandemic. The Management Board adopter the Agency amending budget on the 28 August 2020 (MB/2020/18).

Principle 7: ENISA identifies risks to the achievement of its objectives across the organisation and analyses risk 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. Both management and staff are involved through a process at the level of the Management team. Every output of the work programme requires an inception and a finalisation. The template of this process require a risk assessment for each output.

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.

Nevertheless, Risk Management in 2020 was not centralised and didn't have a holistic approach yet. This created a weakness in the management of risks. In order to minimise this issue, the Agency created a Compliance and Control Sector in the course of the reorganisation to centralise all risks of the Agency in order to address them correctly and efficiently.

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

ENISA renewed its anti-fraud strategy and action plan, both adopted by the Management Board in February.

Principle 9: ENISA identifies and analyses significant change

The risk identification process considers changes in the internal and external environment. The mitigation actions engaged as early as March when the COVID-19 crisis emerged are clear examples of this process. These measures included teleworking, access to premises with prior approval. Response to this As a result, a review of annual work programme and associated budget took place. Coordination between departments could have been organised in a smoother way to allow earlier approval of the amending budget by the Management Board. This was rectified by introducing new budgetary monitoring and reporting framework – establishment of internal Budget Management Committee and including specific KPI's in relation to budget implementation for middle managers.

Besides, the Executive Director established several task forces to initiate the changes needed by the Agency. Different mitigation measures were taken such as the change of the organisational structure to adapt it to the objectives of the CSA; the analysis of internal synergies to improve ; the revision of the financial circuits and actors.

The Agency will be relocated to a new headquarter mid-2021 is expected to stir up a significant change. ENISA launched the relocation process in the reporting year. This is expected to allow for a smooth transition from the old building to the new one. The Executive Director created a dedicated task force and relocation team to support this change.

1.3 Assessment of control activities component

The control activities component consists in 3 principles.

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

Results of control and performance indicators are monitored as to ensure achieving related objectives. These controls take place twice a year (mid-term review and end of year report).

In order to ensure a high level of control, the Agency applies *ex ante* verification on 100 % of its financial transactions. In order to complete this control, an *ex post* control verification is performed every year.

The Business Continuity Plan is being revised and will be finalised by the end of 2021.

There was no map of critical and sensitive posts established in 2020. Such mapping is expected to be carried out in the course of 2021.

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

ENISA applies appropriate controls to ensure the security of the main IT systems which the Agency is the system owner of. It is done in accordance with the IT security governance principles, in particular as regards data protection, professional secrecy, availability, confidentiality and integrity.

A dedicated staff member acts as Information security officer. Regular vulnerability assessments and penetrations tests were performed. ENISA provided to all staff its the security awareness policy and an improved IT Security training. Non-compliances with policy were identified and addressed.

In order to reinforce these controls, an IT risk assessment was conducted in 2020. The new IT Management Committee set up in Q4 of 2020 is currently revising the IT strategy and the IT security policy. The Agency keeps a complete recording of security breaches and addresses them properly.

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

Internal control activities were deployed thanks to the revision of objectives and deliverables by Head of Units and Department, to the measurement of results against the forecasted expectations; and the validation of deliverables by expert communities, including the reorganisation process. The Agency performed an external ex-post evaluation of its activities based on effectiveness; efficiency; coherence; coordination and added value of its activities.

The Agency performed an external ex post evaluation of its activities based on effectiveness; efficiency; coherence; coordination and added value of its activities.

The Agency regularly updates its Register of Exceptions as needed. The contents of the 2020 Register of exceptions are detailed in paragraph 2.7.3 on ex-post controls and evaluations.

1.4 Assessment of information and communication component

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

ENISA has the information required to support the functioning of the internal control system and the achievement of its objectives.

The Agency uses a centralised external communication tool for incoming/outgoing documents. Official documents (outgoing and incoming) are registered, numbered and archived.

The fact that Agency can retrieve 100 % of the documents requested by the IAS/ECA is an excellent indicator. All documents are archived on ENISA's intranet; paperless and requests for financial reports can be processed on the spot using Business Object and ABAC.

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

ENISA and the management communicate internally about their objectives, challenges, actions taken and results achieved. Internal communication is performed using different channels. Communication to staff is enabled through Staff Meetings; Unit meetings, Minutes of Management Team meetings distributed the same day to all staff via email and published on the Intranet.

The Agency uses different tools for internal communications. Most common tools are the ENISA's intranet; email; Skype for Business and WebEx. The Agency carried out all internal communications remotely and through online meetings as of mid March 2020.

Mid-term reviews of the budget are also used as an opportunity to communicate on objectives achieved and ongoing projects or on changes needed as well as the strategy to be followed to deliver the Agency's outputs.

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

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

The Agency communicates on its Internal Controls through the Annual Activity Report and regularly at Management level.

Also, regular reporting on IAS and ECA recommendations and their follow up is provided to the Executive Board and through the discharge procedure.

1.5 Assessment of monitoring activities component

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 designed to identify internal control deficiencies, to register and assess the results of controls, and identify control deviations and exceptions.

The Agency follows up, in a timely manner, the recommendations of auditors as well as risks identified in the *ex-ante*, *ex post* controls and evaluations. The status of these recommendations is communicated twice (mid-term review and Annual Activity Report).

ENISA did not perform any change in relation to these processes in the reporting year.

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

Internal control deficiencies identified 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 closely these deadlines as well as the result of the mitigation measures proposed.

2 CONCLUSIONS OF ASSESSMENT OF INTERNAL CONTROL SYSTEMS

ENISA carried out an internal controls assessment exercise late 2019 which concluded that the structures supporting internal controls and compliance appear to be spread out and hence weak.

The report for a dedicated task force that carried Issued by the dedicated task force who carried out such assessment, the report suggests the implementation of an independent quality control system to reinforce the monitoring of performance assessment. The task force also advised to restructure horizontal tasks such as internal controls, ex ante verification, ISO, budget monitoring and quality controls.

Those issues were addressed through the reorganisation and overhaul of internal processes undertaken in 2020 and in force as of 01.01.2021. The improvements will be assessed at 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,

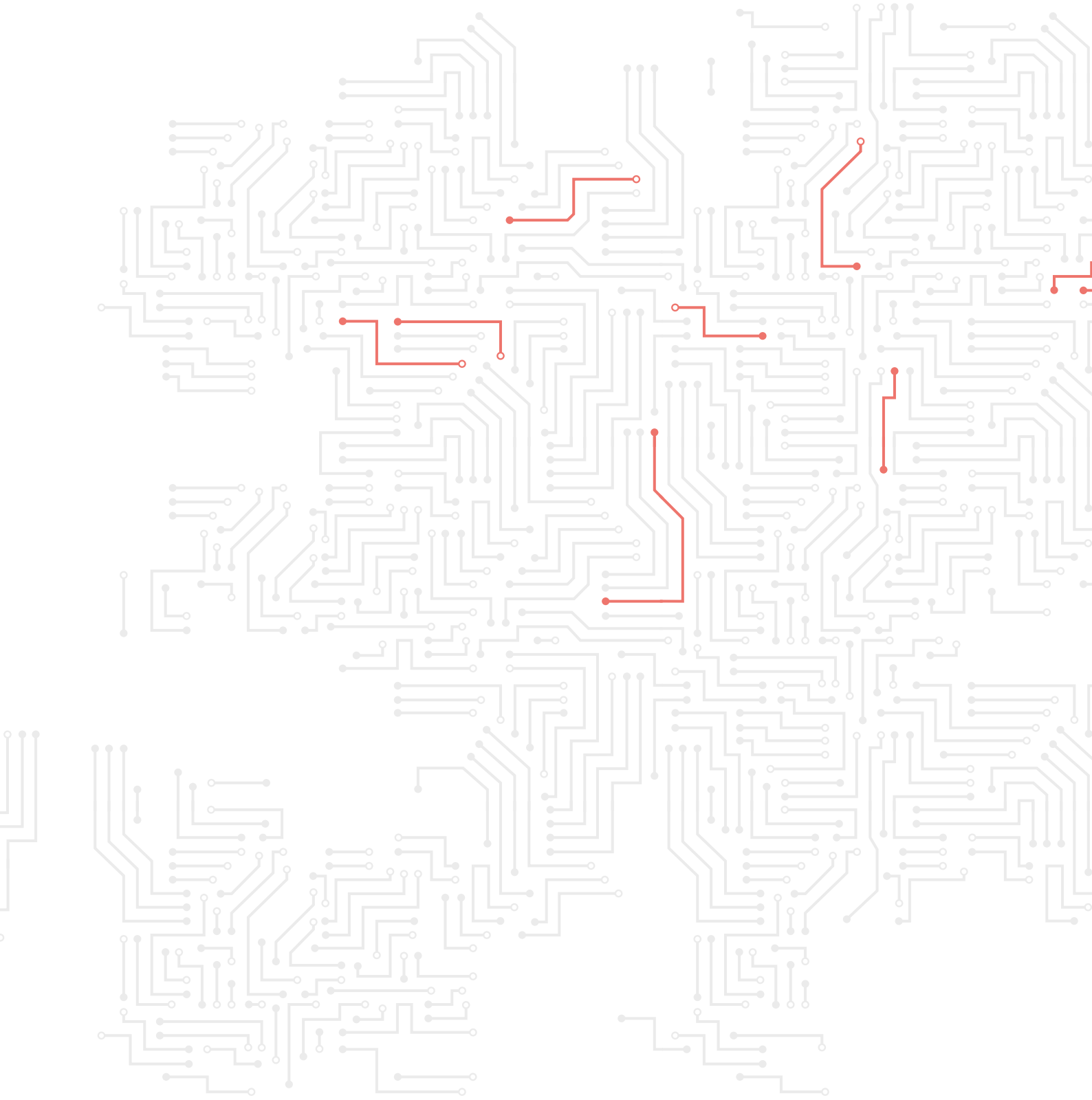
manager in charge of risk management and internal control within the European Union Agency for Cybersecurity (ENISA),

in my capacity as manager in charge of risk management and internal control, declare that, in 2020 risk management and internal controls was responsibility of the Resources Department and this area was identified in problem analysis that led to reorganisation of ENISA in 2020. 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, 30 June 2021

Ingrida TAURINA
Head of Executive Director's Office



IV

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

The management declares having sufficient assurance that ENISA is adequately managed so as to safeguard its financial resources and to pursue the tasks it was entrusted with in 2020.

This assurance is substantiated 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. This assurance is further justified considering that the IAS did not formulate new critical observations.

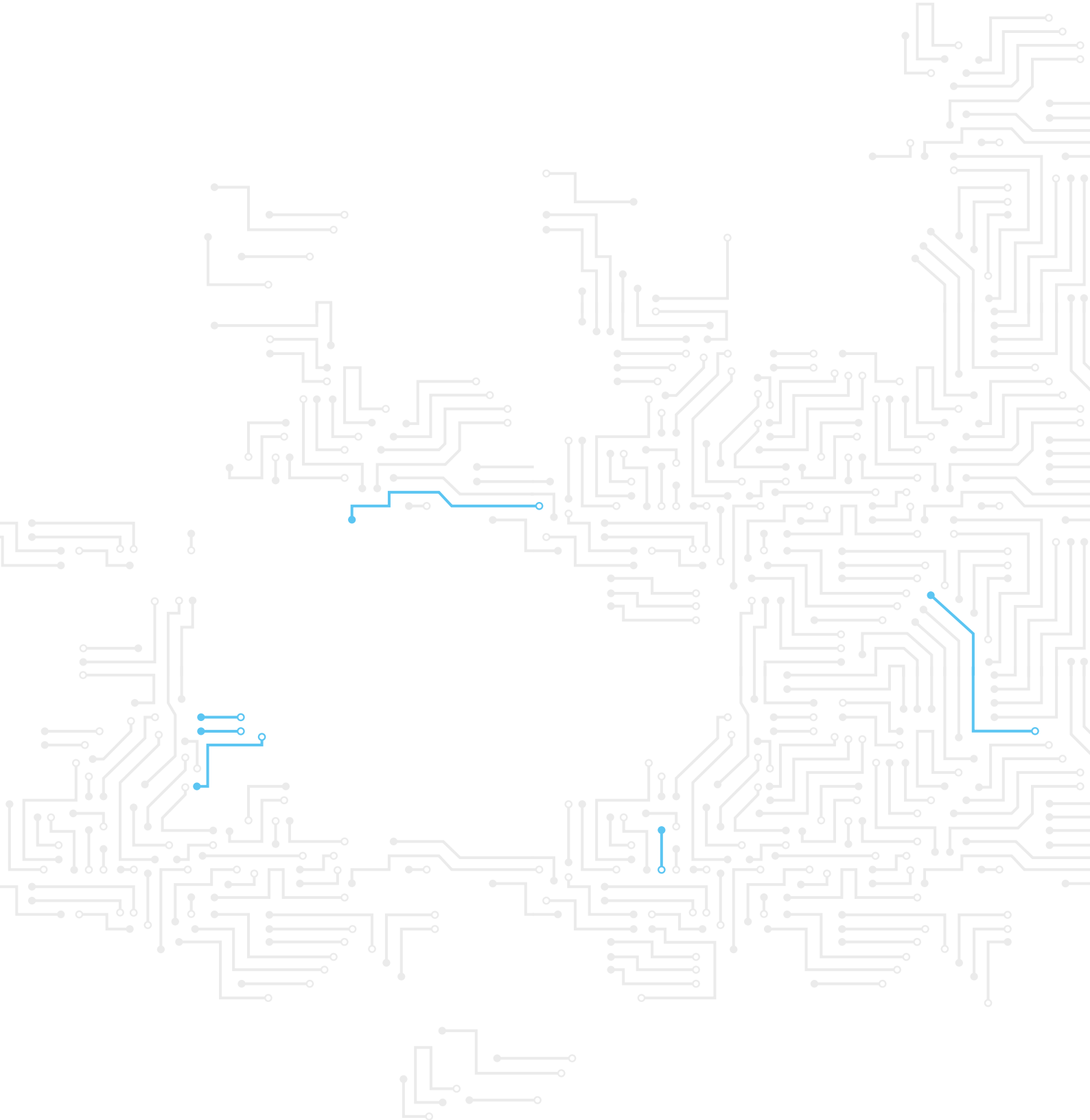
2 RESERVATIONS

Considering the results of the 2020 annual audits performed by the ECA and the IAS, the 2020 results of the internal controls (*ex post* controls and review of the register of exceptions) and the 2020 results of the key financial and operational indicators, the authorising officer can conclude that ENISA operated in 2020 in such a way as to manage appropriately the risks to a large extent.

However, the internal controls and compliance framework applied by the organisation and which to a large extent (except for some urgent modifications in 2020) existed until 31.12.2020, also demonstrated weaknesses, in particular in relation to the unauthorised use of financial rights by staff members in early 2020. Though this incident

represents a breach of trust from the point of view of the authorising officer (Executive Director), it was the inability of internal controls framework to: (1) stop the unauthorised use of the European Commission's corporate financial management system ABAC; (2) restrict the use of financial delegation without prior acceptance of such delegation; and (3) notify the authorising officer on such infringements; which gave rise to the outlined reservations. Though actions were taken, foremost in the framework of the reorganisation in 2020, to address deficiencies and ensure more efficient and effective management of risks, the performance of the internal controls in 2020 was not fully in line with the required standards.

Nevertheless, and after undertaking additional steps in 2020, the authorising officer has reasonable assurance that the allocated resources were used for their intended purposes, in compliance with the legal framework and in accordance with the principle of sound financial management.



V

PART V
DECLARATION OF ASSURANCE

I, the undersigned,

Juhan LEPASSAAR,

Executive Director of the European Union Agency for Cybersecurity,

in my capacity as authorising officer,

declare that the information contained in this report gives a true and fair ([43]) view of the state of the agency's affairs, and state that I have reasonable assurance that the resources assigned to the activities described in this report have been used for their intended purpose and in accordance with the principles of sound financial management, and that the control procedures put in place give the necessary guarantees concerning the legality and regularity of the underlying transactions.

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

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

Athens,

Juhan LEPASSAAR
Executive Director

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

A

ANNEX 1
CORE BUSINESS STATISTICS

No additional information in relation to core business activities.

ANNEX 2
STATISTICS ON FINANCIAL MANAGEMENT

Budget outturn and cancellation of appropriations (in EUR)

Budget outturn	2018	2019	2020
Reserve from the previous years' surplus (+)			
Revenue actually received (+) (*)	11 572 995	16 740 086	21 801 460
Payments made (–)	– 10 345 736	– 11 980 352	-15 050 421
Carry-over of appropriations (–)	– 1 348 657	– 4 357 734	-6 200 614
Cancellation of appropriations carried over (+)	108 302	62 522	180 023
Adjustment for carry-over of assigned revenue appropriations from previous year (+)	124 290	116 393	10 403
Exchange rate difference (+/–)	– 689	– 1 802	-1 291
Adjustment for negative balance from previous year (–)			
Total	**110 505**	**579 113**	**739 560**

(*) Includes the contribution of EUR 435 844 received from the Hellenic authorities to cover office leasing expenditure and EUR 216 496 of other administrative revenues for services to eu-LISA and other minor such as reimbursement of travelling expenditure for staff invited as guest speakers to events.

Execution of commitment appropriations in 2020

In EUR	Chapter	Commitment appropriations authorised *	Commitments made	Commitment rate
A-11	Staff in active employment	6 690 211	6 682 169	99.9%
A-12	Recruitment expenditure	423 139	423 139	100.0%
A-13	Socio-medical services and training	341 041	322 047	94.4%
A-14	Temporary assistance	3 397 012	3 159 097	93.0%
	Title I	10 851 403	10 586 452	97.6%
A-20	Buildings and associated costs	931 889	916 650	98.4%
A-21	Movable property and associated costs	85 120	76 684	90.1%
A-22	Current administrative expenditure	96 954	76 383	78.8%
A-23	Information and communication technologies	2 869 478	2 796 105	97.4%
	Title II	3 983 441	3 865 823	97.0%
B-30	Meetings and missions	247 553	228 544	92.3%
B-32	Horizontal operational activities	1 839 688	1 824 209	99.2%
B-36	Core operational activities	4 772 291	4 620 385	96.8%
	Title III	6 859 532	6 673 138	97.3%
	Total	**21 694 377**	**21 125 412**	**97.38%**

(*) 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) (fund sources C1, C4, C5, R0).

Execution of payment appropriations in 2020

in EUR	Chapter	Payment appropriations authorised (*)	Payments made	Payment rate
A-11	Staff in active employment	6 690 211	6 682 169	99.9%
A-12	Recruitment expenditure	423 139	376 262	88.9%
A-13	Socio-medical services and training	341 041	219 366	64.3%
A-14	Temporary assistance	3 397 012	2 098 896	61.8%
	Title I	10 851 403	9 376 693	86.4%
A-20	Buildings and associated costs	931 889	738 291	79.2%
A-21	Movable property and associated costs	85 120	42 341	49.7%
A-22	Current administrative expenditure	96 954	52 773	54.4%
A-23	Information and communication technologies	2 869 478	1 269 686	44.2%
	Title II	3 983 441	2 103 091	52.8%
B-30	Meetings and missions	247 553	226 382	91.4%
B-32	Horizontal operational activities	1 839 688	561 138	30.5%
B-36	Core operational activities	4 772 291	2 783 118	58.3%
	Title III	6 859 532	3 570 638	52.1%
	Total	**21 694 377**	**15 050 421**	**69.37%**

(*) Payment 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) (fund sources C1, C4, C5, R0).

Breakdown of commitments (with open amounts as of 31 December 2020)

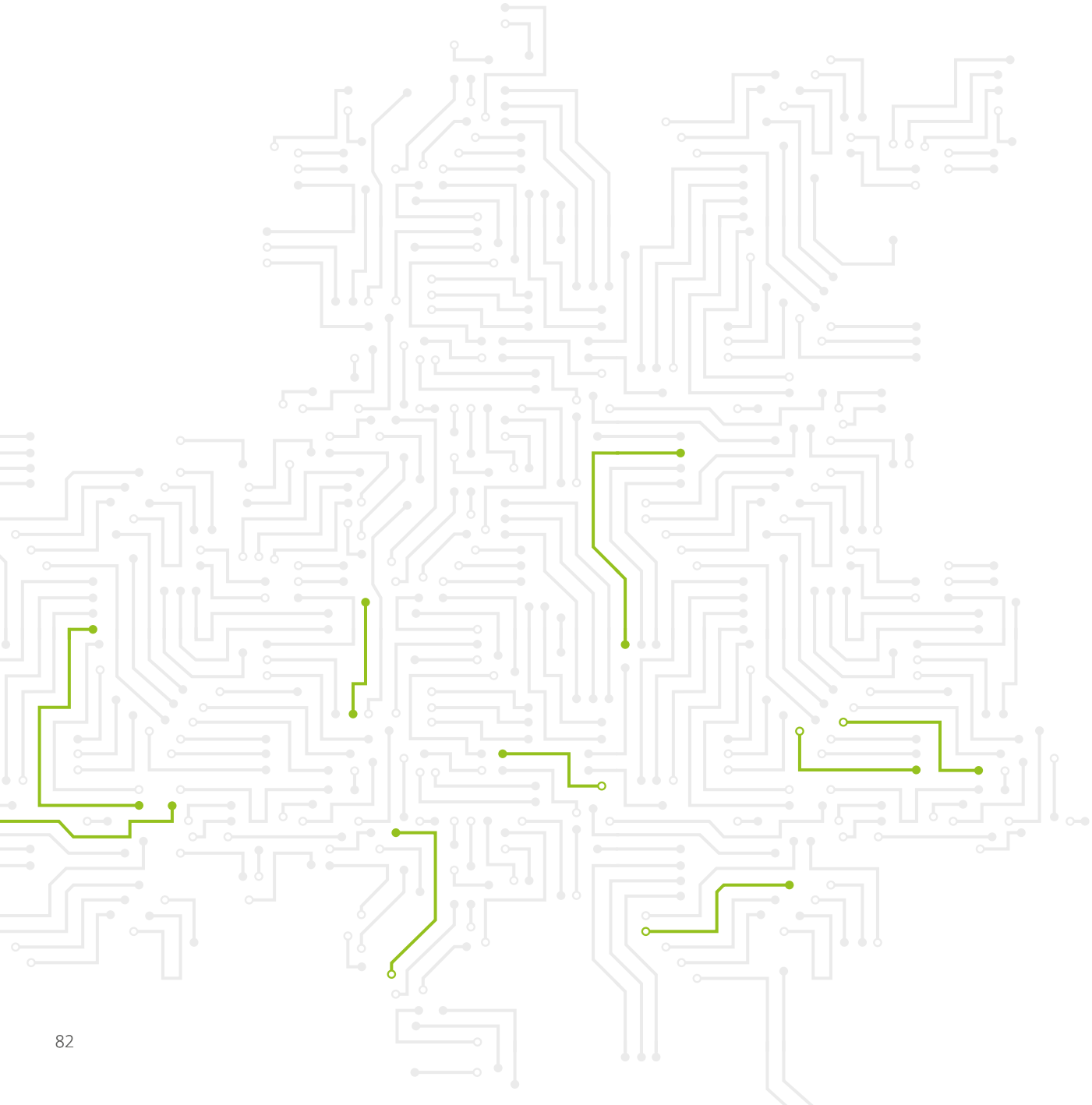
In EUR	Chapter	Commitments made	Payments made	Amount to be paid in 2021	Percentage of amount to be paid
A-11	Staff in active employment	6 682 169	6 682 169	0	0.0%
A-12	Recruitment expenditure	423 139	376 262	46 878	11.1%
A-13	Socio-medical services and training	322 047	219 366	102 680	31.9%
A-14	Temporary assistance	3 159 097	2 098 896	1 060 201	33.6%
	Title I	10 586 452	9 376 693	1 209 759	11.4%
A-20	Buildings and associated costs	916 650	738 291	178 360	19.5%
A-21	Movable property and associated costs	76 684	42 341	34 343	44.8%
A-22	Current administrative expenditure	76 383	52 773	23 610	30.9%
A-23	Information and communication technologies	2 796 105	1 269 686	1 526 419	54.6%
	Title II	3 865 823	2 103 091	1 762 732	45.6%
B-30	Meetings and missions	228 544	226 382	2 162	0.9%
B-32	Horizontal operational activities	1 824 209	561 138	1 263 071	69.2%
B-36	Core operational activities	4 620 385	2 783 118	1 837 267	39.8%
	Title III	6 673 138	3 570 638	3 102 500	46.5%
	Total	**21 125 412**	**15 050 421**	**6 074 991**	**28.8%**

(*) 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) (fund sources C1, C4, C5, R0).

Revenue and income during 2020 (in EUR)

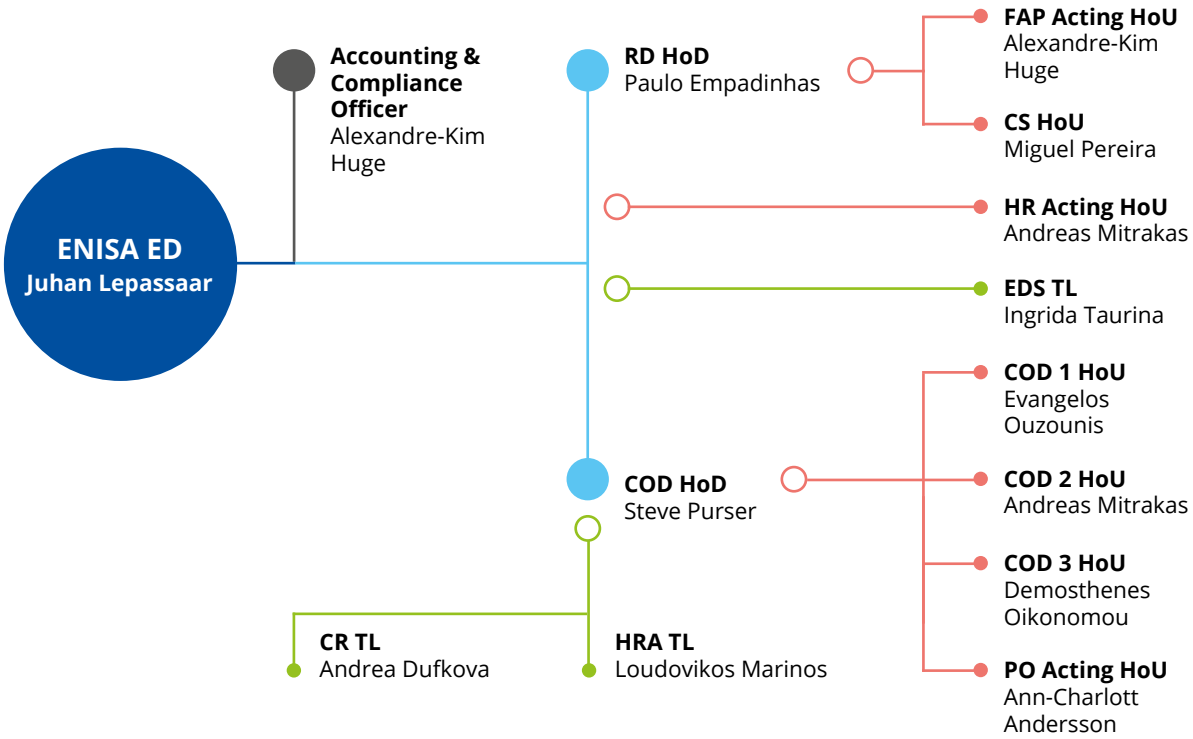
Type of revenue, in EUR	Entitlements established	Revenue received	Amount outstanding at the end of the year
Subsidy from the EU Budget	21 149 120	21 149 120	0
Subsidy from Hellenic Authorities	435 844	435 844	0
Revenue from Administrative Operations	222 096	216 496	5 600
Total	**21 807 060**	**21 801 460**	**5 600**

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



ANNEX 3
ORGANISATIONAL CHART

Internally, ENISA is organised as follows (showing staff as of 31.12.2020).



- Executive Director (ED)
- Head of Department (HoD)
- Head of Unit (HoU)
- Team Leader (TL)

ED – Executive Director
RD – Resource department
HR – Human Resources
FAP – Finance and Procurement
CS – Corporate Services
COD – Core Operations Department
COD 1 – Secure Infrastructure and Services
COD 2 - Data Security and Standardisation
COD 3 - Operational Security
PO – Policy Office
HSA – Horizontal Support and Analysis
CR – CSIRT Relations team
EDS – Executive Director Support Team

ANNEX 4

2020 ESTABLISHMENT PLAN AND ADDITIONAL INFORMATION ON HUMAN RESOURCES MANAGEMENT

2020 establishment plan

Function group (FG) (administrator (AD) / assistant (AST) / assistant-secretary (AST/SC)) and grade	Establishment plan in 2020 voted EU budget		Positions filled as of 31.12.2020[44]	
	Officials	Temporary agents	Officials	Temporary agents
AD 16				
AD 15		1		
AD 14				1
AD 13				
AD 12		6		6
AD 11				
AD 10		5		3
AD 9		12		7
AD 8		21		10
AD 7		3		11
AD 6		3		9
AD 5				
Total number of ADs		51		47
AST 11				
AST 10				
AST 9				
AST 8				
AST 7		4		3
AST 6		8		1
AST 5		5		5
AST 4		1		3
AST 3				2
AST 2				1
AST 1				
Total number of ASTs		18		15

44 Total number includes the in-house AD staff by 31/12/2020 and 9 AD offers sent and accepted by 31/12/2020.

Function group (FG) (administrator (AD) / assistant (AST) / assistant-secretary (AST/SC)) and grade	Establishment plan in 2020 voted EU budget		Positions filled as of 31.12.2020[44]	
	Officials	Temporary agents	Officials	Temporary agents
AST/SC 6				
AST/SC 5				
AST/SC 4				
AST/SC 3				
AST/SC 2				
AST/SC 1				
Total number of AST/SCs				
TOTAL		**69**		**62**

In 2020 the recruitment goal was to reach 69 TA posts; in the end of the year 62 posts were filled. (For the remaining 7 posts offers were duly sent in 2021 with a view to fill them in 2021).

Information on entry level for each type of post

No	Job title	Type of contract (official, temporary agent, contract agent or seconded national expert)	Function group / grade of recruitment	Function (administrative support or operations)
1	Executive director	Temporary agent	AD 14	Top operations
2	Head of department	Temporary agent	AD 11	Administrative/operations
3	Head of unit	Temporary agent	AD 9	Administrative/operations
4	Team leader	Temporary agent	AD 7	Administrative/operations
5	Team coordinator	Contract agent	FG IV	Administrative/operations
6	Team coordinator	Temporary agent	AST 6	Administrative
7	Expert on NIS	Temporary agent	AD 5	Operations
8	Officer for NIS	Contract agent	FG IV	Operations
9	Officer	Contract agent	FG IV	Administrative/operations
10	Assistant	Temporary agent	AST 2	Administrative/operations
11	Assistant	Contract agent	FG I	Administrative/operations
12	Assistant	Temporary agent	AST 4	Administrative/operations
13	Assistant	Contract agent	FG III	Administrative/operations
14	Lead certification expert	Temporary agent	AD 12	Operations
15	Lead policy officer – cybersecurity certification	Temporary agent	AD 8	Operation
16	Lead cybersecurity expert	Temporary agent	AD 9	Operations
17	Seconded national expert	Seconded national expert	n/a	Operations

Information on benchmarking exercise

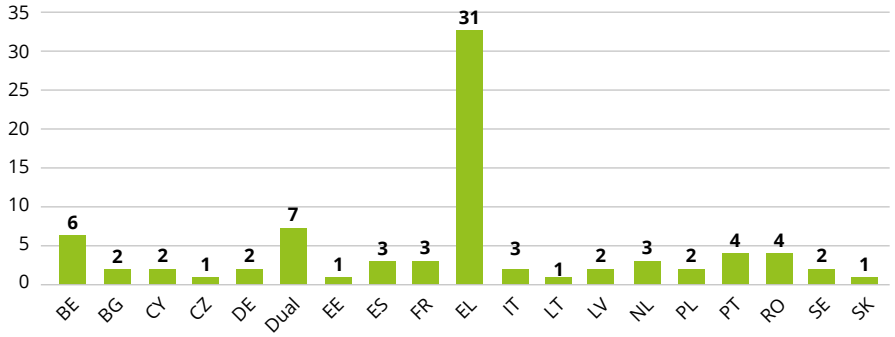
Job type	2020	2019
Total administrative support and coordination	**17.12 %**	**18.37 %**
Administrative support	14.41 %	15.31 %
Coordination	2.70 %	3.06 %
Total operational	**72.97 %**	**70.41 %**
Total operational coordination	4.50 %	5.10 %
General operational	68.47 %	65.31 %
Total neutral	**9.91 %**	**11.22 %**
Finance and control	9.91 %	11.22 %

The bechmarking exercise follow the European Commission's methodology.

Human resources statistics

On 31 December 2020, the agency had a total of 79 statutory staff in-house ([45]).

Employees by nationality



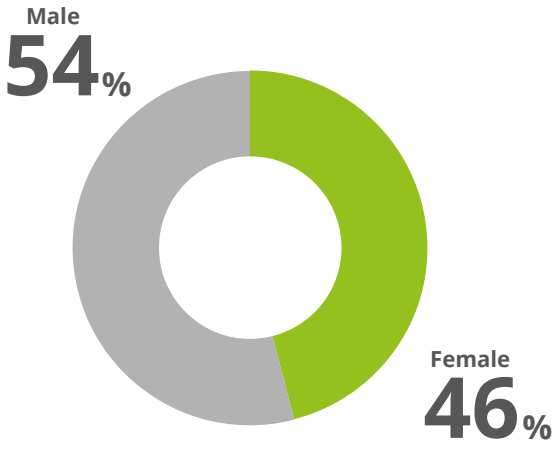
Most represented nationality ([46])	2015		2020	
	Number	%	Number	%
Greek	18 (out of 63)	28.6	31 (out of 79)	39.2

Looking back in 2019 and 2020 positive measures to improve the diversity of nationalities included broad outreach campaigns on popular media across the European Union, closer consideration on the nationality spread in relation to competencies requested, and specific provisions on the vacancy notices have been continued.

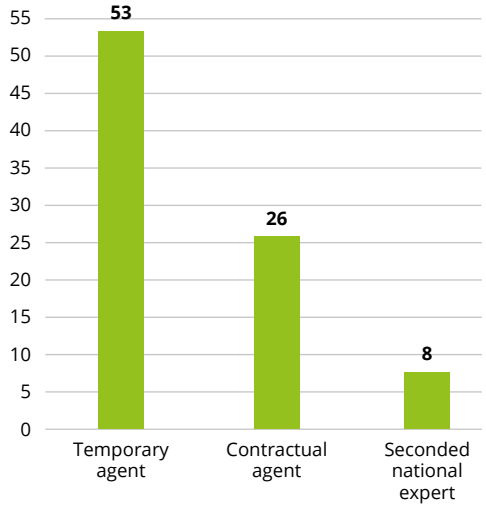
45 The data does not include the additional 9 AD appointments as per footnote 15.

46 The imbalance in the most represented nationality at ENISA is related to several factors, such as the level of posts and related salaries, which may be perceived as less appealing for job seekers from relatively more advanced Member State economies; the fact that ENISA is considered to offer better working conditions than the average conditions offered in the Greek job market; the small job market in Greece for cybersecurity professionals; and historical decisions taken by previous Appointing Authority powers delegated to the Executive Director (AIPNs). Other reasons that may be cited are the need for stability during the start-up phase of the Agency, with staff members from the hosting Member State (Greece) being less likely to resign (resulting in lower turnover), which, because of the relatively young age of the Agency, is still having an impact; the relatively better academic profile of Greek candidates applying for lower level posts; the relatively smaller payroll cost for Greek staff who are better qualified than average and who do not require an expatriation allowance; and the general tendency for people to remain in lower level positions in the home country.

Gender distribution – all departments



Number of employees by contract type



	2015		2020	
	Number	%	Number	%
Female managers	0	0	2	20
Male managers	10	100	8	80

Implementing rules

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

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

Appraisal and reclassification/promotions

Implementing rules in place

		Yes	No	if no, which other implementing rules are in place
Reclassification of temporary agents	Model decision C(2015)9560	x		
Reclassification of contract agents	Model decision C(2015)9561	x		

Reclassification of temporary agents

Grades	2017 (Ref year 2016)	2018 (Ref year 2017)	2019 (Ref year 2018)	2020 (Ref year 2019)	Actual average over 5 years	Average over 5 years according to decision C(2015)9563
AD05	–	–	–	–	–	2.8
AD06	1	1	2	3	3.7	2.8
AD07	1	–	–	–	4	2.8
AD08	1	–	1	1	5.7	3
AD09	–	–	–	1	10	4
AD10	–	–	–	–	–	4
AD11	–	1	–	–	3	4
AD12	–	–	–	–	–	6.7
AD13	–	–	–	–	–	6.7
AST1	–	–	–	–	–	3
AST2	–	–	–	–	–	3
AST3	2	1	1	1	4.4	3
AST4	–	1	1	1	5.6	3
AST5	1	–	1	–	5.5	4
AST6	1	–	–	–	4	4
AST7	–	–	–	–	–	4
AST8	–	–	–	–	–	4
AST9	–	–	–	–	–	n/a
AST10 (senior assistant)	–	–	–	–	–	5

*There are no AST/SCs at ENISA

Reclassification Contract agents Re

Contract agents	Grade	Staff members reclassified in 2020 (Ref year 2019)	Average number of years in grade of reclassified staff members	Average number of years in grade of reclassified staff members according to decision C(2015)9561
Function group IV	17	–	–	Between 6 and 10 years
	16	–	–	Between 5 and 7 years
	15	–	–	Between 4 and 6 years
	14	–	–	Between 3 and 5 years
	13	–	–	Between 3 and 5 years
Function group III	11	–	–	Between 6 and 10 years
	10	–	–	Between 5 and 7 years
	9	3	5.7	Between 4 and 6 years
	8	1	4.8	Between 3 and 5 years
Function group II	6	–	–	Between 6 and 10 years
	5	–	–	Between 5 and 7 years
	4	–	–	Between 3 and 5 years
Function group I	3	–	–	n/a
	2	–	–	Between 6 and 10 years
	1	–	–	Between 3 and 5 years

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 school year 2020–2021, 12 service-level agreements are in place

ANNEX 5
HUMAN AND FINANCIAL RESOURCES BY ACTIVITY

Human resources by activity

Activities	Planned full-time equivalents	Actual full-time equivalents
Activity 1: EXPERTISE. Anticipate and support Europe's knowledge in facing emerging cybersecurity challenges	14.45	13.62
Activity 2: POLICY. Promote Network and Information Security as an EU policy priority	17.29	13.45
Activity 3: CAPACITY. Support Europe in maintaining state-of-the-art Network and Information Security capacities	12.78	12.19
Activity 4. Cooperation. Foster the operational cooperation within European cybersecurity community	14.45	12.22
Activity 5 – Cybersecurity certification. Developing cybersecurity certification schemes for digital products, services and processes.	14.45	7.33
Activity 6 – Enabling. Reinforce ENISA´s impact	37.58	62.23
TOTAL ACTIVITIES 1–6	**111**	**121**[47]

NB: The figures above provide an estimation of the human resources (i.e. number of employees) allocated to each of the agency's activities.

47 121 FTEs comprises: 108 FTEs used in 2020; 6 FTEs – interims were assigned to specific projects and not part of the SPD; 7 FTEs – interims were assigned for extra workload.

ANNEX 6
GRANT, CONTRIBUTION AND SERVICE-LEVEL AGREEMENT

ENISA does not receive any form of grant.

As per the provisions of the seat agreement (Greek law 4627/2019) concluded with the Hellenic authorities, ENISA received a contribution of EUR 435 844 to cover the 2020 leasing expenditure of its offices.

In addition, a service-level agreement with the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA) was active in 2020 for the purposes of sharing its knowledge and resources related to the organisation of eu-LISA's security exercises along with making its online exercise platform available. The generated income amounts to EUR 97 920 per year to cover staff costs and overheads. Two full-time equivalents, each equivalent to a contract agent post, are allocated to these tasks.

ENISA signed a Service-Level agreement with Cedefop in the reporting year to increase cooperation and to share services between the two Agencies.

ANNEX 7
ENVIRONMENTAL MANAGEMENT

See point 2.10 for information in relation to environmental management at ENISA.

ANNEX 8
ANNUAL ACCOUNTS

Statement of financial position

Assets and liabilities	Financial position on 31.12.2020 (in EUR)	Financial position on 31.12.2019 (in EUR)
I. Non-current assets	2 124 212	746 216
Intangible fixed assets	25 094	52 469
Tangible fixed assets	2 082 618	677 247
Guarantee for leased building	16 500	16 500
II. Current assets	7 256 337	5 084 080
Short-term receivables	347 054	180 191
Cash and cash equivalents	6 909 283	4 903 889
TOTAL ASSETS (I + II)	**9 380 549**	**5 830 296**
III. Non-current liabilities	0	0
Long-term provision for risk and charges	0	0
IV. Current liabilities	2 067 160	1 392 974
Commission pre-financing received	739 560	579 113
Accounts payable	70 605	41 578
Accrued liabilities	1 256 995	772 283
TOTAL LIABILITIES (III + IV)	**2 067 160**	**1 392 374**
V. Net assets	7 313 389	4 437 322
Accumulated result	4 437 322	1 696 700
Surplus (/deficit) for the year	2 876 067	2 740 622
TOTAL LIABILITIES AND NET ASSETS (III + IV + V)	**9 380 549**	**5 830 296**

Statement of financial performance

Revenue and expenses	2020 financial performance (in EUR)	2019 financial performance (in EUR)
Revenue from the EU subsidy	20 409 560	15 713 839
Revenue from administrative operations	553 302	557 472
Total operating revenue	20 962 862	16 271 311
Administrative expenses	– 13 511 894	– 10 411 311
Staff expenses	– 7 796 310	– 6 369 310
Fixed-asset-related expenses	– 347 811	– 234 090
Other administrative expenses	– 5 367 773	– 3 807 911
Operational expenses	– 4 573 301	– 3 115 939
Total operating expenses	– 18 085 195	– 13 527 250
Surplus (/deficit) from operating activities	2 877 677	2 744 061
Financial expenses	– 309	– 1 637
Exchange rate loss	– 1 291	– 1 802
Surplus (/deficit) from non-operating activities	– 1 600	– 3 439
Surplus (/deficit) from ordinary activities	2 876 067	2 740 622
Surplus (/deficit) for the year	2 876 067	2 740 622

ANNEX 9

LIST OF ACRONYMS, INITIALISMS AND ABBREVIATIONS

AD	Administrator
APF	Annual Privacy Forum
AST	Assistant
AST/SC	Assistant-secretary
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CESICAT	Centre de Seguretat de la Informació de Catalunya
CEF	Connecting Europe Facility
CEP	Cyber exercise platform
CERT-EU	Computer Emergency Response Team for the EU Institutions, Bodies and Agencies
CIIP	Critical information infrastructure protection
CISO	Chief information security officer
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
CTI	Cyberthreat intelligence
CyLEE	Cyber law enforcement exercise
DSP	Digital service provider
EASA	European Union Aviation Safety Agency
EC3	Europol's European Cybercrime Centre
ECA	European Court of Auditors
ECCG	European Cybersecurity Certification Group
ECSC	European Cyber Security Challenge
ECSO	European Cyber Security Organisation
ECSM	European Cyber Security Month
EDPS	European data protection supervisor
EEA	European Economic Area
EECC	European Electronic Communications Code
EFTA	European Free Trade Association
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cybersecurity
ERA	European Union Agency for Railways
ETL	ENISA threat landscape
ETIS	The community for Telecom professionals
ETSI	European Telecommunications Standards Institute

EU	European Union
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
GDPR	General data protection regulation
HoD	Head of department
HoU	Head of unit
IAS	Internal Audit Service
ICT	information and communications technology
IoT	internet of things
ISAC	Information Sharing and Analysis Centre
IT	information technology
MeliCERTes	Name of a project funded by the EU to connect CSIRTS around the Member States
NCSS	National cybersecurity strategy
NIS	Network and information security
NIS CG	NIS Cooperation Group
NISD	NIS directive
OES	Operator of essential services
OpenCSAM	Open Cyber Situational Awareness Machine
SCCG	Stakeholder Cybersecurity Certification Group
SOP	Standard operating procedure
SOPex	SOP exercise

NOTES

TPAB-21-001-EN-N

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

Publications Office
of the European Union

ISBN 978-92-9204-502-9